PKI-FORUM

Стандартизация и унификация процессов формирования и проверки электронной подписи

Татьяна Станкевич
менеджер по продукту
ООО «Газинформсервис»
к.т.н., доцент ИнИБ ПГУПС
stankevich-t@gaz-is.ru,
тел. +7(911) 931-27-24

ГАЗИНФОРМСЕРВИС

Математическая корректность ЭП

- ГОСТ 34.10-2012 (2001) «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи»

- ГОСТ 34.11-2012 «Информационная технология. Криптографическая защита информации. Функция хэширования»

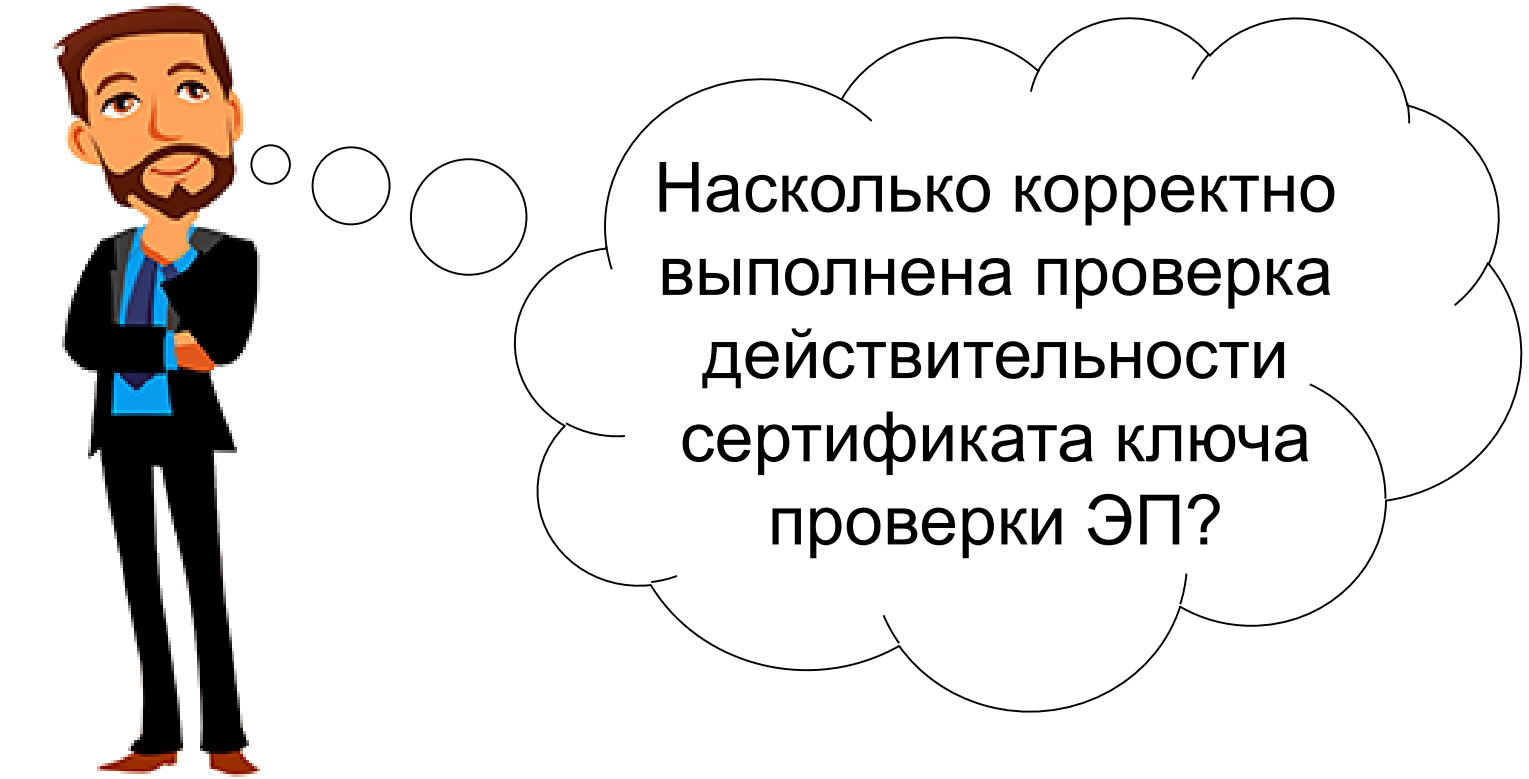
Нормативно-правовое регулирование PKI

- Федеральный закон Российской Федерации от 06.04.2011 №63-ФЗ «Об электронной подписи» (в ред. Федерального закона от 30.12.2015 N 445-ФЗ);

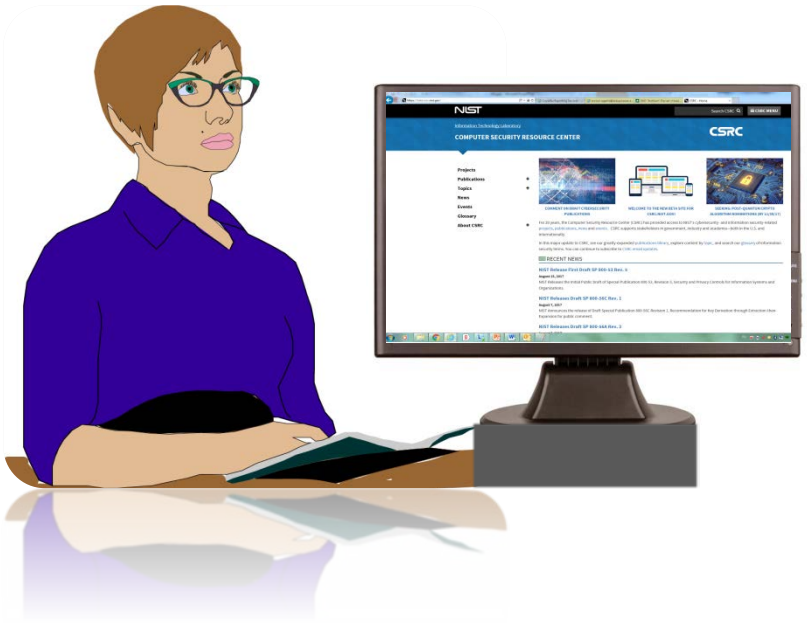
- Приказ ФСБ России от 27.12.2011 № 796 «Об утверждении Требований к средствам электронной подписи и Требований к средствам удостоверяющего центра»;

- Приказ ФСБ РФ от 27.12.2011 г. N 795 «Об утверждении Требований к форме квалифицированного сертификата ключа проверки электронной подписи»

«Упущенные моменты» нормативно-правового регулирования PKI

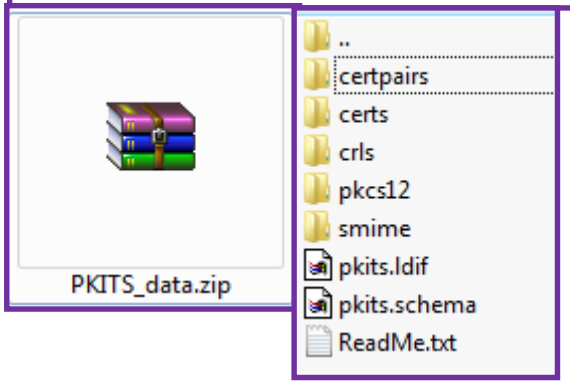


Соответствие международным рекомендациям



Public Key Interoperability Test Suite (PKITS) Certification Path Validation

224 Теста



Path Validation Testing Program

Test descriptions http://csrc.nist.gov/groups/ST/crypto_apps_infra/documents/PKITS.pdf

Test data http://csrc.nist.gov/groups/ST/crypto_apps_infra/pki/pkitesting.html

Независимое экспертное исследование

Тест российских средств электронной подписи и шифрования документов

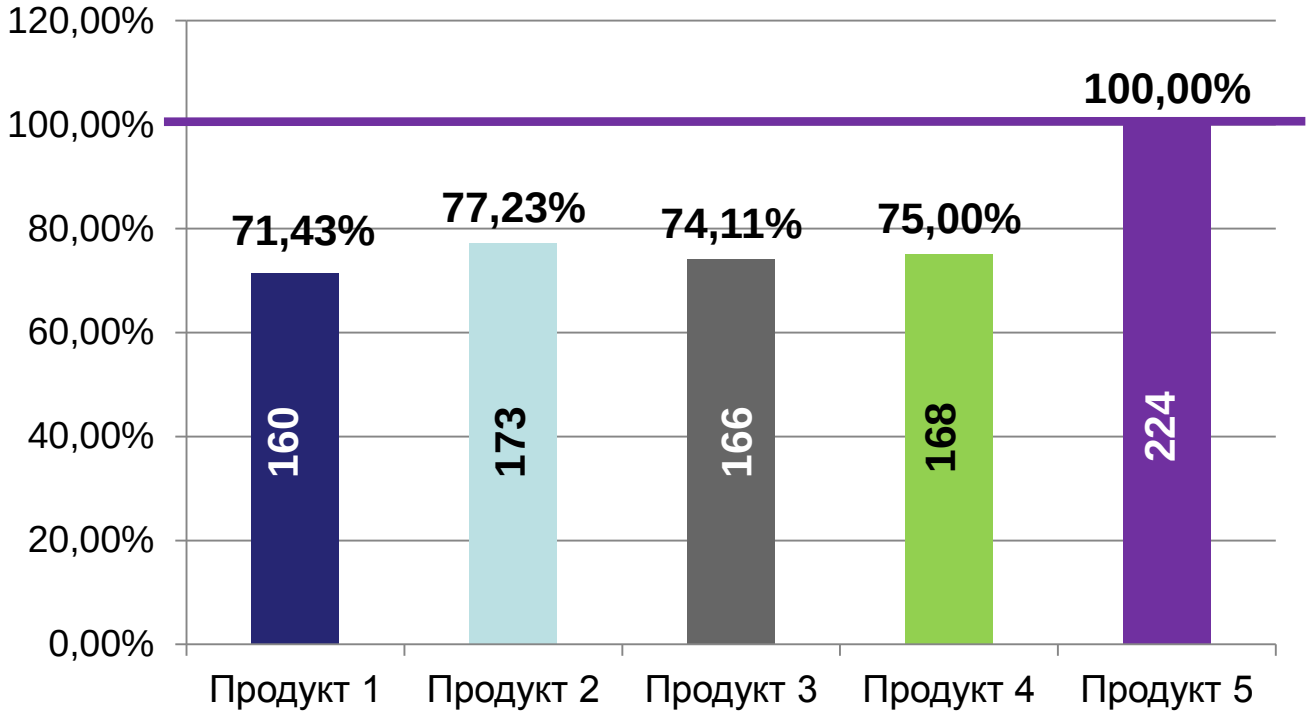
Александр Панасенко
Главный-редактор Anti-Malware.ru

Сравнения | Корпорации | Admin-PKI | File-PRO | Litoria Desktop | ...

Для того чтобы признать электронный документ равным с юридической точки зрения бумажному с подписью и печатью, необходима электронная подпись, а безопасная отправка чувствительных данных должна быть обеспечена посредством их шифрования. Но несмотря на то, что государство всячески пропагандирует переход к электронному взаимодействию, нормативно-правовая база, регулирующая направление PKI, развита слабо, в ней отсутствуют строго определенные принципы построения инфраструктуры открытых ключей.

С результатами независимого тестирования можно ознакомиться здесь
https://www.anti-malware.ru/compare/test_russian_digital_signature_and_encryption_documents

Итоги независимого исследования



«Недоделочка». Примеры тестов

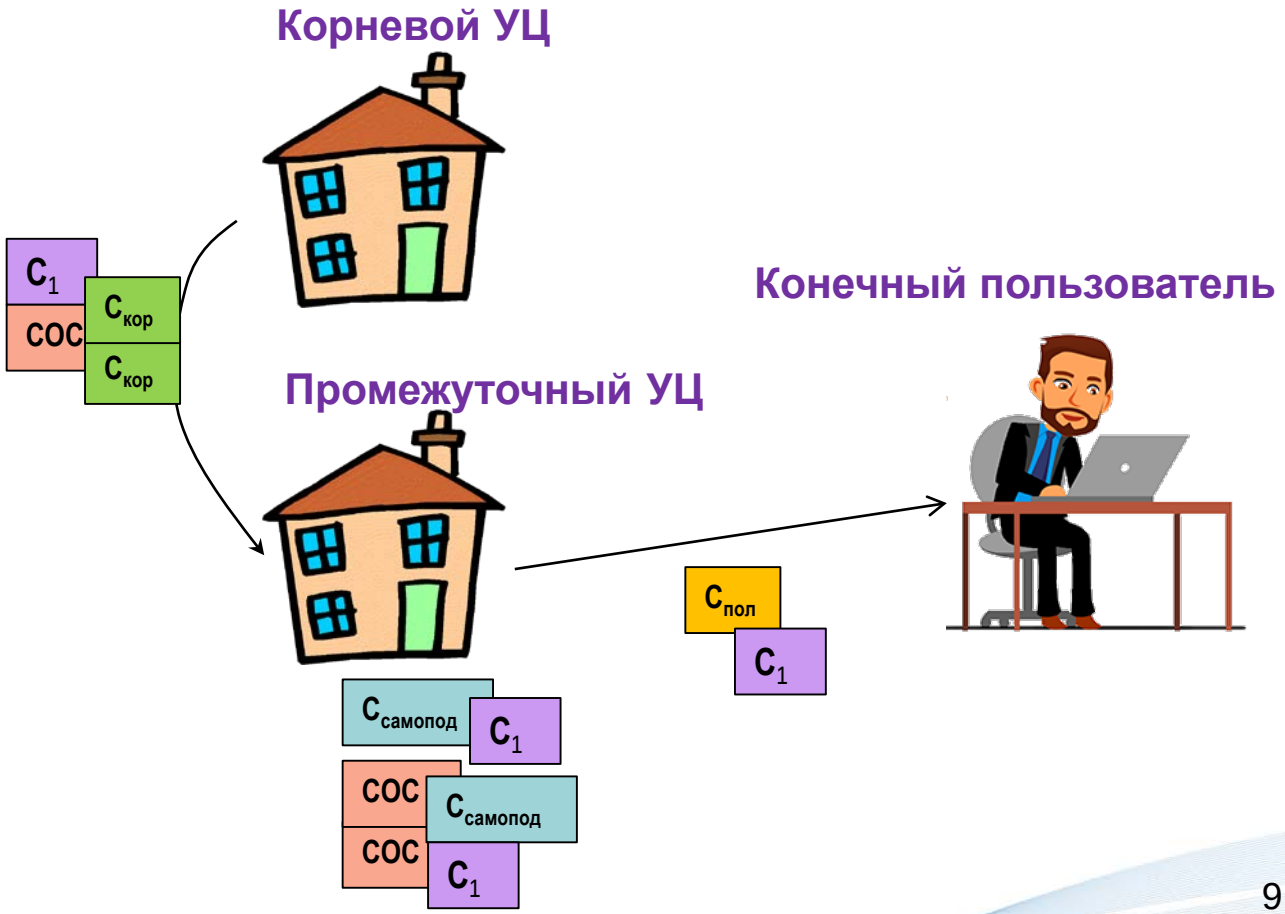
Раздел	Номер теста	Название теста	Название сертификата конечного объекта (Кому выдан)	Статус цепочки	Описание проблемы	Продукт 5	Продукт 1	Продукт 2	Продукт 3	Продукт 4
4.5.	4.	Valid Basic Self-Issued New With Old Test4	Valid Basic Self-Issued New With Old EE Certificate Test4	корректна		+	-	-	-	-
4.5.	5.	Invalid Basic Self-Issued New With Old Test5	Invalid Basic Self-Issued New With Old EE Certificate Test5	некорректна	Пользовательский сертификат отозван	+	#	#	#	#
4.5.	6.	Valid Basic Self-Issued CRL Signing Key Test6	Valid Basic Self-Issued CRL Signing Key EE Certificate Test6	корректна		+	-	-	-	-

+	Статус сертификата ключа проверки ЭП отображается верно
-	Статус сертификата ключа проверки ЭП отображается неверно
#	Статус сертификата ключа проверки ЭП под вопросом (пояснения в комментарии)
x	Программное обеспечение не предоставляет возможность проверки статуса сертификата

П1: «Статус неизвестен».
П2: «Статус отзыва сертификата не может быть определен».
П3: «Цепочка содержит сертификат, статус отозванности которого неизвестен»
П4: «Функция отзыва не смогла произвести проверку отзыва для сертификата»

Тест 4.5.6.

Успешный результат проверки пользовательского сертификата по CRL, заверенному самоподписанным сертификатом промежуточного УЦ



«Недоделочка». Примеры тестов

Раздел	Номер теста	Название теста	Название сертификата конечного объекта (Кому выдан)	Статус цепочки	Описание проблемы	Продукт 5	Продукт 1	Продукт 2	Продукт 3	Продукт 4
4.9.	3.	Invalid RequireExplicitPolicy Test3	Invalid requireExplicitPolicy EE Certificate Test3	некорректна	Не соответствие политик	+	-	+	-	-
4.9.	4.	Valid RequireExplicitPolicy Test4	Valid requireExplicitPolicy EE Certificate Test4	корректна		+	x	x	x	x
4.14.	16.	Invalid onlySomeReasons Test16	Invalid onlySomeReasons EE Certificate Test16	некорректна	Пользовательский сертификат приостановлен	+	#	#	#	#

П1: «Сертификат действителен»
П2: «Ошибка проверки сертификата»
П3: «Сертификат действителен»
П4: «В порядке. Статус сертификата проверен по локальному СОС»

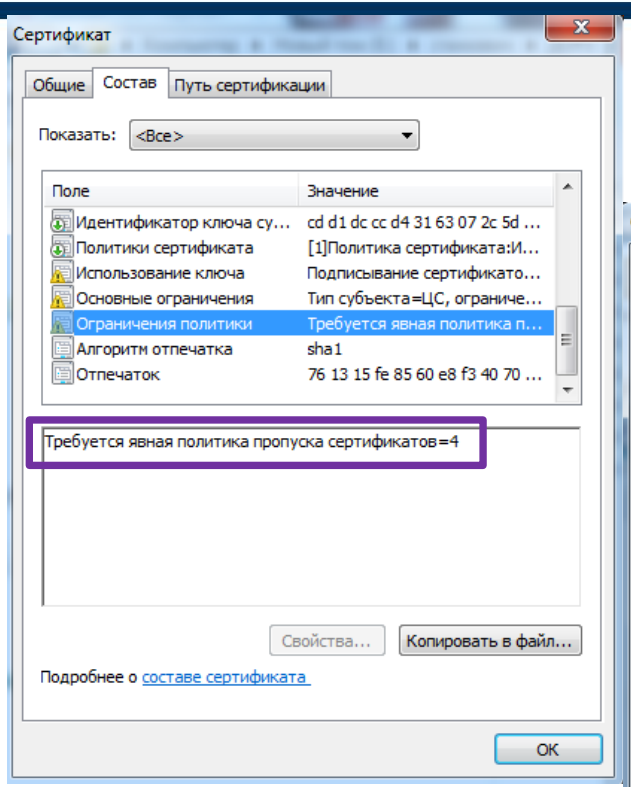
П1: «Сертификат недействителен, Сертификат отозван»
П2: «Сертификат был отозван»
П3: «Цепочка содержит сертификат, статус отозванности которого неизвестен»
П4: «Функция отзыва не смогла произвести проверку отзыва для сертификата»

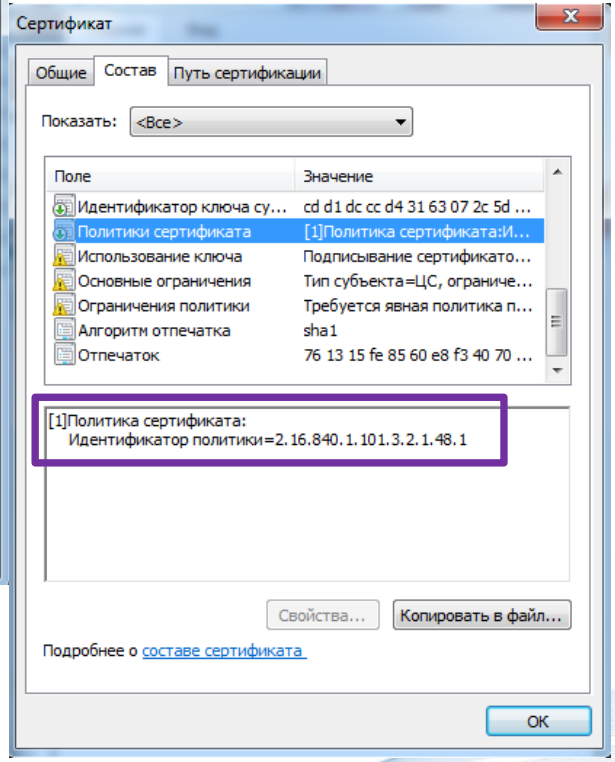
+	Статус сертификата ключа проверки ЭП отображается верно
-	Статус сертификата ключа проверки ЭП отображается неверно
#	Статус сертификата ключа проверки ЭП под вопросом (пояснения в комментарии)
x	Программное обеспечение не предоставляет возможность проверки статуса сертификата

Тест 4.9.3

Отрицательный результат проверки пользовательского сертификата по причине несоответствия ограничений политики

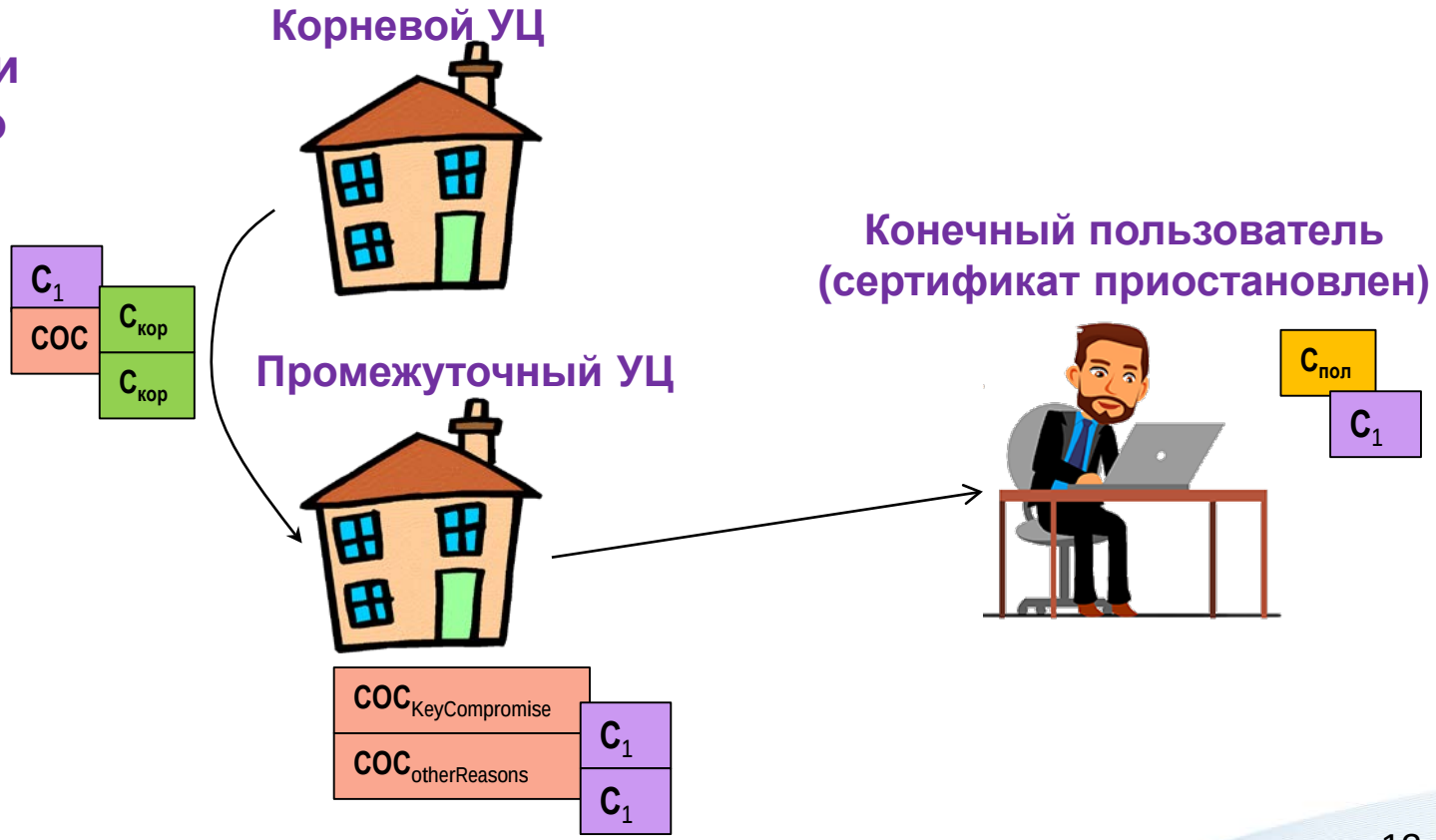
requireExplicitPolicy=4





Тест 4.14.16

Отрицательный результат проверки пользовательского сертификата по причине его приостановки



А что если…

- приложения для работы с ЭП
- платформы и приложения операторов ЭДО
- платформы и приложения государственных ИС
- банковские ИС

выполняют <u>некорректные</u> проверки ЭП?

Мы принимаем желаемое за действительное?

Последствия

1) Финансовые потери

2) Имиджевые (репутационные) потери:

- отзыв лицензий на деятельность;
- лишение аккредитации компании;
- занесение в списки недобросовестных поставщиков.

Главный вывод

Стандартизация процессов формирования и проверки ЭП необходима!

Спасибо за внимание!

Татьяна Станкевич
менеджер по продукту
ООО «Газинформсервис»
к.т.н., доцент ИнИБ ПГУПС
stankevich-t@gaz-is.ru,
тел. +7(911) 931-27-24