

XIX международная научно-практическая конференция
«РусКрипто'2017»

Комплекс тестов, рекомендованных NIST, для
подтверждения корректности функционирования PKI-
решений

Камозин Алексей
Инженер-проектировщик
ООО «Газинформсервис», г. Санкт-Петербург
Kamozin-A@gaz-is.ru
www.gaz-is.ru



Целостность документа

Действительность сертификата



Подпись верна

Построение цепочки сертификации в Litoria Desktop

The screenshot shows the 'Сертификат' (Certificate) window in Litoria Desktop. At the top, it displays 'Цепочка корректна' (Chain is correct). Below this, a tree view shows the 'Цепочка сертификации' (Certificate chain) starting with 'Trust Anchor' and ending with 'Valid pathLenConstraint EE Certificate Test13'. The 'Состав сертификата' (Certificate composition) table is shown below, and the 'Дополнительная информация' (Additional information) section indicates the certificate is valid.

Цепочка сертификации

- Trust Anchor
 - pathLenConstraint6 CA
 - pathLenConstraint6 subCA4
 - pathLenConstraint6 subsubCA41
 - pathLenConstraint6 subsubsubCA41X
 - Valid pathLenConstraint EE Certificate Test13

Состав сертификата Показать: Основная информация

Поле	Значение
Субъект	Общее имя = Valid pathLenConstraint EE Certificate Test13 Организация = Test Certificates 2011 Страна = US
Действителен с	01.01.2010 11:30:00
Действителен до	31.12.2030 11:30:00
Серийный номер	01

Дополнительная информация:
Сертификат действителен.

Сохранить Проверить Просмотр

Обновить

Long
GOOD
Good
Goo
Negat
Test C
onlyC
Test C
Test C
pathL
pathL
pathL
pathL
pathL
Mapp
Good
P12 M
P1any
P1any
P12 M
P1 M

Детально

NLST

**Public Key Interoperability
Test Suite (PKITS)
Certification Path Validation**

Номер группы тестов	На что направлены тесты	Количество тестов
1	Проверка ЭП на каждом сертификате в цепочке сертификации	6
2	Проверка срока действия сертификата	8
3	Проверка имен цепочки сертификации	11
4	Проверка списков отозванных сертификатов	21
5	Проверка списков отозванных сертификатов подписанных новым ключом ЦС	8
6	Проверка способности средств ЭП обрабатывать расширение basicConstraints	17
7	Проверка способности средств ЭП обрабатывать расширение keyUsage, в сертификате, используемом для проверки другого сертификата	5
8	Проверка способности средств ЭП обрабатывать расширение certificatePolicies	20

Номер группы тестов	На что направлены тесты	Количество тестов
9	Проверка способности средств ЭП обрабатывать поле requireExplicitPolicy из расширения policyConstraints	8
10	Проверка способности средств ЭП обрабатывать расширение policyMappings	14
11	Проверка способности средств ЭП обрабатывать поле inhibitPolicyMapping из расширения policyConstraints	11
12	Проверка способности средств ЭП обрабатывать расширение inhibitAnyPolicy и обрабатывать сертификаты, которые устанавливают OID anyPolicy, когда использование anyPolicy было запрещено.	10
13	Проверка способности средств ЭП обрабатывать расширение nameConstraints	38
14	Проверка способности средств ЭП обрабатывать расширение сертификата cRLDistributionPoints и расширение CRL issuingDistributionPoint	35
15	Проверка способности средств ЭП обрабатывать расширение deltaCRLIndicator	10
16	Проверка способности средств ЭП обрабатывать сертификаты, которые включают неизвестные расширения	2

Промежуточный
сертификат в расширение
«Использование ключа»
не содержит значения
«Подпись списка отзыва»



Нельзя доверять CRL
содержащему подпись
такого промежуточного
ЦС

Litoria Desktop
Интерфейс Справка

Сертификат

Статус отзыва сертификата или одного из сертификатов в цепочке не определен.

Цепочка сертификации

- Trust Anchor
 - keyUsage Not Critical cRLSign False CA
 - Invalid keyUsage Not Critical cRLSign False EE Certificate Test5

Состав сертификата Показать: Основная информация

Поле	Значение
Субъект	Общее имя = Invalid keyUsage Not Critical cRLSign False EE Certificate Test5 Организация = Test Certificates 2011 Страна = US
Действителен с	01.01.2010 11:30:00
Действителен до	31.12.2030 11:30:00
Серийный номер	01

Дополнительная информация:
Статус отзыва сертификата неопределен.

Сохранить Проверить Просмотр

Сертификат конечного пользователя содержит критическое **неизвестное** расширение



Такой сертификат не должен проходить проверку

Сертификат

Сертификат или один из сертификатов в цепочке содержит неподдерживаемое критическое расширение.

Цепочка сертификации

- Trust Anchor
 - Invalid Unknown Critical Certificate Extension EE Cert Test2

Состав сертификата Показать: Основная информация

Поле	Значение
Субъект	Общее имя = Invalid Unknown Critical Certificate Extension EE Cert Test2 Организация = Test Certificates 2011 Страна = US
Действителен с	01.01.2010 11:30:00
Действителен до	31.12.2030 11:30:00
Серийный номер	5f

Дополнительная информация:

Сертификат содержит критическое расширение, которое не может быть распознано.

Сохранить Проверить Просмотр

Обновить

16
t7
t8
Test20
Test21
st2
8

Детально

В полном CRL сертификат содержится как приостановленный.

В deltaCRL содержится информация об удалении сертификата из базового CRL



Сертификат признается действительным

The screenshot displays a software interface with several windows. The main window, titled 'Сертификат', shows a 'Цепочка сертификатов' (Certificate Chain) with a 'Trust Anchor' containing 'deltaCRL CA1' and 'Valid deltaCRL EE Certificate Test5'. Below this, the 'Состав сертификата' (Certificate Composition) table is visible:

Поле	Общие	Организац	Страна
Субъект			
Действителен с	01.01.2011		
Действителен до	31.12.2030		
Серийный номер	04		

Two 'Информация о списке отзыва' (Revocation List Information) windows are also shown. The left one displays the following details:

Версия: 2
Действителен с: 01.01.2011 11:30:00
Действителен до: 31.12.2030 11:30:00
Общее имя = deltaCRL CA1
Организация = Test Certificates 2011
Страна = US

The right window shows a table of 'Отозванные сертификаты' (Revoked Certificates):

Серийный номер	Дата отзыва	Причина отзыва
02	01.01.2010 11:30:00	Компрометация ключа
04	01.01.2010 11:30:00	Сертификат на удержании
05	01.01.2010 11:30:00	Сертификат на удержании

The table in the right window also includes entries 03 and 06 with the reason 'Сертификат был в списке отзвов, но сейчас дейст...'.

Сравнение успешности прохождения тестов

Номер группы тестов	Количество пройденных тестов	
	Litoria Desktop 1.0.31	Litoria Desktop 1.0.43
1	3/6	3/6
2	8/8	8/8
3	11/11	11/11
4	21/21	21/21
5	8/8	8/8
6	17/17	17/17
7	0/5	5/5
8	0/20	20/20
9	0/8	8/8
10	0/14	14/14
11	0/11	11/11
12	0/10	10/10
13	0/38	38/38
14	0/35	35/35
15	0/10	10/10
16	0/2	2/2
Итого:	68/224	221/224

LITORIA®
Desktop

Сертификат соответствия
Регистрационный номер: СФ/124-3064 от 07 февраля 2017 г.
Действителен до 31 декабря 2018 г.



Спасибо за внимание!

Камозин Алексей
Инженер-проектировщик
ООО «Газинформсервис», г. Санкт-Петербург
Kamozin-A@gaz-is.ru
www.gaz-is.ru