ГАЗИНФОРМСЕРВИС

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

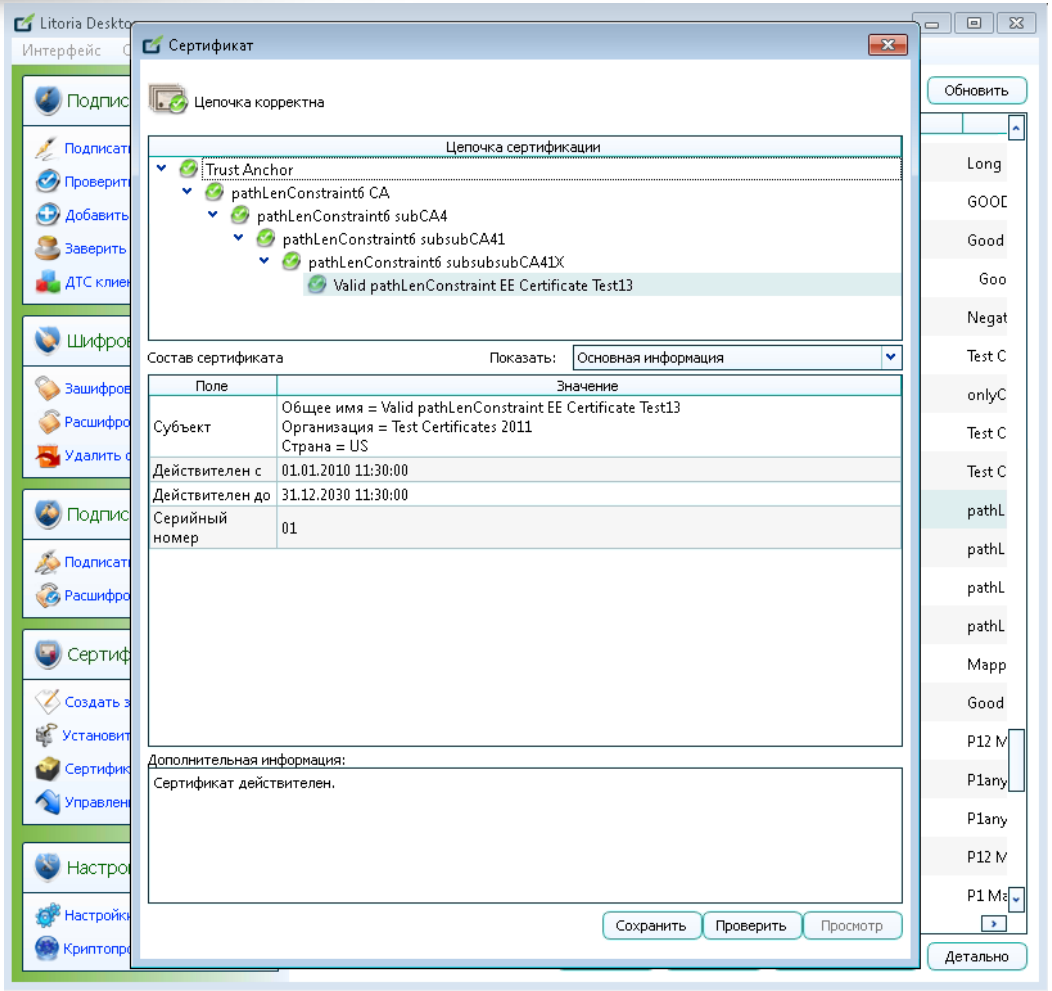
Целостность документа

Действительность сертификата

Подпись верна

Построение цепочки сертификации в Litoria Desktop

ГАЗИНФОРМСЕРВИС



ГАЗИНФОРМСЕРВИС

NIST

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 inihibitPolicyMapping 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

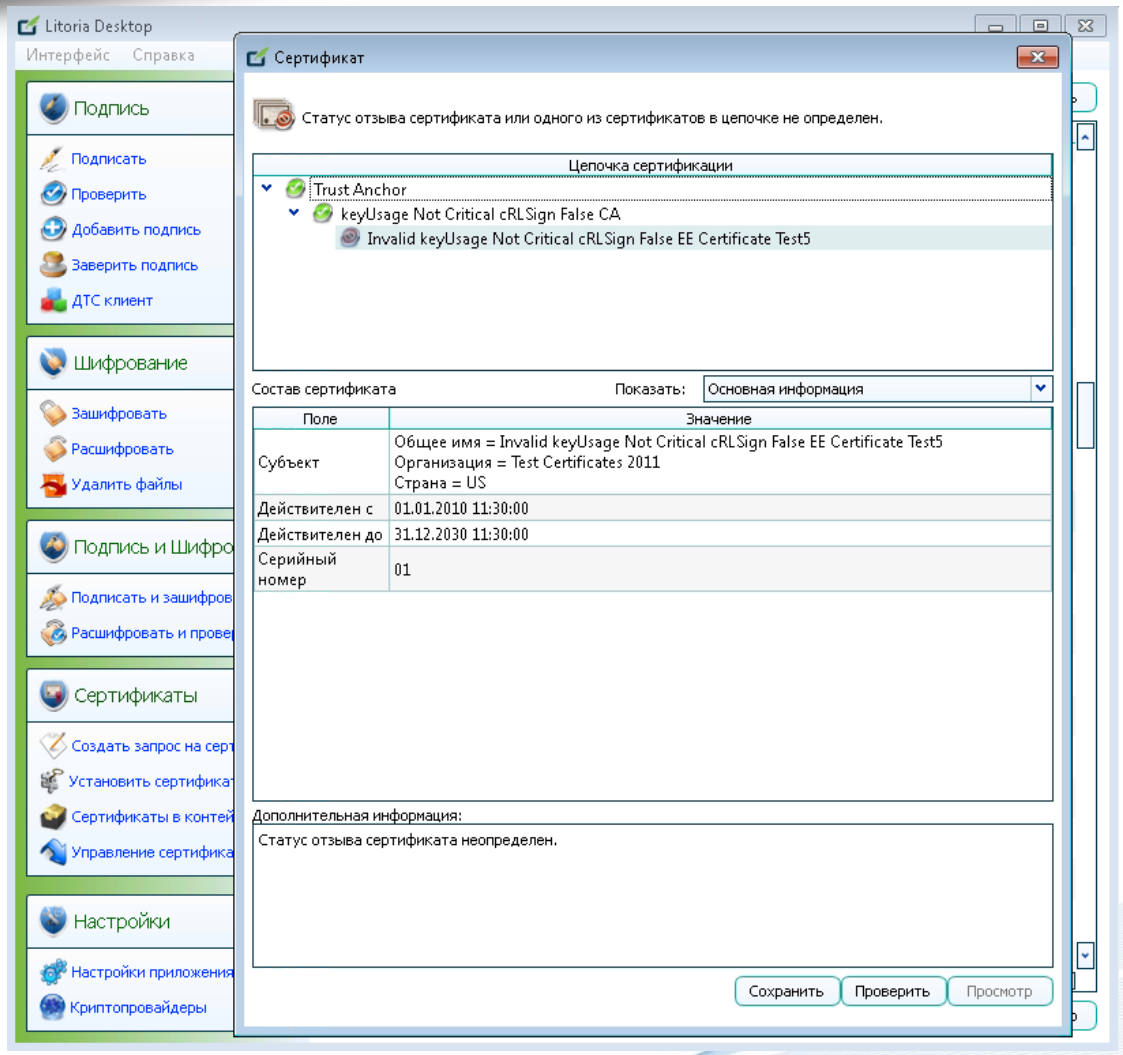
Тест 4.7.5

ГАЗИНФОРМСЕРВИС

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

↓

Нельзя доверять CRL содержащему подпись такого промежуточного ЦС

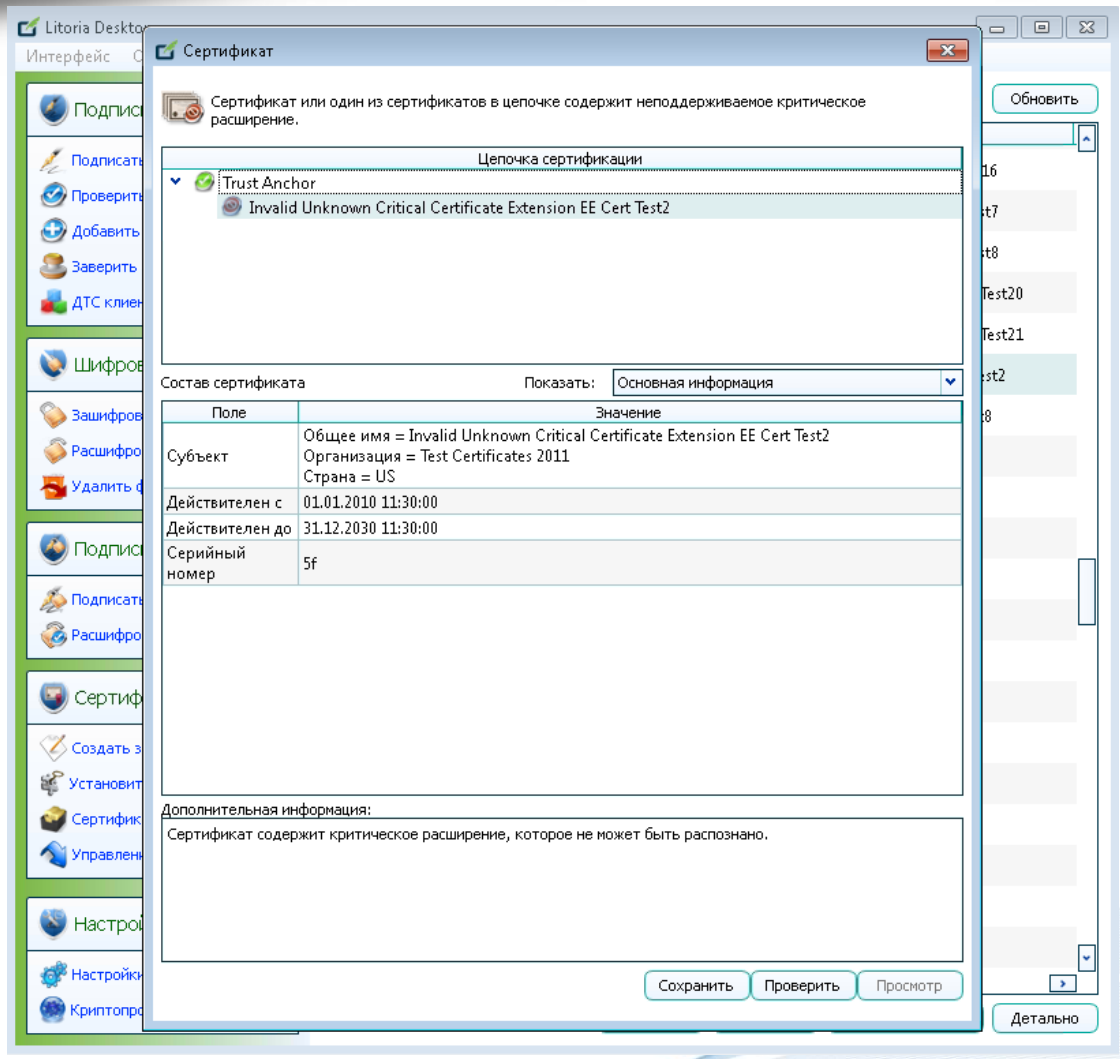


Тест 4.16.2

ГАЗИНФОРМСЕРВИС

Сертификат конечного пользователя содержит критическое **неизвестное** расширение

Такой сертификат не должен проходить проверку



Тест 4.15.5

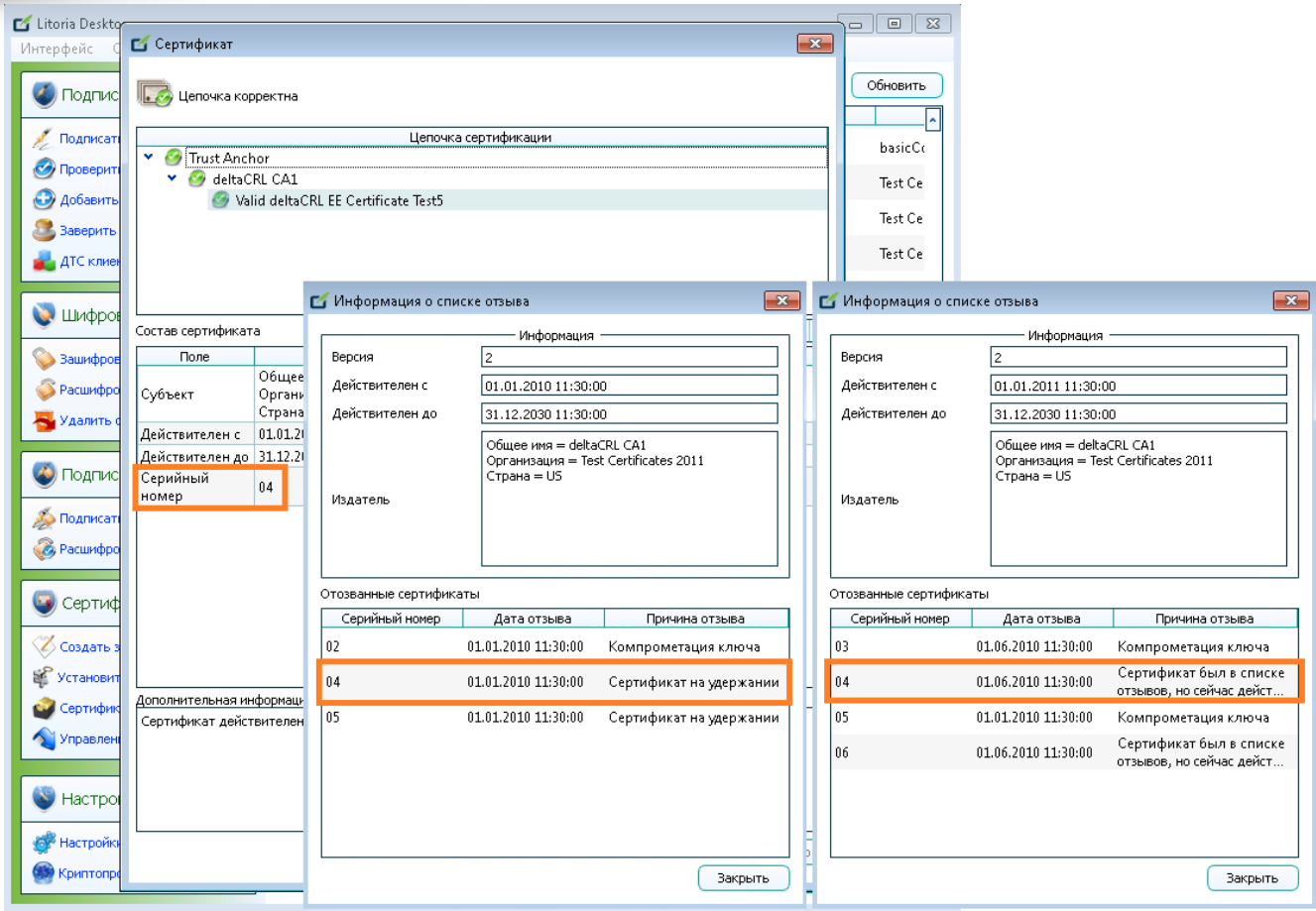
ГАЗИНФОРМСЕРВИС

В полном CRL сертификат содержится как приостановленный.

В deltaCRL содержится информация об удалении сертификата из базового CRL

↓

Сертификат признается действительным



Сравнение успешности прохождения тестов

ГАЗИНФОРМСЕРВИС

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

ГАЗИНФОРМСЕРВИС

LITORIA® Desktop

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

ГАЗИНФОРМСЕРВИС

Спасибо за внимание!

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