GIS ГАЗИНФОРМ СЕРВИС

Особенности проверки действительности цепочки квалифицированных сертификатов в соответствии с требованиями руководящих документов

Ермина Екатерина
Ведущий инженер

Ermina-E@gaz-is.ru

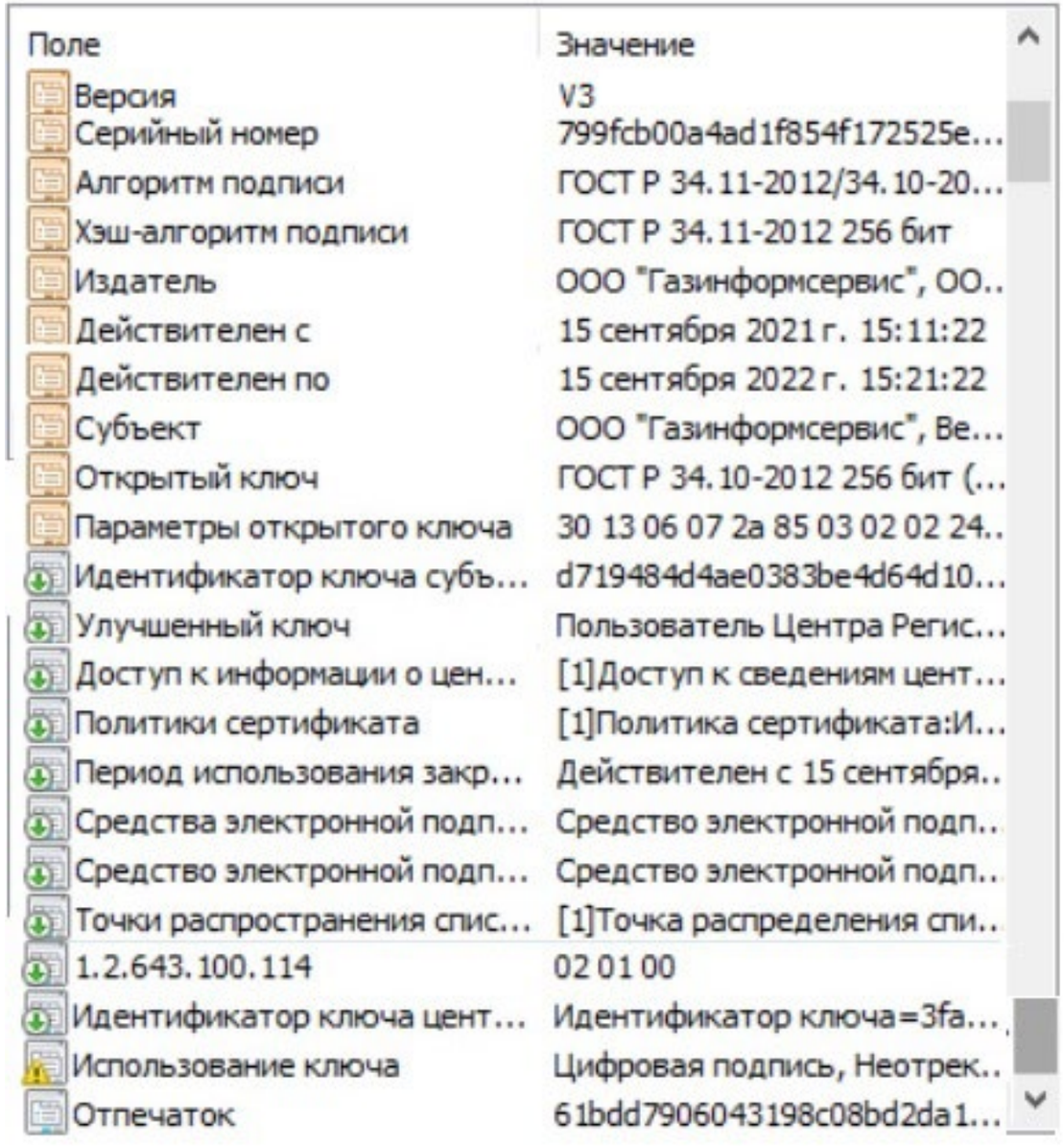
PKI Forum 2022
13-15 сентября 2022 года
www.gaz-is.ru

Содержание доклада

1. Проверка действительности цепочки квалифицированных сертификатов
2. Требования к атрибутам поля Subject, не учитывающие особенности ведения хозяйственной деятельности субъектов как РФ, так и иностранных государств
3. Существующие ограничения при проверке сертификатов в СМЭВ и возможные пути их решения
4. Особенности выдачи сертификатов службам УЦ (OCSP и TSP) и ДТС и возможные пути их решения

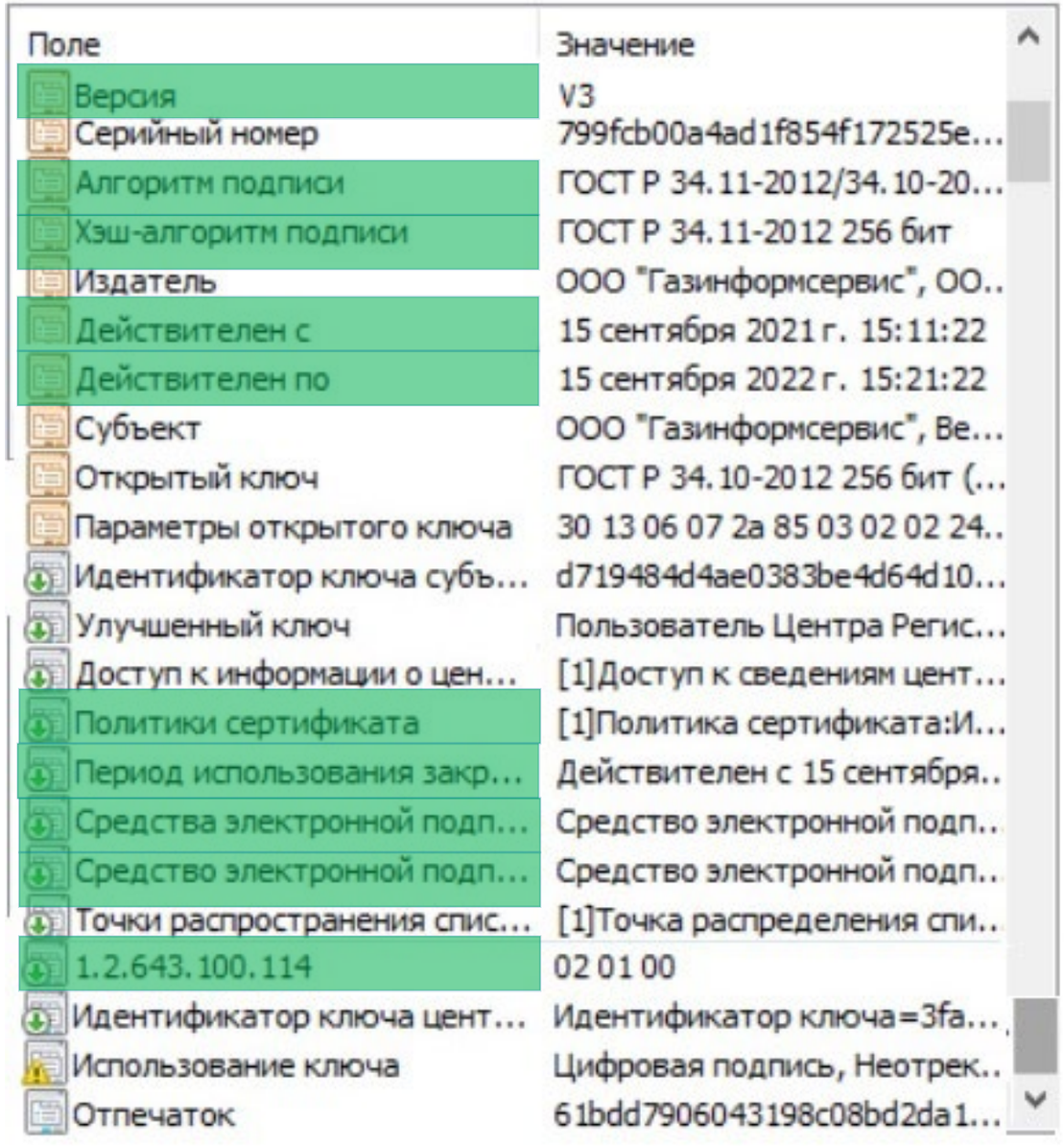
Проверка действительности цепочки квалифицированных сертификатов

Проверка действительности цепочки квалифицированных сертификатов



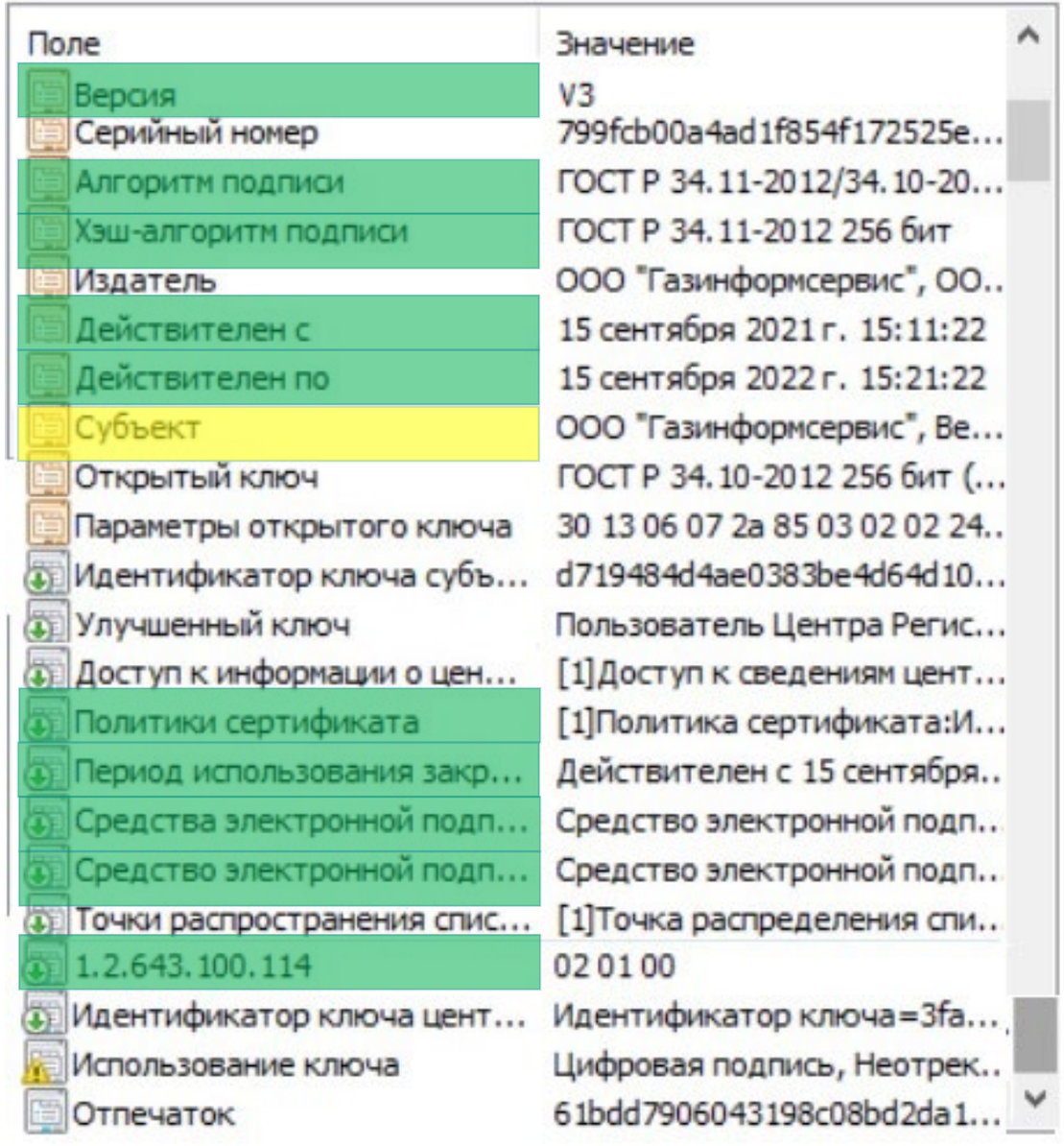
Поле	Значение
Версия	V3
Серийный номер	799fcb00a4ad1f854f172525e...
Алгоритм подписи	ГОСТ Р 34.11-2012/34.10-20...
Хэш-алгоритм подписи	ГОСТ Р 34.11-2012 256 бит
Издатель	ООО "Газинформсервис", ОО..
Действителен с	15 сентября 2021 г. 15:11:22
Действителен по	15 сентября 2022 г. 15:21:22
Субъект	ООО "Газинформсервис", Ве...
Открытый ключ	ГОСТ Р 34.10-2012 256 бит (...
Параметры открытого ключа	30 13 06 07 2a 85 03 02 02 24..
Идентификатор ключа субъ...	d719484d4ae0383be4d64d10...
Улучшенный ключ	Пользователь Центра Регис...
Доступ к информации о цен...	[1]Доступ к сведениям цент...
Политики сертификата	[1]Политика сертификата:И...
Период использования закр...	Действителен с 15 сентября..
Средства электронной подп...	Средство электронной подп..
Средство электронной подп...	Средство электронной подп..
Точки распространения спис...	[1]Точка распределения спи..
1.2.643.100.114	02 01 00
Идентификатор ключа цент...	Идентификатор ключа=3fa...
Использование ключа	Цифровая подпись, Неотрек..
Отпечаток	61bdd7906043198c08bd2da1...

Проверка действительности цепочки квалифицированных сертификатов



Поле	Значение
Версия	V3
Серийный номер	799fcb00a4ad1f854f172525e...
Алгоритм подписи	ГОСТ Р 34.11-2012/34.10-20...
Хэш-алгоритм подписи	ГОСТ Р 34.11-2012 256 бит
Издатель	ООО "Газинформсервис", ОО..
Действителен с	15 сентября 2021 г. 15:11:22
Действителен по	15 сентября 2022 г. 15:21:22
Субъект	ООО "Газинформсервис", Ве...
Открытый ключ	ГОСТ Р 34.10-2012 256 бит (...
Параметры открытого ключа	30 13 06 07 2a 85 03 02 02 24..
Идентификатор ключа субъ...	d719484d4ae0383be4d64d10...
Улучшенный ключ	Пользователь Центра Регис...
Доступ к информации о цен...	[1]Доступ к сведениям цент...
Политики сертификата	[1]Политика сертификата:И...
Период использования закр...	Действителен с 15 сентября..
Средства электронной подп...	Средство электронной подп..
Средство электронной подп...	Средство электронной подп..
Точки распространения спис...	[1]Точка распределения спи..
1.2.643.100.114	02 01 00
Идентификатор ключа цент...	Идентификатор ключа=3fa...
Использование ключа	Цифровая подпись, Неотрек..
Отпечаток	61bdd7906043198c08bd2da1...

Проверка действительности цепочки квалифицированных сертификатов



Поле	Значение
Версия	V3
Серийный номер	799fcb00a4ad1f854f172525e...
Алгоритм подписи	ГОСТ Р 34.11-2012/34.10-20...
Хэш-алгоритм подписи	ГОСТ Р 34.11-2012 256 бит
Издатель	ООО "Газинформсервис", ОО..
Действителен с	15 сентября 2021 г. 15:11:22
Действителен по	15 сентября 2022 г. 15:21:22
Субъект	ООО "Газинформсервис", Ве...
Открытый ключ	ГОСТ Р 34.10-2012 256 бит (...
Параметры открытого ключа	30 13 06 07 2a 85 03 02 02 24..
Идентификатор ключа субъ...	d719484d4ae0383be4d64d10...
Улучшенный ключ	Пользователь Центра Регис...
Доступ к информации о цен...	[1]Доступ к сведениям цент...
Политики сертификата	[1]Политика сертификата:И...
Период использования закр...	Действителен с 15 сентября..
Средства электронной подп...	Средство электронной подп..
Средство электронной подп...	Средство электронной подп..
Точки распространения спис...	[1]Точка распределения спи..
1.2.643.100.114	02 01 00
Идентификатор ключа цент...	Идентификатор ключа=3fa...
Использование ключа	Цифровая подпись, Неотрек..
Отпечаток	61bdd7906043198c08bd2da1...

Требования к атрибутам поля Subject. stateOrProvinceName, localityName, streetAddress

stateOrProvinceName (наименование штата или области)

Приказ ФСБ России № 795: «В качестве значения данного атрибута имени следует использовать текстовую строку, содержащую наименование соответствующего субъекта Российской Федерации»

Приложение N 2
к Требованиям (п. 32)

Список изменяющих документов
(в ред. Приказа ФСБ России от 29.01.2021 N 31)

ОБЩИЙ ВИД КВАЛИФИЦИРОВАННОГО СЕРТИФИКАТА
НА БУМАЖНОМ НОСИТЕЛЕ ДЛЯ ВЛАДЕЛЬЦА - ЮРИДИЧЕСКОГО ЛИЦА

```
Номер квалифицированного сертификата: <serialNumber>
Действие квалифицированного сертификата: с <notBefore>
                                          по <notAfter>

        Сведения о владельце квалифицированного сертификата

Наименование юридического лица: <commonName>
Основной государственный регистрационный номер: <OGRN>
Идентификационный номер налогоплательщика: <INNLE>
Место нахождения юридического лица: <countryName>,
<stateOrProvinceName>, <localityName>, <streetAddress>
* Уполномоченный представитель юридического лица: <title> <surname>
<givenName>
Тип идентификации при выдаче сертификата: <identificationKind>
```

Требования к атрибутам поля Subject. stateOrProvinceName, localityName, streetAddress

Приложение N 3
к Требованиям (п. 32)

Список изменяющих документов
(введено Приказом ФСБ России от 29.01.2021 N 31)

Общий вид квалифицированного сертификата
на бумажном носителе для владельца - физического лица,
являющегося индивидуальным предпринимателем

Номер квалифицированного сертификата: <serialNumber>
Действие квалифицированного сертификата: с <notBefore>
по <notAfter>

Сведения о владельце квалифицированного сертификата

Фамилия, имя, отчество: <commonName>
Страховой номер индивидуального лицевого счета: <SNILS>
Индивидуальный номер налогоплательщика: <INN>
Основной государственный регистрационный номер индивидуального предпринимателя: <OGRNIP>
Тип идентификации при выдаче сертификата: <identificationKind>

Сведения об издателе квалифицированного сертификата

Требования к атрибутам поля Subject. INN, INNLE, SNILS

Приложение N 1
к Требованиям (п. 32)

Список изменяющих документов
(в ред. Приказа ФСБ России от 29.01.2021 N 31)

ОБЩИЙ ВИД КВАЛИФИЦИРОВАННОГО СЕРТИФИКАТА
НА БУМАЖНОМ НОСИТЕЛЕ ДЛЯ ВЛАДЕЛЬЦА - ФИЗИЧЕСКОГО ЛИЦА

```
Номер квалифицированного сертификата: <serialNum
Действие квалифицированного сертификата: с <notB
                                          по <not

        Сведения о владельце квалифицированного

Фамилия, имя, отчество: <commonName>
Страховой номер индивидуального лицевого счета:
Индивидуальный номер налогоплательщика: <INN>
Тип идентификации при выдаче сертификата: <ident

        Сведения об издателе квалифицированного
```

Приложение N 2
к Требованиям (п. 32)

Список изменяющих документов
(в ред. Приказа ФСБ России от 29.01.2021 N 31)

ОБЩИЙ ВИД КВАЛИФИЦИРОВАННОГО СЕРТИФИКАТА
НА БУМАЖНОМ НОСИТЕЛЕ ДЛЯ ВЛАДЕЛЬЦА - ЮРИДИЧЕСКОГО ЛИЦА

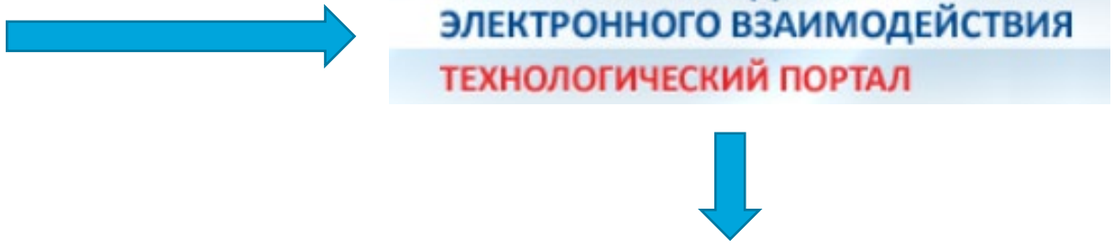
```
Номер квалифицированного сертификата: <serialNumber>
Действие квалифицированного сертификата: с <notBefore>
                                          по <notAfter>

        Сведения о владельце квалифицированного сертификата

Наименование юридического лица: <commonName>
Основной государственный регистрационный номер: <OGRN>
Идентификационный номер налогоплательщика: <INNLE>
Место нахождения юридического лица: <countryName>,
<stateOrProvinceName>, <localityName>, <streetAddress>
* Уполномоченный представитель юридического лица: <title> <surname>
<givenName>
Тип идентификации при выдаче сертификата: <identificationKind>
```

Существующие ограничения при проверке сертификатов в СМЭВ и возможные пути их решения

14.7. Анализ проводится во взаимодействии с информационными ресурсами Российской Федерации, содержащими необходимую информацию, в целях установления взаимного соответствия сведений о владельце сертификата ключа проверки электронной подписи, обязанных содержаться в сертификате согласно части 2 статьи 17 Закона «Об электронной подписи».



ЮЛ → выписки из ЕГРЮЛ по запросам органов государственной власти

ИП → выписки из ЕГРИП по запросам органов государственной власти

ФЛ → о соответствии фамильно-именной группы, даты рождения, пола и СНИЛС

Существующие ограничения при проверке сертификатов в СМЭВ и возможные пути их решения

- Проверка фамилии, имени, отчества и ИНН ФЛ в СМЭВ
- Проверка сведений о ЮЛ иностранного государства
- Невозможность запроса сведений в СМЭВ доверенной третьей стороной

Существующие ограничения при проверке сертификатов в СМЭВ и возможные пути их решения

Проект

ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ

ПОСТАНОВЛЕНИЕ

от №

МОСКВА

О внесении изменений в Правила присоединения информационных систем организаций к инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг и исполнения государственных и муниципальных функций в электронной форме

Правительство Российской Федерации **п о с т а н о в л я е т:**

Особенности выдачи сертификатов службам УЦ и ДТС и возможные пути их решения

Статья 10. Обязанности участников электронного взаимодействия при использовании усиленных электронных подписей

2. Участники электронного взаимодействия **не вправе** устанавливать иные, за исключением предусмотренных настоящим Федеральным законом, ограничения признания усиленной квалифицированной электронной подписи. Нарушение запрета на ограничение или отказ от признания электронных документов, подписанных квалифицированной электронной подписью, соответствующей предъявляемым к ней требованиям, равнозначными документам на бумажном носителе, подписанным собственноручной подписью, а также нарушение запрета операторами государственных и муниципальных информационных систем, информационных систем, использование которых предусмотрено нормативными правовыми актами, или информационных систем общего пользования на предъявление требований о наличии в квалифицированном сертификате информации, не являющейся обязательной в соответствии с настоящим Федеральным законом и принимаемыми в соответствии с ним нормативными правовыми актами, по любым причинам, кроме предусмотренных настоящим Федеральным законом, не допускается.

Особенности выдачи сертификатов службам УЦ и ДТС и возможные пути их решения

Internet X.509 Public Key Infrastructure Certificate
and Certificate Revocation List (CRL) Profile

4.2.1.4. Certificate Policies

The certificate policies extension contains a sequence of one or more policy information terms, each of which consists of an object identifier (OID) and optional qualifiers.…

In an end entity certificate, these policy information terms indicate the policy under which the certificate has been issued and the purposes for which the certificate may be used. In a CA certificate,

Особенности выдачи сертификатов службам УЦ и ДТС и возможные пути их решения

Сертификат OCSP-сервера (служба онлайн проверки СКП ЭП)

- OID 1.3.6.1.5.5.7.3.9
- расширение EKU должно быть помечено как критическое
- назначение «Подпись ответов службы OCSP» (id-kp-OCSPSigning)
- для обеспечения доверия, сертификат OCSP-серверу должен выдать УЦ, выдавший проверяемый сертификат

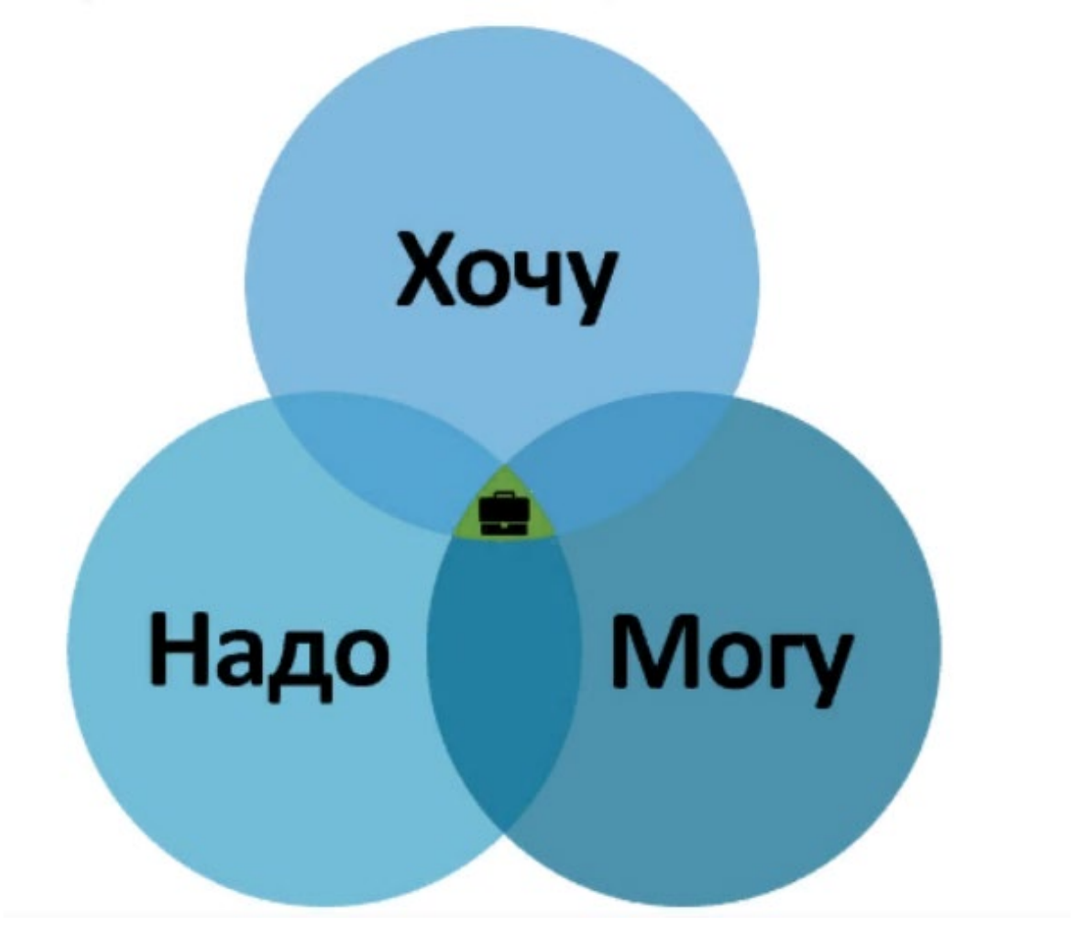
Сертификат TSP-сервера (служба меток доверенного времени)

- OID 1.3.6.1.5.5.7.3.8
- расширение EKU должно быть помечено как критическое
- назначение «Подпись штампов времени» (id-kp-timeStamping)

Сертификат DVCS-сервера (служба Доверенной третьей стороны)

- OID 1.3.6.1.5.5.7.3.10
- расширение EKU должно быть помечено как критическое
- назначение «Подпись ответов службы DVCS» (id-kp-dvcs)

Особенности выдачи сертификатов службам УЦ и ДТС и возможные пути их решения



Предложения для внесения в итоговую декларацию

1. Рассмотреть возможность выдачи сертификатов службам TSP и OCSP аккредитованным УЦ, к которому данные службы относятся.
2. Рассмотреть возможность внесения изменений в 63ФЗ о допустимости использовать специальные объектные идентификаторы для ДТС и служб TSP и OCSP. Требования к наличию OID в сертификатах должны быть приведены в нормативно-технических документах (стандартах, рекомендациях по стандартизации) на соответствующий протокол.
3. Рассмотреть возможность выполнения обновления (дополнения) справочника СМЭВ в части недостающих для проверки сведений о владельце сертификата, а также скорректировать список получателей сведений СМЭВ, дополнив его ДТС.
4. Рассмотреть возможность внесения изменений в Приказ ФСБ России № 795, предусматривающих необязательность использования атрибутов INNLE, INN и SNILS для юридических и физических лиц иностранных государств.
5. Рассмотреть возможность внесения изменений в Приказ ФСБ России № 795, предусматривающих возможность использования атрибута stateOrProvinceName для юридических лиц иностранных государств, а также урегулировать случаи заполнения атрибутов LocalityName и StreetAddress.

GIS ГАЗИНФОРМ СЕРВИС

Спасибо за внимание!

Ермина Екатерина
Ermina-e@gaz-is.ru