Политика применения сертификатов и регламент удостоверяющего центра национальной грид-сети Республики Беларусь

Версия 1.3

Идентификатор документа: 1.3.6.1.4.1.24432.11.1.1.3

14 октября 2010

Содержание

Политика применения сертификатов и регламент удостоверяющего центра национальной грид-сети Республики Беларусь

1 Введение

Данный документ описывает правила и процедуры, используемые удостоверяющим центром национальной грид-сети Республики Беларусь (далее – УЦ).

1.1 Обзор

УЦ обеспечивает функционирование инфраструктуры открытых ключей (далее – ИОК), необходимой для использования и предоставления грид-ресурсов в Республике Беларусь.

Государственное научное учреждение "Объединенный институт проблем информатики Национальной академии наук Беларуси" (далее – ОИПИ НАН Беларуси) координирует работу УЦ.

Этот документ объединяет политику применения сертификатов и регламент УЦ, содержит набор процедур УЦ, описывающих порядок выпуска сертификатов и обязанности вовлеченных сторон.

УЦ расположен в здании ОИПИ НАН Беларуси.

Настоящий документ структурирован согласно стандарту RFC 3647.

Настоящий документ был выпущен 14 октября 2010 и вступил в силу 15 октября 2010.

Срок действия настоящего документа определяется периодом функционирования УЦ.

Настоящий документ разработан в соответствии с Законом «Об информации, информатизации и защите информации» от 10.11.2008 г. № 455-З, Законом «Об электронном документе» 10.01.2000 №357-З, СТБ П 34.101.24-2008 «Информационные технологии. Электронные цифровые подписи и инфраструктуры».

1.2 Наименование и обозначение документа

1.2.1 Заголовок документа: “Политика применения сертификатов и регламент удостоверяющего центра национальной грид-сети Республики Беларусь”.

1.2.2. Версия документа: 1.3.

1.2.3. Идентификатор объекта (далее – ИО): 1.3.6.1.4.1.24432.11.1.1.3. (стандарт записи ASN.1)

Таблица 1 описывает значение ИО.

Таблица 1 – Значение ИО

1.3.6.1.4.1	Префикс комитета по цифровым адресам в интернете IANA
.24432	ОИПИ НАН Беларуси
.11	УЦ
.1	CP/CPS (Политика применения сертификатов и регламент УЦ)
.1.3	главный и второстепенный номер CP/CPS

1.3 Участники инфраструктуры открытых ключей

ИОК обеспечивает аутентификацию с помощью открытых ключей и содержит в своей структуре УЦ, который состоит из сертификационного центра (далее – СЦ) и не менее одного регистрационного центра (далее – РЦ).

1.3.1 Сертификационный центр

СЦ непосредственно издает сертификаты для абонентов УЦ. СЦ не издает сертификаты для СЦ нижних уровней (подчиненных).

1.3.2 Регистрационный центр

Функции РЦ определяет администратор СЦ. Операторы РЦ несут ответственность за проверку идентификационных данных абонентов и подтверждение запросов на выдачу сертификатов. Операторы РЦ не издают сертификаты. Список РЦ доступен на сайте УЦ: http://ca.grid.by.

РЦ должен обмениваться данными с СЦ безопасными методами, такими как подписанные электронные письма и защищённые с помощью SSL веб-страницы, подлинность которых подтверждена посредством двусторонней аутентификации.

Каждые два года каждый РЦ должен подписывать соглашение с УЦ, подтверждая строгое соблюдение процедур, описанных в настоящем документе.

1.3.3 Абоненты

УЦ выпускает сертификаты для физических лиц, серверов и служб. Физические лица, имеющие право на получение сертификата УЦ – сотрудники, аспиранты и студенты организаций-резидентов Республики Беларусь, вовлеченных в использование или развертывание грид-инфраструктуры.

1.3.4 Доверяющие стороны

Участники вычислительной грид-инфраструктуры, которые используют открытые ключи выпущенных УЦ сертификатов для проверки подписи и/или шифрования, рассматриваются как доверяющие стороны.

1.3.5 Другие участники

Не определены.

1.4 Использование сертификата

1.4.1 Допустимое использование сертификатов

Сертификаты физических лиц используются при аутентификации физических лиц для получения доступа к ресурсам грид-сети.

Сертификаты серверов используются для аутентификации ресурсов грид-сети, например вычислительных узлов.

Сертификаты служб используются для аутентификации серверных приложений, работающих в грид-сети, и/или для шифрования данных при передаче.

Кроме того, допустимо применять сертификаты физических лиц для подписания электронной почты и аутентификации физических лиц, используя протокол HTTPS (Hypertext Transfer Protocol Secure).

1.4.2 Ограничения использования сертификатов

Использование сертификатов не в соответствии с действующим законодательством Республики Беларусь недопустимо.

1.5 Администрирование политики

1.5.1 Организация, администрирующая документ

Настоящий документ разработан и сопровождается Объединенным институтом проблем информатики Национальной академии наук Беларуси (ОИПИ НАН Беларуси).

Адрес УЦ для обращения по вопросам функционирования:

Удостоверяющий центр национальной грид-сети

Объединенный институт проблем информатики Национальной академии наук Беларуси

Ул. Сурганова, 6

Минск 220012, Беларусь
Тел: +375 17 2842083

1.5.2 Контактное лицо

Контактное лицо по вопросам относительно этого документа или УЦ:
Юрий Земцов
Объединенный институт проблем информатики Национальной академии наук Беларуси
Ул. Сурганова, 6
Минск 220012, Беларусь
Тел: +375 17 2842083
E-mail: ca@newman.bas-net.by

1.5.3 Лицо, определяющее соответствие УЦ требованиям регламента

Лицо, определяющее соответствие УЦ требованиям регламента, указано в пункте 1.5.2.

1.5.4 Процедура квалифицирования регламента

Новые версии регламента УЦ проверяются на соответствие минимальным требованиям, определенным федерацией International Grid Trust Federation (IGTF). После того как одобрены существенные изменения (если таковые имеются) документ предоставляется для утверждения Европейской Федерации управления политиками European Policy Management Authority for Grid Authentication (EUGridPMA). О несущественных изменениях в документе достаточно сообщить EUGridPMA.

1.6 Определения и сокращения

Абонент – тот (то), кто (что) делает заявку на получение сертификата или которому (чему) выдан сертификат.

Удостоверяющий центр – доверенный центр одного или более абонентов для создания и передачи прав сертификатов.

Регламент — это документ, содержащий описание процедур и действий, которые удостоверяющий центр использует при выдаче, управлении, отзыве и обновлении сертификатов.

Политика применения сертификата – определенный свод правил, который указывает на применимость сертификата в определенных кругах и/или класс применения в соответствии с общими требованиями безопасности.

Сертификат – электронный документ, который содержит открытый ключ абонента и подписан удостоверяющим центром. Сертификат также содержит сведения о владельце открытого ключа, например, информацию, которая его дополнительно идентифицирует. Таким образом, выдавая сертификат, издатель удостоверяет подлинность связи между открытым ключом абонента и информацией, которая его идентифицирует.

Список отозванных сертификатов – подписанный список, в котором указывается ряд сертификатов, более не признаваемых действительным эмитентом сертификатов.

Определения и сокращения приведены в таблице 2:

Таблица 2 – Определения и сокращения

ASN.1	Abstract Syntax Notation One
CN	Common Name
CP/CPS	Certificate Policy/Certification Practice Statement
DN	Distinguished Name
DNS	Domain Name System
EUGridPMA	European Policy Management Authority for Grid Authentication

FQDN	Fully Qualified Domain Name
HTTPS	Hypertext Transfer Protocol Secure
IANA	Internet Assigned Numbers Authority
IGTF	International Grid Trust Federation
OCSP	Online Certificate Status Protocol
OID	Object Identifier
RFC	Request For Change
SSL	Secure Sockets Layer
TLS	Transport Layer Security
USB	Universal Serial Bus
ИО	Идентификатор объекта
ИОК	Инфраструктура открытых ключей
О	Организация
ОИПИ НАН Беларуси	Объединенный институт проблем информатики Национальной академии наук Беларуси
РЦ	Регистрационный Центр
СОС	Список отозванных сертификатов
СЦ	Сертификационный Центр
УЦ	Удостоверяющий Центр
ФИО	Фамилия Имя Отчество

2 Публикации и обязанности репозитория

2.1 Репозиторий

УЦ использует онлайновый репозиторий, который содержит:
– корневой сертификат УЦ;
– списки отозванных сертификатов (СОС);
– копию последней версии настоящего документа и всех предыдущих версий;
– список функционирующих в настоящее время РЦ;
– ссылки к доверенным репозиториям, где опубликована информация УЦ;
– другую значимую информацию.

Контактная информация УЦ для обращений по вопросам, касающимся репозитория:

Удостоверяющий центр национальной грид-сети
Объединенный институт проблем информатики
Национальной академии наук Беларуси
ул. Сурганова, 6
Минск 220012, Беларусь
Тел: +375 17 2842083
E-mail: ca@newman.bas-net.by
Сайт: http://ca.grid.by

2.2 Публикация информации о сертификации

УЦ обязан поддерживать онлайновый репозиторий, описанный в пункте 2.1.

2.3 Время или частота публикации

Корневой сертификат УЦ публикуется, как только он издан.
Частота публикации СОС определена в пункте 4.9.7.
Настоящий документ публикуется при внесении каких-либо изменений.

2.4 Средства управления доступом к репозиторию

Онлайновый репозиторий поддерживается на основании принципа максимальных усилий и доступен 24 часа в сутки, 7 дней в неделю. УЦ может наложить более ограниченную политику управления доступом к репозиторию по его усмотрению. Однако УЦ не ограничивает доступ к настоящему документу, размещенным сертификатам и СОС.

3 Идентификация и аутентификация

3.1 Назначение имен

3.1.1 Типы имен

Все отличительные имена DN, в соответствии с данным документом, начинаются с атрибутов “DC=by, DC=grid”.

Имена абонентов должны быть отформатированы в соответствии со стандартом X.501, части имени domainComponent должны иметь тип IA5String, части имени organizationName и commonName должны иметь тип PrintableStrings.

3.1.1.1. Корневой сертификат:

– commonName должно быть “Belarusian Grid Certification Authority”.

– organizationName должно быть “uiip.bas-net.by”.

3.1.1.2. Сертификат физического лица:

– commonName должно включать имя и фамилию физического лица.

– organizationName должно включать имя домена организации.

3.1.1.3. Сертификат сервера:

– commonName должно быть полным доменным именем сервера (FQDN).

– organizationName должно включать имя домена организации.

3.1.1.4. Сертификат грид-службы:

– commonName должно включать префикс "servicename/", за которым следует полное доменное имя сервера (FQDN).

– organizationName должно включать имя домена организации.

3.1.2 Необходимость персональных данных

Имя физического лица, указанное в сертификате, должно совпадать с персональными данными идентификационного документа.

Для сертификатов физических лиц, атрибут CN содержит имя и фамилию физического лица (строго в указанном порядке) в английском алфавите как представлено в паспорте резидента Республики Беларусь. Чтобы разрешить неоднозначность между различными физическими лицами с одним и тем же именем или позволить одному и тому же физическому лицу иметь более одного сертификата, атрибут CN сертификата физического лица может содержать другой дополнительный текст, кроме идентификационного имени физического лица. Дополнительный текст должен быть отформатирован так, чтобы его нельзя было перепутать с именем физического лица; рекомендуется, чтобы текст следовал за именем физического лица после пробела в качестве разделителя и был заключен в круглые скобки. УЦ никак иначе не проверяет содержимое дополнительного текста, и поэтому доверяющим сторонам запрещается полагаться на содержание дополнительного текста.

Для сертификатов сервера атрибут CN содержит полное доменное имя сервера.

Для сертификатов служб атрибут CN содержит название службы и через разделитель (/) полное доменное имя сервера, на котором будет работать данная служба.

3.1.3 Анонимность или псевдонимы абонентов

Анонимные сертификаты или сертификаты с использованием псевдонимов не издаются УЦ.

3.1.4 Правила интерпретации различных форм имен

См. пункты 3.1.1 и 3.1.2.

3.1.5 Уникальность имен

Отличительное имя DN должно быть уникальным для каждого абонента. Если DN, представленное абонентом не уникально, то УЦ потребует, чтобы абонент повторно представил запрос с некоторым изменением атрибута CN, чтобы обеспечить уникальность имени. Согласно настоящему документу два имени считаются идентичными, если они отличаются только регистром, количеством символов подчеркивания или пробелов между словами. Таким образом, регистр, символы подчеркивания или пробела не должны использоваться для различия имен. Сертификат должен относиться к уникальному физическому лицу или ресурсу или службе. Сертификат должен использоваться только владельцем.

УЦ гарантирует, что отличительное имя DN не будет использоваться повторно другим абонентом. Если физическое лицо запрашивает сертификат с таким же DN, как в уже существующем сертификате (независимо от статуса этого сертификата), и запрос не является запросом на обновление или замену сертификата, то оператор РЦ обратится к персональной удостоверяющей информации, чтобы проверить, что физическое лицо – тот же субъект, который был идентифицирован при получении первоначального сертификата. Если эта идентичность не может быть установлена, имя DN не будет использоваться повторно.

3.1.6 Признание, аутентификация и роль товарных марок

Не оговаривается.

3.2 Изначальная проверка подлинности

3.2.1 Способ доказательства обладания личным ключом

При запросе на выдачу сертификата УЦ проверяет факт обладания личным ключом, соответствующим открытому ключу, на который запрашивается сертификат: при идентификации РЦ сравнивает распечатанный запрос на выдачу сертификата с полученным электронным запросом.

3.2.2 Аутентификация организации

РЦ должен проверить идентификационную информацию организации, чтобы убедится в том, что:

– организация является участником грид-проекта;

– организация зарегистрирована и функционирует в Республике Беларусь. Регистрация подтверждается Свидетельством о государственной регистрации в Едином государственном регистре юридических лиц и индивидуальных предпринимателей.

Физическое лицо, которое делает запрос, должно представить доказательство, подтверждающее принадлежность к организации, которую он представляет.

3.2.3 Аутентификация абонента

3.2.3.1. Сертификат физического лица:

Абонент, запрашивающий сертификат, должен сгенерировать запрос на получение сертификата, распечатать запрос на выдачу сертификата, указать свое имя, фамилию,

номер телефона, электронный адрес и поставить подпись для дальнейшего сравнения. Абонент должен встретиться лично с представителем РЦ и показать следующие документы: паспорт резидента Республики Беларусь, подтверждая, абонент – действительный субъект; действительные документы, выданные организацией абонента и подтверждающие принадлежность к данной организации; распечатанный запрос на выдачу сертификата. Если предоставленный адрес электронной почты корректен, паспорт действителен, фотография соответствует предъявителю, и распечатанный запрос на выдачу сертификата соответствует полученному электронному запросу, тогда РЦ должен считать абонента успешно аутентифицированным. РЦ должен убедиться в правомерности использования доменного имени организации в атрибуте отличительного имени organizationName, указанного в запросе. РЦ регистрирует все действия по идентификации личности. При идентификации абонентов РЦ делает копии предоставленных документов. Копии отправляются в СЦ для архивного хранения.

Запрос, отправленный в РЦ, будет считаться аутентифицированным, если он подписан личным ключом, который соответствует действительному сертификату абонента.

3.2.3.2. Сертификат сервера или службы:

Сертификаты серверов могут запрашивать только администраторы, ответственные за данные серверы. Подписанные личным ключом, который соответствует действительному сертификату ответственного администратора, запросы на выдачу сертификата отправляют в РЦ по электронной почте. Чтобы сделать запрос на выдачу сертификата сервера, должны быть выполнены следующие условия:

– сервер должен иметь правильное полное доменное имя (FQDN);

– администратор должен уже обладать действительным сертификатом УЦ;

– РЦ должен убедиться, что администратор является ответственным за сервер.

РЦ должен архивировать все подтвержденные запросы на выдачу сертификата сервера или службы, полученные по электронной почте.

3.2.4 Непроверяемая информация абонента

Не определена.

3.2.5 Проверка полномочий

Абонент, запрашивающий услугу УЦ, должен предоставить действительные документы, подтверждающие его принадлежность к организации.

3.2.6 Критерии взаимодействия

Не определены.

3.3 Идентификация и аутентификация запросов на замену ключей в сертификате

3.3.1 Идентификация и аутентификация запросов при плановой замене ключей

Предупреждения об истечении срока действия сертификатов будут отосланы абонентам прежде, чем наступит время плановой замены ключей в сертификате. Замена ключей до истечения срока действия может осуществляться при предоставлении запроса, подписанного личным ключом, который соответствует действительному сертификату физического лица. При замене ключей в сертификате по истечению срока действия используется такая же процедура аутентификации как при получении первоначального сертификата. Каждые три года РЦ должен аутентифицировать абонента, как описано в пункте 3.2.3.

3.3.2 Идентификация и аутентификация запросов на замену ключей в сертификате после отзыва

Процедура аутентификации такая же, как и при получении первоначального сертификата, как описано в пункте 3.2.3.

3.4 Идентификация и аутентификация запроса на отзыв

Запрос на отзыв сертификата должен быть аутентифицирован одним из следующих способов:

– подписанием электронного запроса на отзыв личным ключом, соответствующим сертификату, который требуется отозвать; сертификат, выданный УЦ должен быть действителен, с неистекшим сроком действия и не отозван;

– для абонентов, которые не имеют действительного сертификата УЦ, но имеют основание на отзыв: при личной идентификации как описано в пункте 3.2.3;

– если запрос на отзыв сертификата сервера или службы, то электронное письмо должно быть подписано личным ключом, соответствующим сертификату физического лица, ответственному за сервер или службу. При невозможности провести аутентификацию по электронной почте, запрос будет аутентифицирован, используя процедуру, описанную в пункте 3.2.3;

– запрос на отзыв от РЦ должен быть сделан посредством электронной почты и подписан действительным ключом оператора РЦ.

4 Операционные требования к жизненному циклу сертификата

4.1 Заявка на выдачу сертификата

4.1.1 Кто может подать заявку на выдачу сертификата

Абонент, подающий заявку на получение сертификата, должен:

– отвечать требованиям к абонентам, описанным в пункте 1.3.3;

– прочитать и соблюдать все положения настоящего документа;

– сгенерировать ключевую пару, используя надежный метод. Личный ключ должен быть не менее 1024 бита;

– использовать сложный пароль, длиною не менее 12 символов.

4.1.2 Процесс регистрации и обязанности

4.1.2.1. Сертификат физического лица:

Абонент должен предоставить запрос на получение сертификата посредством электронной почты обслуживающему РЦ. Обслуживающий РЦ должен аутентифицировать абонента согласно процедуре, описанной в пункте 3.2.3. При замене ключей в сертификате абонент должен следовать процедурам, описанным в пункте 4.7.

4.1.2.2. Сертификат сервера или службы:

Абонент должен иметь действительный сертификат физического лица, прежде чем сделать запрос на выдачу сертификата сервера или службы. Запрос на выдачу сертификата должен быть сделан посредством электронной почты. Абонент должен отправить электронное письмо по адресу электронной почты, указанному в пункте 1.5.2, с прикрепленными запросом на выдачу сертификата, подписанным личным ключом, соответствующим сертификату физического лица, и утверждением в теле электронного письма, что он – лицо, ответственное за сервер/службу. Запрос на выдачу сертификата будет отправлен соответствующему РЦ, который подтвердит или не подтвердит запрос согласно пунктам 4.2.1 и 4.2.2.

4.2 Обработка заявки на выдачу сертификата

4.2.1 Аутентификации и идентификации заявки

Все заявки на выдачу сертификата будут аутентифицироваться и подтверждаться РЦ согласно пункту 3.2.3. Процедура при запросе на замену ключей в сертификате рассмотрена в пункте 3.3.1. При успешной аутентификации, информация, включенная в запрос на выдачу сертификата, будет подтверждаться СЦ.

4.2.2 Одобрение или отклонение заявки на выдачу сертификата

Запрос на выдачу сертификата должен удовлетворять следующим требованиям:

– абонент должен быть аутентифицирован РЦ;

– абонент должен отвечать требованиям к абонентам в соответствии с настоящим документом;

– абонент должен иметь действительный адрес электронной почты;

– абонент должен предоставить отличительное имя, удовлетворяющее требованиям к отличительным именам УЦ;

– отличительное имя должно быть уникально;

– длина ключа должна быть 1024 или 2048 бит;

– абонент, подающий заявку на получение сертификата, должен самостоятельно сгенерировать ключевую пару;

– запросы на выдачу сертификата сервера или службы должны быть представлены посредством электронной почты, подписанные личным ключом, который соответствует сертификату физического лица, выпущенному УЦ;

– запросы на получение сертификата с экспонентой равной 3 будут отклонены.

Если запрос на выдачу сертификата не удовлетворяет хотя бы одному из вышеупомянутых требований, он будет отклонен и абоненту будет отослано электронное уведомление с адреса электронной почты, указанному в пункте 1.5.2.

4.2.3 Срок обработки заявки на выдачу сертификата

Запрос на выдачу сертификата обрабатывается в течение 5 рабочих дней после того, как были получены электронный запрос на выдачу сертификата и распечатанный запрос с данными абонента.

При отсутствии или электронного или распечатанного запроса по истечении двух недель запрос может быть отклонен.

4.3 Выдача сертификата

4.3.1 Действия удостоверяющего центра во время выдачи сертификата

Принятый запрос на выдачу сертификата с помощью сменного носителя передается на выделенную ЭВМ УЦ. Сертификат издается и отсылается абоненту и оператору соответствующего РЦ, информируя таким образом о факте выдачи сертификата.

4.3.2 Уведомление абонента СЦ об издании сертификата

Об издании сертификата абонента уведомляют по электронной почте, указанной в запросе.

4.4 Прием сертификата

Считается, что сертификат принят абонентом, если тот явным образом не заявил обратное посредством доверенного канала связи с УЦ.

4.4.1 Процедура приема сертификата

Не определены.

4.4.2 Публикация сертификата удостоверяющим центром

Не определена.

4.4.3 Уведомление других объектов о выдаче сертификата

Соответствующий РЦ, который взаимодействовал с абонентом, будет уведомлен о выдаче сертификата.

4.5 Использование пары ключей и сертификата

4.5.1 Использование пары ключей и сертификата абонентом

Использование личного ключа абонента наряду с использованием выданных УЦ сертификатов определено в пункте 1.4.1. Личный ключ не должен быть раскрыт или использован другими абонентами, за исключением абонента для которого был издан сертификат.

4.5.2 Использование сертификата и открытого ключа доверяющей стороной

Доверяющие стороны используют открытые ключи и сертификаты для:

– шифрования электронной почты и проверки подписи (только сертификаты физических лиц);

– аутентификации сервера (только сертификаты серверов) и шифрования данных при передаче;

– аутентификации абонента. Доверяющие стороны должны загружать СОС не менее одного раза в день и учитывать отозванные сертификаты при проверке достоверности сертификатов.

4.6 Обновление сертификата

4.6.1 Основания обновления сертификата

УЦ не обновляет сертификаты абонентов. Абоненты должны следовать процедуре замены пары ключей, как описано в пункте 4.7.

4.6.2 Кто может запросить обновление сертификата

См. пункт 4.6.1.

4.6.3 Обработка запросов на обновление сертификата

См. пункт 4.6.1.

4.6.4 Уведомление пользователя о выдаче обновленного сертификата

См. пункт 4.6.1.

4.6.5 Процедура приема обновленного сертификата

См. пункт 4.6.1.

4.6.6 Публикация обновленного сертификата УЦ

См. пункт 4.6.1.

4.6.7 Уведомление УЦ о выдаче сертификата другим объектам

См. пункт 4.6.1.

4.7 Замена ключей в сертификате

4.7.1 Основания для замены ключей в сертификате

Ключи в сертификате могут быть заменены, если до истечения срока действия сертификата осталось менее чем 31 день.

4.7.2 Кто может запросить новый открытый ключ

См. пункт 4.1.1, при основаниях, описанных в пункте 4.7.1.

4.7.3 Обработка запросов на замену ключей в сертификате

Предупреждения об истечении срока действия сертификатов будут отосланы абонентам прежде, чем наступит время плановой замены ключей в сертификате. Замена ключей до истечения срока действия сертификата может быть выполнена при предоставлении запроса, подписанного личным ключом, который соответствует действительному сертификату физического лица. При замене ключей в сертификате по истечению срока действия используется такая же процедура аутентификации как при получении первоначального сертификата. Согласно пункту 3.3.1 каждые три года абонент должен пройти процедуру аналогичную процедуре изначальной проверки подлинности. В случае запроса на выдачу нового сертификата в связи с отзывом сертификата, абонент также должен следовать процедуре изначальной проверки подлинности.

4.7.4 Уведомление абонента о выдаче сертификата с замененными ключами

См. пункт 4.3.2

4.7.5 Процедура приема сертификата с замененными ключами

См. пункт 4.4.1

4.7.6 Публикация сертификата УЦ с замененными ключами

См. пункт 4.4.2

4.7.7 Уведомление УЦ о выдаче сертификата другим объектам

См. пункт 4.4.3

4.8 Изменение сертификата

4.8.1 Основания изменения сертификата

УЦ не изменяет сертификаты.

4.8.2 Кто может запросить изменение сертификата

См. пункт 4.8.1.

4.8.3 Обработка запросов на изменение сертификата

См. пункт 4.8.1.

4.8.4 Уведомление абонента о выдаче измененного сертификата

См. пункт 4.8.1.

4.8.5 Процедура приема измененного сертификата

См. пункт 4.8.1.

4.8.6 Публикация измененного сертификата УЦ

См. пункт 4.8.1.

4.8.7 Уведомление УЦ о выдаче измененного сертификата другим объектам

См. пункт 4.8.1.

4.9 Отзыв и приостановка действия сертификата

4.9.1 Основания отзыва

Сертификат будет отозван в случае:

– УЦ проинформирован, что абонент больше не является участником грид–проекта;

– личный ключ абонента утерян или подозревается в компрометации;

– информация в сертификате абонента неверна или неточна, или подозревается в неверности или неточности;

– абонент нарушает свои обязательства;

– абонент не нуждается больше в сертификате;

– получено основание для отзыва сертификата, представленное от другого субъекта.

4.9.2 Кто может запросить отзыв

УЦ, РЦ, абонент сертификата или любой другой субъект, имеющий основания для отзыва сертификата, может запросить отзыв.

4.9.3 Процедура запроса на отзыв

Абонент, запрашивающий отзыв сертификата, аутентифицируется, подписывая запрос на отзыв личным ключом, соответствующим действительному сертификату физического лица. Либо аутентификация будет выполнена, как описано в пункте 3.2.3. Также, если УЦ или РЦ могут лично проверить, что основание для отзыва, предоставленное третьим лицом, является достаточно веским, то оно будет принято как действительный запрос.

4.9.4 Период отсрочки запроса на отзыв

Максимальное время для принятия решения об отзыве и непосредственно отзыва составляет один день (исключая выходные и праздничные дни Республики Беларусь). Тем не менее, запросы на отзыв УЦ обрабатывает как приоритетные.

4.9.5 Время обработки запроса на отзыв для УЦ

УЦ обработает все запросы на отзыв сертификатов в течение одного дня после получения (исключая выходные и праздничные дни республики Беларусь).

4.9.6 Требования к проверке статуса отзыва сертификата для доверяющей стороны

Доверяющие стороны должны загружать СОС с репозитория [пункт 2.2] не менее одного раза в день и использовать его при проверке действительности сертификатов.

4.9.7 Частота выпуска СОС

СОС обновляются, переиздаются и публикуются в течение одного часа после каждого подтвержденного отзыва сертификата, но по крайней мере каждые 30 дней и не менее чем за 7 дней до установленного времени обновления последнего выпущенного СОС.

4.9.8 Максимальное время задержки публикации СОС

Не определено.

4.9.9 Сервис онлайновой проверки статуса сертификата

В настоящее время УЦ не предлагает сервиса проверки статуса сертификата.

4.9.10 Требования к проверке статуса отзыва в режиме онлайн

См. пункт 4.9.9.

4.9.11 Другие формы доступных уведомлений об отзыве

Не определены.

4.9.12 Особые требования при замене скомпрометированной пары ключей

Не определены.

4.9.13 Основания приостановки действия сертификата

УЦ не приостанавливает сертификаты.

4.9.14 Кто может запросить приостановку действия сертификата

См. пункт 4.9.13.

4.9.15 Процедура запроса на приостановку действия сертификата

См. пункт 4.9.13.

4.9.16 Пределы периода приостановки действия сертификата

См. пункт 4.9.13.

4.10 Услуги информирования о статусе сертификата

4.10.1 Эксплуатационные характеристики

УЦ использует онлайновый репозиторий, который содержит все СОС, которые были изданы. При отзыве сертификата СОС в репозитории сразу должен быть изменен.

4.10.2 Доступность сервера

Онлайновый репозиторий поддерживается на основании принципа максимальных усилий и доступен круглосуточно.

4.10.3 Дополнительные особенности

Не определены.

4.11 Окончание подписки

Не определено.

4.12 Депонирование и восстановление ключа

4.12.1 Политика и практика депонирования и восстановления ключа

УЦ не принимает ключи на депонирование или восстановление, а также не предоставляет ключи на депонирование.

4.12.2 Политика и практика инкапсуляции и восстановления ключей

Не определены.

5 ФИЗИЧЕСКИЕ, ОРГАНИЗАЦИОННЫЕ И ЭКСПЛУАТАЦИОННЫЕ МЕРЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

5.1 Физические меры обеспечения безопасности

5.1.1 Размещение и местоположение УЦ

УЦ находится в защищенной комнате, расположенной в ОИПИ НАН Беларуси. Как минимум один сотрудник ОИПИ НАН Беларуси круглосуточно присутствует в здании.

5.1.2 Физический доступ

Физический доступ к УЦ ограничен только уполномоченным персоналом.

5.1.3 Электроснабжение и кондиционирование воздуха

В помещении, содержащем оборудование УЦ, находится кондиционер.

5.1.4 Подверженность водному воздействию

В связи с местоположением УЦ наводнение невозможно. Помещение, в котором безопасно функционирует УЦ, достаточно водонепроницаемо; риск водного воздействия минимален.

5.1.5 Противопожарные меры безопасности и защита

Здание, в котором находится оборудование УЦ, должно соответствовать законодательству РБ по предотвращению и защите от пожара.

5.1.6 Хранение носителей информации

Резервные копии должны быть сохранены на съемных носителях.

Ключ УЦ хранится на нескольких съемных носителях.

Резервные копии информации УЦ хранятся на USB запоминающих устройствах и CD-ROM.

5.1.7 Утилизация отходов

Сменные носители информации физически уничтожаются перед утилизацией.

5.1.8 Резервное копирование вне сети

Не определено.

5.2 Процедурные меры обеспечения безопасности

5.2.1 Доверенные роли

Не определены.

5.2.2 Количество сотрудников, необходимое для обеспечения функционирования УЦ

Не определено.

5.2.3 Идентификация и аутентификация каждой роли

Не определены.

5.2.4 Роли, требующие разделения режимов работы

Не определены.

5.3 Управление персоналом

5.3.1 Требования к квалификации, стажу работы и допуску

Персонал СЦ набирается из числа сотрудников центра грид-технологий ОИПИ НАН Беларуси. Они хорошо осведомлены о значимости ИОК, технически и профессионально компетентны.

Персонал РЦ набирается из числа сотрудников соответствующих организаций.

5.3.2 Процедуры проверки личной биографии

Не определены.

5.3.3 Требования к обучению

Операторам СЦ и РЦ предоставляется обучение.

5.3.4 Частота и требования к переподготовке

Не определены.

5.3.5 Частота и последовательность ротации должностей

Не определены.

5.3.6 Санкции за несанкционированные действия

Не определены.

5.3.7 Требования к персоналу подрядчиков

Не определены.

5.3.8 Документация, предоставляемая персоналу

Документация относительно всех эксплуатационных процедур УЦ предоставляется персоналу в течение периода начального обучения.

5.4 Процедуры регистрации проверок

5.4.1 Типы регистрируемых событий

СЦ должен регистрировать следующие события:
– запросы на выдачу сертификата;
– изданные сертификаты;
– запросы на отзыв;
– выпущенные СОС;
– вход /выход /перезагрузка системы.
Каждый РЦ должен регистрировать следующее:
– каждый принятый запрос, как он принят;
– каждый отклоненный запрос, почему он отклонен;
– каждый принятый запрос на отзыв, причину отзыва;
– каждый отклоненный запрос на отзыв, причину отзыва и причину отклонения запроса.

5.4.2 Частота обработки журнала проверок

Журналы проверок обрабатываются не менее одного раза в квартал.

5.4.3 Срок хранения журнала проверок

Журналы проверок хранятся минимум 3 года.

5.4.4 Защита журнала проверок

Только уполномоченному персоналу УЦ разрешено просматривать и обрабатывать журналы проверок. Журналы проверок хранятся в сейфе в помещении с ограниченным доступом.

5.4.5 Процедуры резервного копирования журнала проверок

Журналы проверок копируются на съемные носители и хранятся в сейфе в помещении с ограниченным доступом.

5.4.6 Система сбора данных проверок (внутренняя и внешняя)

Система сбора данных проверок управляется изнутри.

5.4.7 Уведомление абонента, активировавшего событие

Не предусмотрено.

5.4.8 Оценки уязвимости

Не предусмотрены.

5.5 Архивирование записей

5.5.1 Типы регистрируемых событий

УЦ регистрирует и архивирует следующие данные и файлы:
– запросы на выдачу сертификата;
– изданные сертификаты;
– запросы на отзыв;
– выпущенные СОС;
– все электронные письма РЦ и СЦ;
– вход /выход /перезагрузку системы;
– личные копии идентификационных данных, собранные РЦ.

Зарегистрированные СЦ события записываются на бумаге, архивируются и хранятся в сейфе в помещении СЦ.

Каждый РЦ должен архивировать журнал регистрации следующих событий:
– каждый принятый запрос, как он был принят;
– каждый отклоненный запрос, почему он отклонен;
– каждый принятый запрос на отзыв, причину отзыва;
– каждый отклоненный запрос на отзыв, причину отзыва и причину отклонения запроса.

Зарегистрированные РЦ события регистрируются в электронном виде и хранятся в помещении РЦ с ограниченным доступом.

5.5.2 Срок хранения архива

Личная информация, используемая для получения сертификата абонента с конкретным отличительным именем DN, должна храниться, пока абонент имеет действительный сертификат с этим DN, включая обновление сертификата или замену ключей в сертификате, и как минимум в течение трех лет по окончанию срока действия или отзыва сертификата абонента.

Данные, используемые для получения сертификата сервера или службы, должны храниться, пока абонент является ответственным администратором сервера, для которого был получен сертификат, и как минимум в течение трех лет по окончанию срока действия или отзыва сертификата абонента, или при передаче прав администратора.

5.5.3 Защита архива

Архив хранится в сейфе в помещении с ограниченным доступом.

5.5.4 Процедуры резервного копирования архива

Все данные и файлы копируются на автономные носители.

5.5.5 Требования к проставлению временных отметок записей

Не предъявляются.

5.5.6 Система сбора архивных данных (внутренняя или внешняя)

Система сбора архивных данных управляется изнутри.

5.5.7 Процедуры получения и проверки архивной информации

Не определены.

5.6 Смена ключей

Личный ключ СЦ периодически заменяется; после замены будет действителен новый ключ для подписания новых сертификатов или новых СОС. Период перекрытия прежнего и нового ключа должен быть не менее чем максимальный период действия сертификатов как определено в пункте 6.3.2. Прежний, но все еще действительный сертификат должен быть доступен для проверки подписей и соответствующий этому сертификату личный ключ должен использоваться для подписания СОС, пока все подписанные сертификаты не будут отозваны или их срок действия не истечет.

5.7 Восстановление при компрометациях и сбоях

5.7.1 Процедура восстановления в случае компрометации

Если личный ключ СЦ скомпрометирован (или подозревается в компрометации), СЦ:

– сообщит EUGridPMA;

– сообщит РЦ, абонентам и доверяющим сторонам, о которых осведомлен УЦ;

– закончит выдачу и распространение сертификатов и СОС;

– сгенерирует новый сертификат СЦ с новой парой ключей, который будет вскоре доступен на сайте.

Если личный ключ оператора РЦ скомпрометирован или подозревается в компрометации, оператор РЦ или администратор должен сообщить СЦ и запросить отзыв сертификата оператора РЦ.

5.7.2 Повреждение вычислительных ресурсов, программного обеспечения и/или данных

Не определено.

5.7.3 Процедуры компрометации личного ключа абонента

Не определены.

5.7.4 Способность восстановления деятельности при сбоях

Не определена.

5.8 Прекращение функционирования СЦ и РЦ

Прежде, чем СЦ прекратит оказывать услуги, СЦ:

– сообщит РЦ, абонентам, и доверяющим сторонам, о которых осведомлен УЦ;

– разместит информацию о прекращении предоставления услуг на своем сайте;

– прекратит выдачу сертификатов;

– уничтожит все копии личных ключей.

Прежде, чем РЦ прекратит оказывать услуги, РЦ:

– сообщит СЦ;
– прекратит принимать запросы на выдачу сертификата;
– безопасно переместит свой архив в СЦ.

Не менее чем за 60 дней будет сделано предварительное уведомление в случае запланированного прекращения предоставления услуг СЦ или РЦ.

6 ТЕХНИЧЕСКИЕ МЕРЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

6.1 Создание и установка пары ключей

6.1.1 Создание пары ключей

Ключи для корневого сертификата УЦ создаются на выделенной ЭВМ, изолированной от сети. Программное обеспечение, используемое для создания ключей – EJBCA и/или OpenSSL. Каждый абонент должен создать собственную пару ключей.

6.1.2 Предоставление личного ключа абоненту

Поскольку каждый абонент создает свою собственную пару ключей, УЦ не имеет доступа к личным ключам абонентов.

6.1.3 Предоставление открытого ключа издателю сертификата

Определено в пункте 4.1.2.

6.1.4 Предоставление открытого ключа УЦ доверяющим сторонам

Корневой сертификат УЦ доступен на сайте, указанном в пункте 2.1.

6.1.5 Размеры ключей

Для сертификата физического лица или сервера размер ключа – 1024 бита или 2048 битов. Размер ключа УЦ – 2048 битов.

6.1.6 Параметры создания открытого ключа

Не определены.

6.1.7 Цели использования ключей (согласно полю Key Usage формата X.509 v3)

Ключи могут использоваться для аутентификации, шифрования данных, обеспечения целостности сообщения и создания защищенных сессий.

Личный ключ УЦ используется только для подписания СОС и новых сертификатов.

6.2 Защита личного ключа и средства управления конструкцией криптографического модуля

6.2.1 Средства управления конструкцией и стандарты криптографического модуля

Не определены.

6.2.2 Контроль личного ключа (n из m) несколькими людьми

Не определено.

6.2.3 Депонирование личного ключа

УЦ не осуществляет депонирование личного ключа.

6.2.4 Резервное копирование личного ключа

Резервная копия личного ключа УЦ хранится в зашифрованном виде в нескольких копиях на USB запоминающих устройствах и CD-ROM. Пароль для личного ключа хранится отдельно на бумаге, доступ к которому контролируется. Только уполномоченный персонал УЦ имеет доступ к резервным копиям.

6.2.5 Помещение в архив личного ключа

УЦ не помещает в архив личные ключи.

6.2.6 Ввод в криптографический модуль или извлечение из него личного ключа

УЦ не использует криптографический модуль.

6.2.7 Хранение личного ключа в криптографическом модуле

См. пункт 6.2.6.

6.2.8 Способ активации личного ключа

Личный ключ УЦ активируется при использовании пароля. См. пункт 6.4.1

6.2.9 Метод деактивации личного ключа

Не определен.

6.2.10 Способ уничтожения личного ключа

После прекращения функционирования УЦ все носители, которые содержат личный ключ УЦ, будут уничтожены, согласно наилучшим практическим рекомендациям.

6.2.11 Оценка криптографического модуля

Не определена.

6.3 Другие аспекты управления парой ключей

Не определены.

6.3.1 Помещение в архив открытого ключа

Открытые ключи всех выданных сертификатов помещаются в архив.

6.3.2 Сроки действия сертификатов и сроки использования пары ключей

Корневой сертификат УЦ имеет срок действия двадцать лет. Максимальный срок действия сертификата абонента – один год и один месяц.

6.4 Данные активации

6.4.1 Создание и установка данных активации

УЦ не создает данные активации для абонентов. Абонент создает сложный пароль, чтобы использовать его в качестве данных активации своего личного ключа.

Личный ключ УЦ защищен паролем длиной не менее 15 символов и известен только уполномоченному персоналу УЦ.

6.4.2 Защита данных активации

Абонент ответственен за защиту данных активации личного ключа.

УЦ использует пароль, чтобы активировать личный ключ, который известен только администратору УЦ и операторам УЦ. Копия пароля записана на бумаге, запечатана в конверте и хранится в сейфе. Доступ к сейфу имеет только администратор УЦ и

операторы УЦ. При изменении служебного персонала УЦ данные активации должны быть изменены. Прежние данные активации уничтожаются согласно наилучшим практическим рекомендациям.

6.4.3 Другие аспекты данных активации

Не определены.

6.5 Средства управления компьютерной безопасностью

6.5.1 Специфические технические требования к компьютерной безопасности

Компьютеры, работающие в УЦ, удовлетворяют следующим требованиям:

– ЭВМ для подписи сертификатов изолирована для доступа;

– операционные системы поддерживаются на высоком уровне защиты, при регулярном применении всех рекомендованных и соответствующих патчей защиты;

– мониторинг осуществляется для обнаружения несанкционированных программных изменений;

– количество запущенных системных служб сведено к минимуму.

6.5.2 Оценка компьютерной безопасности

Не определена.

6.6 Технические средства управления жизненным циклом

6.6.1 Контроль разработки системы

Не определен.

6.6.2 Средства управления безопасностью

Не определены.

6.6.3 Управление безопасностью жизненного цикла

Не определено.

6.7 Средства управления сетевой безопасностью

Сертификаты изготавливаются на ЭВМ, изолированной от сети. Безопасность других машин обеспечивается межсетевыми экранами.

6.8 Проставление временных отметок

Не применимо.

7 Шаблоны сертификатов, COC и OCSP

7.1 Описание сертификата

7.1.1 Номер версии

УЦ поддерживает и использует сертификат формата X.509 версии 3.

7.1.2 Расширения сертификата

УЦ поддерживает и использует следующие расширения сертификата формата X.509 версии 3. Расширения для корневого сертификата УЦ:

– X509v3 Основные Ограничения Basic Constraints: critical, CA:TRUE

– X509v3 Назначение ключа Key Usage: critical, CRL Sign, Key Cert Sign

– X509v3 Идентификатор ключа абонента Subject Key Identifier: <CA key ID>

– X509v3 Идентификатор ключа издателя Authority Key Identifier: keyid: < CA key ID >

Расширения для сертификата физического лица:

– X509v3 Основные Ограничения Basic Constraints: critical, CA:FALSE

– X509v3 Назначение ключа Key Usage: critical, Digital Signature, Key Encipherment, Data Encipherment, Key Agreement

– X509v3 Расширенная область назначения ключа Extended Key Usage: TLS Web Client Authentication, E-mail Protection

– X509v3 Идентификатор ключа физического лица Subject Key Identifier: <subject key ID>

– X509v3 Идентификатор ключа издателя Authority Key Identifier: keyid: <CA key ID>

– X509v3 Альтернативное имя физического лица Subject Alternative Name: email: <user's email address>

– X509v3 Политика сертификатов Certificate Policies:

Policy: 1.2.840.113612.5.2.2.1

Policy: <OID of the effective CP/CPS>

– X509v3 Пункт распространения списка отозванных сертификатов (COC) CRL Distribution Points: URI: http: // ca.grid.by/bygca-crl.crl

Расширения сертификатов серверов и служб:

– X509v3 Основные Ограничения Basic Constraints: critical, CA: FALSE

– X509v3 Назначение ключа Key Usage: critical, Digital Signature, Key Encipherment, Data Encipherment, Key Agreement

– X509v3 Расширенная область назначения ключа Extended Key Usage: TLS Web Server Authentication, TLS Web Client Authentication

– X509v3 Идентификатор ключа абонента Subject Key Identifier: <subject key ID>

– X509v3 Идентификатор ключа издателя Authority Key Identifier: keyid: <CA key ID>

– X509v3 Альтернативное имя абонента Subject Alternative Name: DNS: FDQN

– X509v3 Политика сертификатов: Certificates Policies:

Policy: 1.2.840.113612.5.2.2.1

Policy: <идентификатор объекта в соответствии с которым выдан сертификат OID of the effective CP/CPS>

– X509v3 Пункт распространения списка отозванных сертификатов (COC) CRL Distribution Points: URI: http: // ca.grid.by/bygca-crl.crl

7.1.3 Идентификаторы алгоритма

Для дайджеста сообщения, который обеспечивает целостность сертификата, не должны использоваться известные слабые криптографические подписи или хеш-функции, такие как MD5. Должна использоваться самая безопасная хеш-функция, которая поддерживается всеми потенциальными клиентами УЦ, по крайней мере, SHA-1 или лучше.

7.1.4 Типы имен

Издатель: DC=by, DC=grid, O=uiip.bas-net.by, CN= Belarusian Grid Certification Authority

Физическое лицо: DC=by, DC=grid, O=domain.by, CN=Firstname Lastname

Сервер: DC=by, DC=grid, O=domain.by, CN=host/fully.qualified.domain.name

Служба: DC=by, DC=grid, O=domain.by, CN=servicename/fully.qualified.domain.name

Структура поля атрибута CN для сертификата физического лица или сервера/службы описана в разделе 3.1.

CN-часть отличительного имени физического лица может содержать только английские символы алфавита, цифры и специальные символы: левая круглая скобка (‘(’), правая круглая скобка (‘)’), пробел (‘ ‘)и дефис (‘-‘). CN-часть отличительного имени сервера или службы может содержать только английские символы алфавита, цифры и следующие специальные символы: точка (‘.‘) и дефис (‘-‘). Кроме того, в имени сертификата грид-сервера и сертификата грид-службы может использоваться символ ‘/’. Максимальная длина CN – 64 символа для всех типов сертификатов.

7.1.5 Ограничения в написании имени

См. пункт 3.1.2.

7.1.6 Идентификатор объекта политики сертификата

Сертификаты абонента в расширении Certificates Policies содержат ИО профиля аутентификации УЦ стандарта X.509 с безопасной инфраструктурой и ИО документа, согласно которому они были выпущены.

7.1.7 Использование расширения Policy Constraints (политика ограничений)

Не определено.

7.1.8 Синтаксис и семантика квалификаторов политики

Не определены.

7.1.9 Обработка семантики критического расширения Certificates Policy (политика сертификатов)

Не определена.

7.2 Описание COC

7.2.1 Номер версии

Все COC издаются в формате X.509 версии 2.

7.2.2 COC и расширения COC

УЦ поддерживает и использует расширения COC:

– идентификатор ключа издателя authorityKeyIdentifier: уникальный идентификатор ключа издателя согласно RFC 3280;

– порядковый номер COC cRLNumber: монотонно увеличивающийся порядковый номер для каждого выпущенного COC согласно RFC 3280;

– код причины отзыва Reason Code CRL: некритическое расширение, содержащее код причины отзыва как определено в пункте 5.3.1 RFC3280.

7.3 Описание OCSP

7.3.1 Номер версии

Не определен.

7.3.2 Расширения OCSP

Не определены.

8 Проверка соответствия и другие оценки

8.1 Частота или основания проведения оценки

Члены EUGridPMA должны иметь возможность проводить аудит УЦ, чтобы проверить соответствие функционирования УЦ правилам и процедурам, указанным в данном документе. Любые затраты, связанные с такой проверкой должны быть оплачены запрашивающей стороной. Служебный персонал УЦ подвергается аудиту не менее одного раза в год.

8.2 Идентификация/квалификации эксперта

Не определена.

8.3 Отношение эксперта к оцениваемому объекту

Не определено.

8.4 Темы, затрагиваемые при проведении оценки

Не определены.

8.5 Действия, предпринимаемые в результате несоответствия функционирования УЦ данному документу

При выявлении нарушений в функционировании УЦ разработает и опубликует календарный план действий по устранению выявленных нарушений. Если выявленные нарушения привели к выдаче сертификатов, нарушающих безопасность ИОК, эти сертификаты будут немедленно отозваны.

В случае выявления нарушений в функционировании УЦ сообщит о действиях, которые необходимо предпринять для восстановления надлежащего функционирования. Если в процессе изготовления сертификатов УЦ функционировал с нарушениями, выпущенные в это время сертификаты должны быть отозваны.

8.6 Сообщение о результатах

Не определено.

9 Другие коммерческие и юридические вопросы

9.1 Пошлины

9.1.1 Пошлины за выдачу или обновление сертификата

Пошлины не взимаются.

9.1.2 Пошлины за доступ к сертификату

См. пункт 9.1.1.

9.1.3 Пошлины за доступ к информации статуса сертификата

См. пункт 9.1.1.

9.1.4 Пошлины за другие услуги

См. пункт 9.1.1.

9.1.5 Политика возмещения расходов

Пошлины не взимаются и политика возмещения расходов не определена.

9.2 Финансовая ответственность

УЦ не несет финансовой ответственности за прямые и (или) косвенные убытки, связанные с его функционированием.

9.2.1 Общая сумма рисков по договору страхования

Не определены.

9.2.2 Другие активы

Не определены.

9.2.3 Сфера действия страхования и гарантии для конечных объектов

Не определены.

9.3 Конфиденциальность коммерческой информации

9.3.1 Пределы конфиденциальной информации

Не определены.

9.3.2 Информация вне пределов конфиденциальной информации

Не определена.

9.3.3 Обязательства по защите конфиденциальной информации

Не определены.

9.4 Конфиденциальность личной информации

УЦ получает личную информацию об абонентах в соответствии с законом Республики Беларусь “Об информации, информатизации и защите информации” (№ 455-З). Абонент подтверждает, что УЦ вправе использовать и хранить такие данные.

9.4.1 План по обеспечению конфиденциальности

Не определен.

9.4.2 Информация, рассматриваемая как конфиденциальная

УЦ собирает копии предоставленных идентификационных документов, которые считаются личными и конфиденциальными.

9.4.3 Информация не являющаяся конфиденциальной

УЦ собирает следующую информацию, которая не считается конфиденциальной:
– адрес электронной почты абонента;
– ФИО абонента;
– название организации абонента;
– сертификат абонента.

Статистика относительно выдачи и отзыва сертификатов не содержит никакой личной информации и не считается конфиденциальной.

9.4.4 Обязательства по защите конфиденциальной информации

УЦ несет ответственность за защиту конфиденциальной информации, определенную в пункте 9.4.2. Копии идентификационных документов хранятся в сейфе УЦ и используются только во время аудита и для обеспечения требований к отличительным именам. Данные копий документов не используются для других целей.

9.4.5 Предупреждение об использовании и разрешение на использование конфиденциальной информации

Не определены.

9.4.6 Разглашение информации в случаях, установленных законодательством

Деятельность УЦ регулируется законодательством Республики Беларусь. УЦ обязуется использовать конфиденциальную и личную информацию для установления полномочий в соответствии с установленным порядком.

9.4.7 Другие основания разглашения информации

Не определены.

9.5 Права на интеллектуальную собственность

При составлении настоящего документа использовались следующие материалы:
– RFC 3647;
– IGTF-AP-classic;
– UK e-Science CA CP/CPS;
– Macedonian Academic and Research Grid Initiative CA CP/CPS;
– Baltic Grid CA CP/CPS;
– CA for Latvian Grid CP/CPS;
– Grid Certificate Profile;
– DutchGrid and NIKHEF CA CP/CPS.

9.6 Обязанности

9.6.1 Обязанности СЦ

УЦ ответственен только за изготовление и управление сертификатами в соответствии с данным документом. УЦ:

– обрабатывает запросы на выдачу сертификатов и издает новые сертификаты:

- подтверждает запросы на выдачу сертификатов от абонентов, запрашивающих сертификаты согласно процедурам, описанным в данном документе;
- издает сертификаты на основе запросов от аутентифицированных абонентов;
- посылает уведомление о выпущенных сертификатах запрашивающим абонентам и соответствующему РЦ;

– обрабатывает запросы на отзыв сертификатов и отзывает сертификаты:

- подтверждает запросы на отзыв сертификатов от абонентов, запрашивающих отзывы сертификатов согласно процедурам, описанным в данном документе;
- выпускает СОС;
- публикует информацию об отозванных сертификатах;
- публикует корневой сертификат УЦ в репозитории EUGridPMA.

9.6.2 Обязанности РЦ

Каждый РЦ:

– принимает условия и следует процедурам, описанным в данном документе;

– обрабатывает запросы на выдачу сертификата:

- проверяет, что информация, предоставленная в запросе на выдачу сертификата, и адрес электронной почты, предоставленный абонентом, являются правильными;

- аутентифицирует личность абонента, запрашивающего сертификат, и отклоняет запросы, если абонент не аутентифицирован;
- проверяет, что абонент ознакомлен и согласен с обязанности абонента, как определено в пункте 9.6.3;
- подтверждает и подписывает запросы на выдачу сертификата;
- уведомляет УЦ о том, что запрос на выдачу сертификата аутентифицирован и подтвержден;

– обрабатывает запросы на отзыв сертификата:

- проверяет, что информация, предоставленная в запросе на отзыв сертификата, правильна;
- подтверждает и подписывает запросы на отзыв;
- уведомляет УЦ, что запрос на отзыв аутентифицирован и подтвержден.

9.6.3 Обязанности абонента

Запрашивая запрос на выдачу сертификата, абоненты соглашаются:

– принять условия и следовать процедурам, описанным в данном документе;

– предоставить достоверную и точную информацию УЦ;

– использовать сертификат в соответствии с настоящим документом и действующим законодательством;

– во время процедуры аутентификации, описанной в данном документе, принять ограничения ответственности УЦ, в соответствии с пунктом 9.8;

– во время процедуры аутентификации, описанной в данном документе, принять обязательства, касающиеся конфиденциальности информации, пункта 9.3;

– сгенерировать пару ключей, используя надежный метод;

– использовать сложный пароль длиной не менее 12 символов для защиты личного ключа;

– гарантировать, что личный ключ сертификата сервера или службы доступен только администратору, ответственному за данный сервер или службу;

– принимать разумные меры для предотвращения потери, раскрытия или несанкционированного использования личного ключа;

– немедленно уведомить УЦ в случае, если личный ключ потерян или скомпрометирован.

9.6.4 Обязанности доверяющих сторон

При использовании сертификата, выданного УЦ, доверяющие стороны соглашаются:

– принять условия и следовать процедурам, описанным в данном документе;

– проверить информацию на отзыв сертификата перед использованием сертификата;

– использовать сертификат в соответствии с настоящим документом и действующим законодательством.

9.6.5 Обязанности других участников

Не определены.

9.7 Отзыв гарантий

Не определены.

9.8 Ограничения ответственности

9.8.1. УЦ гарантирует управление идентификацией запросов на выдачу сертификата согласно процедурам, описанным в данном документе.

9.8.2. УЦ гарантирует управление идентификацией запросов на отзыв согласно процедурам, описанным в данном документе.

9.8.3. Работа УЦ обеспечивается на основании принципа максимальных усилий.

9.8.4. УЦ не несет ответственности в случае нарушения абонентом и /или другими участниками требований настоящего документа.

9.8.5. УЦ не несет ответственности за неисполнение своих обязательств по независящим от него обстоятельствам.

9.9 Компенсации

Не определены.

9.10 Срок действия и прекращение действия

9.10.1 Срок действия

Не определен.

9.10.2 Прекращение действия

Не определено.

9.10.3 Последствия прекращения действия и положения, остающиеся действительными

Не определены.

9.11 Индивидуальные уведомления и сообщения участникам

Не определены.

9.12 Поправки

9.12.1 Внесение поправок

Абонентам не сообщат заранее о внесение поправок в настоящий документ. О поправках сообщают EUGridPMA и утверждают прежде, чем новый документ будет опубликован на сайте, как определено в пункте 2.1. Поправки также публикуются на сайте.

9.12.2 Механизм и период уведомления

Не определены.

9.12.3 Основания, при которых ИО должен быть изменен

ИО должен изменяться всякий раз, когда версия документа обновляется.

9.13 Условия разрешения споров

Разрешение юридических споров, являющихся результатом функционирования УЦ, осуществляется в соответствии с законодательством РБ.

9.14 Действующее законодательство

Юридическая сила, толкование данного документа осуществляется в соответствии с действующим законодательством РБ.

9.15 Соответствие действующему законодательству

Не определено.

9.16 Различные положения

9.16.1 Полнота соглашения
Не определена.

9.16.2 Передача прав
Не определена.

9.16.3 Независимость разделов документов
Не определена.

9.16.4 Взыскание (юридические издержки и освобождение от обязательств)
Не определено.

9.16.5 Форс - мажор
Не определен.

9.17 Прочие положения
Не определены.