# PKI – TopGear: сравнительный анализ средств электронной подписи

Татьяна Станкевич,
Ведущий менеджер по продукту
ООО ВК,
к.т.н.

# О чем поговорим

PKI как набор компонентов для ЭП и шифрования

Валидация действительности цепочки сертификатов и тесты NIST

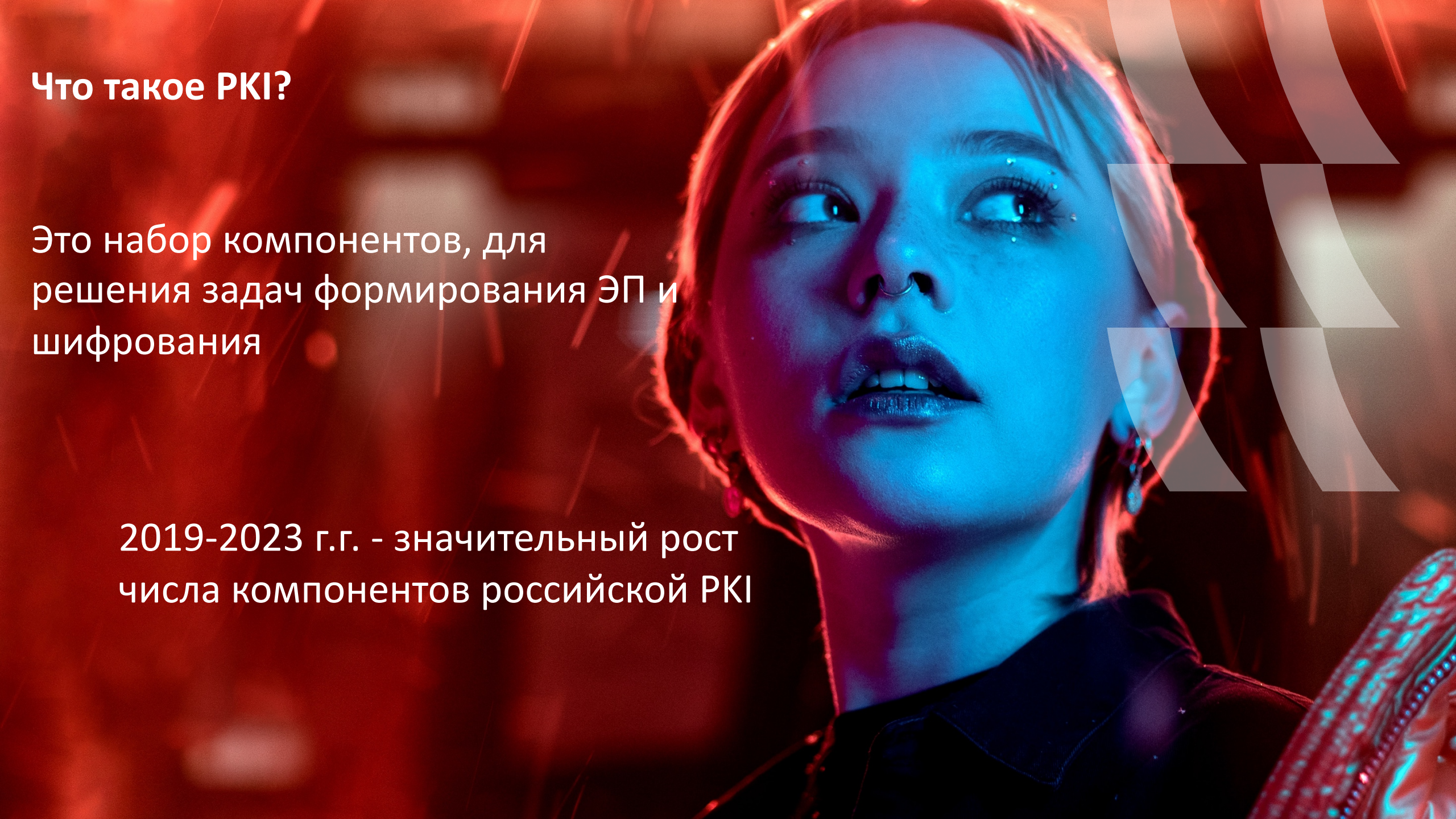
Критерии сравнительного анализа средств ЭП, на которые ориентируются пользователи

Результаты сравнительного анализа

# Что такое PKI?

Это набор компонентов, для решения задач формирования ЭП и шифрования

2019-2023 г.г. - значительный рост числа компонентов российской PKI



# Что такое действительная ЭП?

- Математическая корректность ЭП на ЭД подтверждена;
- Сертификат ключа проверки и цепочка сертификатов для ЭП на ЭД действительны;
- Математическая корректность ЭП на МЧД подтверждена;
- Сертификат ключа проверки и цепочка сертификатов для ЭП на МЧД действительны;
- Полномочия, указанные в МЧД, корректны

*Неквалифицированная ЭП*

*Квалифицированная ЭП*

Валидация действительности цепочки сертификатов.

Тесты NIST

# Что такое действительная ЭП?

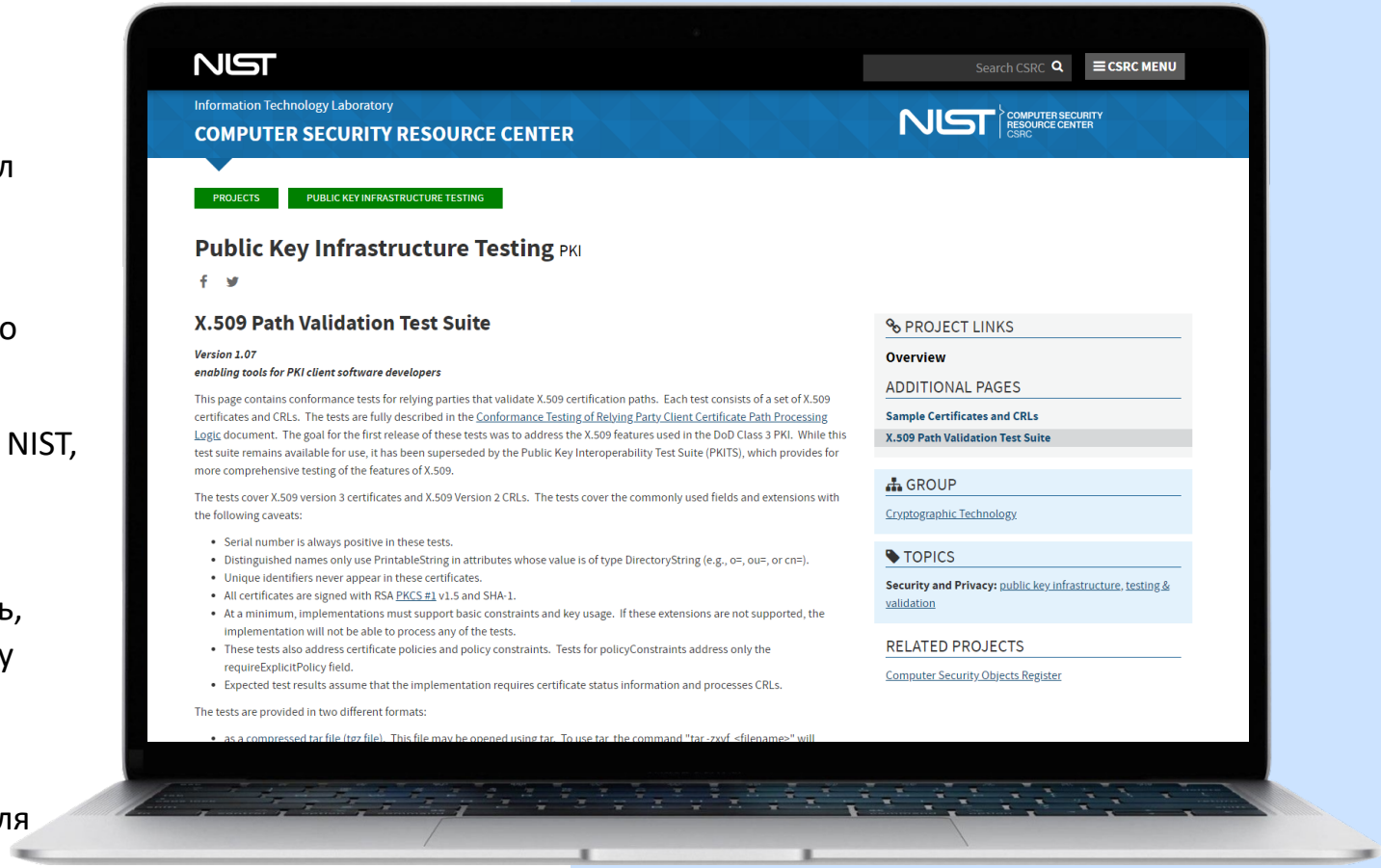
- Математическая корректность ЭП на ЭД подтверждена;
- Сертификат ключа проверки и цепочка сертификатов для ЭП на ЭД действительны;
- Математическая корректность ЭП на МЧД подтверждена;
- Сертификат ключа проверки и цепочка сертификатов для ЭП на МЧД действительны;
- Полномочия, указанные в МЧД, корректны

*Неквалифицированная ЭП*

*Квалифицированная ЭП*

# Зачем проводить тестирование по NIST?

- Специалисты NIST давно пришли к выводу о различиях реализации логики проверки статусов сертификатов различными вендорами. Для унификации этой логики был создан набор тестов
- Различия в логике проверки сертификатов разным программным обеспечением актуальны и для российского рынка
- Тестирование с использованием данных, подготовленных NIST, поможет показать, что результаты проверки ЭП разными решениями будут отличаться
- Проецируя тесты NIST на российский рынок можно сказать, что усиленная неквалифицированная ЭП будет по разному обработана российскими решениями
- Проверка логики валидации сертификата и цепочки сертификации актуальна не только для средств ЭП, но и для прикладного ПО




Источник: [Public Key Infrastructure Testing | CSRC (nist.gov)]

# Тесты NIST, завершенные с результатами отличными от эталонных

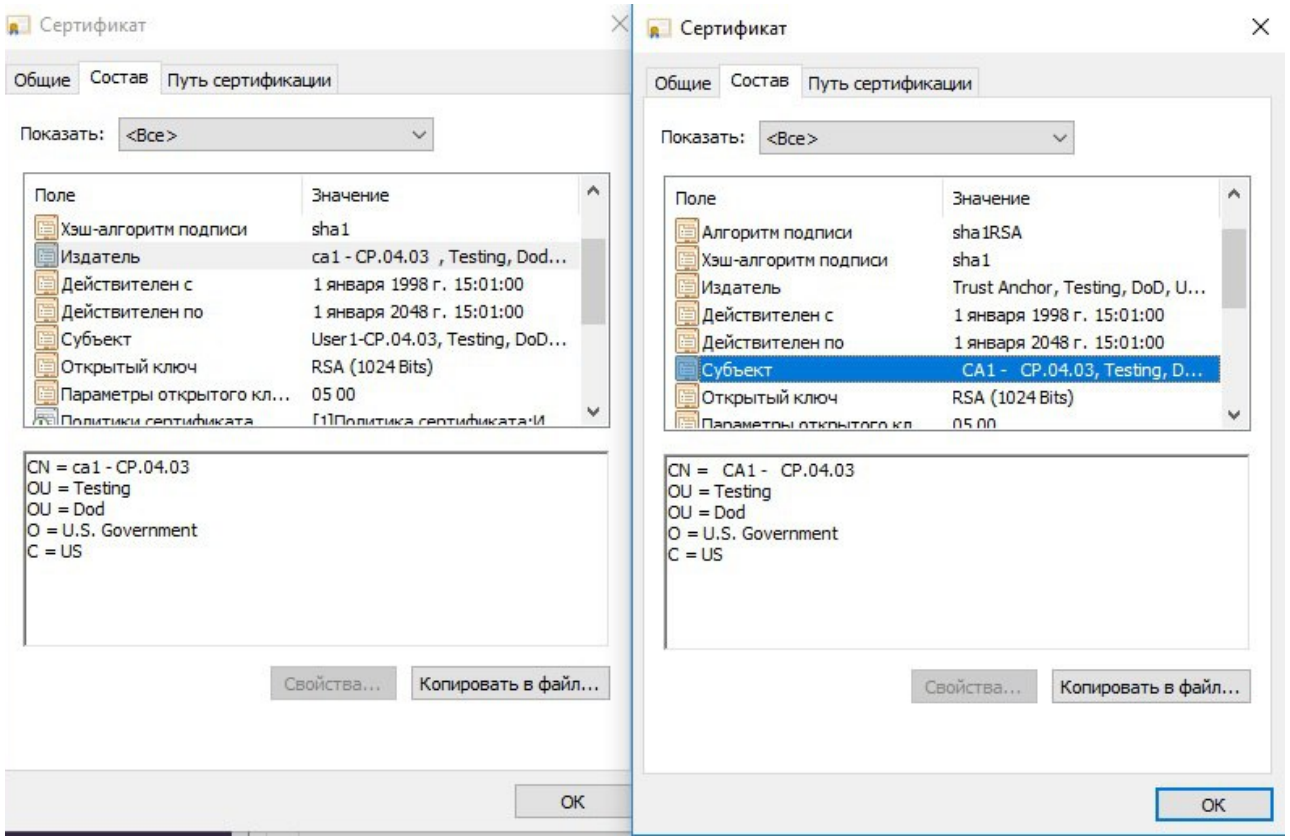
| | Средство ЭП1 | Средство ЭП2 | Средство ЭП3 |
|---|---|---|---|
| **Тесты обработки сертификатов** | | | |
| **CP.04 Приложение должно правильно проверить цепочку сертификатов. Правильная цепочка — это когда издатель каждого сертификата в цепочке равен субъекту вышестоящего сертификата.** | | | |
| CP.04.03<br>Цепочка сертификатов должна быть проверена успешно; имена отличаются только пробелами и заглавными буквами | успех | ошибка | ошибка |
| CP.04.04<br>Цепочка сертификатов должна быть проверена успешно, имена отличаются только пробелами | успех | ошибка | ошибка |
| CP.04.05<br>Цепочка сертификатов должна быть проверена успешно, имена отличаются только начальными/конечными пробелами | успех | ошибка | ошибка |
| CP.04.06<br>Цепочка сертификатов должна быть проверена успешно, имена отличаются только регистром | успех | ошибка | ошибка |
| **Тесты обработки политик** | | | |
| **PP.06 Программное обеспечение должно соответствующим образом обрабатывать явную переменную состояния индикатора политики.** | | | |
| PP.06.03<br>Первый сертификат в пути сертификации (длина 5) содержит расширение ограничений политики, при этом параметр requireExplicitPolicy присутствует и имеет значение 4. | успех | ошибка | ошибка |

# Тесты NIST, завершенные с результатами отличными от эталонных

| | Средство ЭП1 | Средство ЭП2 | Средство ЭП3 |
|---|---|---|---|
| **Тесты длины цепочки сертификатов** | | | |
| **PL 01. Программное обеспечение должно правильно рассчитать допустимую длину пути.** | | | |
| PL.01.02<br>Следующий путь должен быть отклонен. Первый сертификат в пути имеет ограничение длины пути, равное 0 (допускается 0 дополнительных промежуточных сертификатов в пути). Имеется один дополнительный промежуточный сертификат. Конечный сертификат является сертификатом УЦ | успех | ошибка | успех |
| PL.01.06<br>Следующий путь должен быть отклонен. Длина пути равна 4. Первый сертификат в пути имеет ограничение длины пути, равное 6 (допускается 6 дополнительных промежуточных сертификатов в пути). Второй сертификат имеет ограничение длины пути, равное 0. Третий сертификат имеет ограничение длины пути, равное 0. Конечный сертификат является сертификатом УЦ. | успех | ошибка | успех |
| PL.01.08<br>Следующий путь должен быть отклонен. Длина пути равна 5. Первый сертификат в пути имеет ограничение длины пути, равное 6 (допускается 6 дополнительных промежуточных сертификатов в пути). Второй сертификат имеет ограничение длины пути, равное 1. Третий сертификат имеет ограничение длины пути, равное 1. Конечный сертификат является сертификатом УЦ. | успех | ошибка | успех |

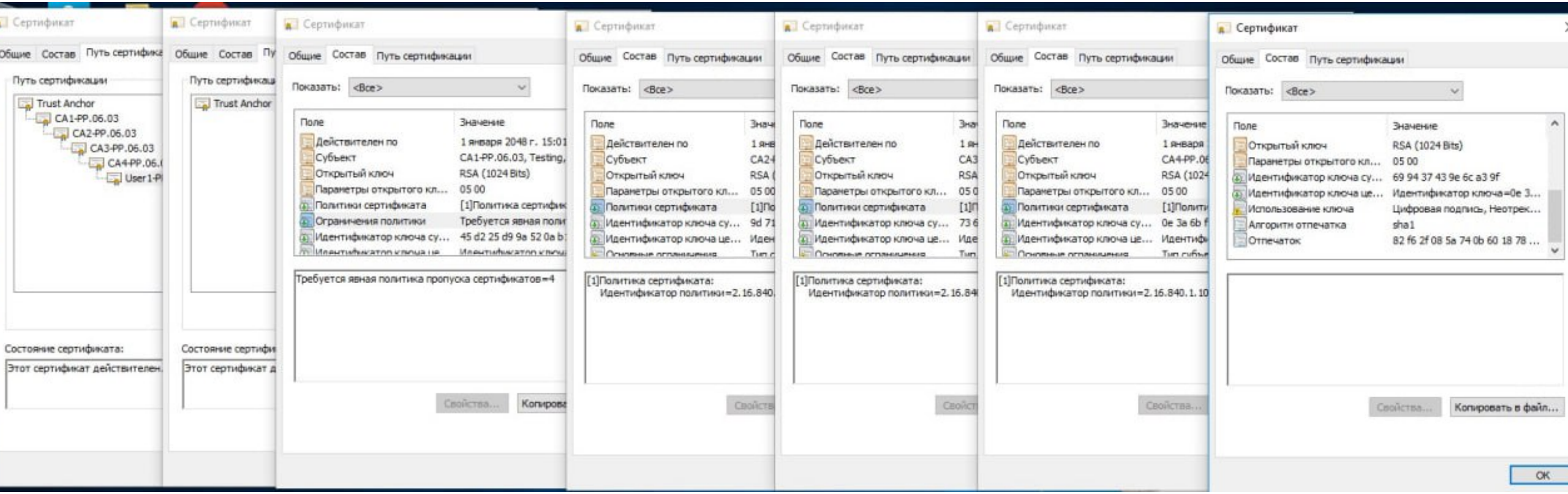
# Тест CP.04.03

- Разница в наименованиях издателя конечного сертификата и субъекта промежуточного сертификата — в пробелах и регистре букв. Конечный сертификат должен быть действительным.



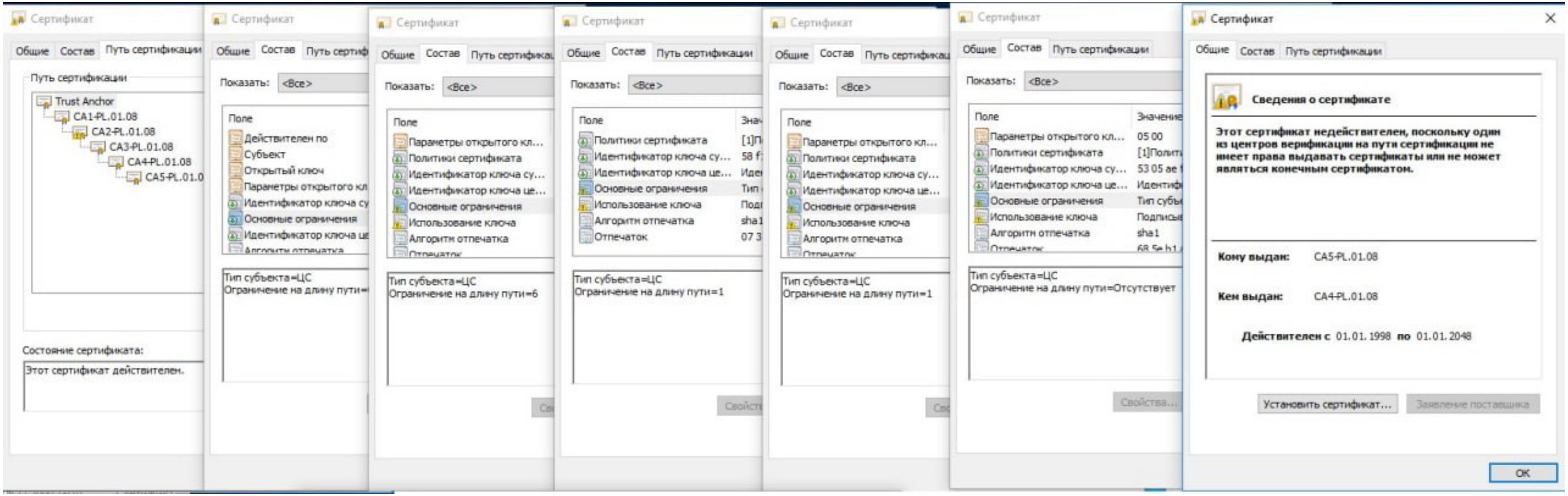
# Тест PP.06.03

- Сертификат первого промежуточного УЦ в цепочке содержит явно определённую политику (через идентификатор), а также расширение ограничения политики (requireExplicitPolicy), равное 4. Если поле «requireExplicitPolicy» присутствует, значение «requireExplicitPolicy» указывает на количество дополнительных сертификатов, которые могут появиться в пути до того, как потребуется явное указание политики. Когда требуется явная политика, необходимо, чтобы все сертификаты в пути содержали идентификатор принимаемой политики. Конечный сертификат должен содержать явное указание политики, но не содержит, поэтому должен быть проверен как недействительный.



# Тест PL.01.08

- Первый промежуточный сертификат в пути имеет ограничение длины пути, равное 6. Второй сертификат имеет ограничение длины пути, равное 1, и должен быть проверен с ошибкой, т. к. это ограничение не выполнено (через один промежуточный сертификат, согласно этому ограничению, должен находиться конечный сертификат). Третий сертификат имеет ограничение длины пути, равное 1. Конечный сертификат должен быть проверен как недействительный, т. к. цепочка сертификатов недействительна.



# 10,5%

Отклонений от эталонных значений тестов NISTвыдало средство ЭП2

# 6,5%

Отклонений от эталонных значений тестов NIST выдало средство ЭП3

Прикладное ПО, реализующее работу с ЭП, также может иметь особенности функционирования

# Критерии сравнительного анализа, на которые ориентируются пользователи

# Критерии

### Сертификат ФСБ России на соответствие Приказу №796

Обязателен для работы с квалифицированной ЭП. Необязателен – для работы с неквалифицированной ЭП

### Соответствие требованиям Приказа ФСБ России №795

Обязательно для формирования запросов на квалифицированные сертификаты с необходимым и достаточным набором полей

### Наличие в Едином реестра российского ПО

Для государственного заказчика исключает дополнительные процедуры согласования закупки, для вендора – исключает уплату НДС с продаж программного обеспечения

### Поддерживаемые форматы ЭП

Характеризует набор дополнительных сведений, которые может включать ЭП в формате CMS/CAdES, а также ЭП для XML и PDF документов в форматах XAdES и PAdES соответственно

# Критерии

### Поддерживаемые форматы электронных документов

Определяет, файлы каких типов могут быть заверены ЭП

### Работа с МЧД

Определяет, готово ли средство ЭП выполнить все необходимые операции для работы с квалифицированной ЭП, включая работу с МЧД, по требованиям ФЗ-63 в актуальной редакции

### Наличие криптопровайдера, реализующего ГОСТовые алгоритмы в составе

Определяет объемы инвестиций и текущих расходов на средство ЭП

### Поддержка работы с зарубежными криптопровайдерами

Определяет возможность использования одного средства ЭП для работы с квалифицированной ЭП (на основе российских алгоритмов) и неквалифицированной ЭП (на основе зарубежных алгоритмов)

# Критерии

### Функция уничтожения ключей ЭП

Характеризует средство ЭП на покрытие требования, внесенного в 63ФЗ Федеральным законом от 4 августа 2023 г. N 457-ФЗ

### Уникальность

Отличительная особенность, присущая только данному средству ЭП

# Результаты сравнительного анализа

# Сравнительный анализ средств ЭП

| | Средство ЭП1 | Средство ЭП2 | Средство ЭП3 | Средство ЭП4 | Средство ЭП5 | Средство ЭП6 | Средство ЭП7 |
|---|---|---|---|---|---|---|---|
| Количество тестов NIST, выполненных с отклонением результатов от эталона (всего тестов 76) | 0 | 8 | 5 | Не поддерживает RSA | Не поддерживает RSA | Не получена демо-сборка | Не тестировалось |
| Сертификат ФСБ России на соответствие требованиям Приказа №796 | да | да | да | да | да | да | да |
| Проверка по актуальной редакции приказа ФСБ 795 (в ред. Приказа ФСБ России от 29.01.2021 N31) | | | | | | | |
| - создание запроса/ проверка сертификата с INNLE (ИНН ЮЛ) | да | да | нет возможности создавать запросы на сертификат из GUI; проверка сертификата - да | да | да | Не получена демо-сборка | да |
| - создание запроса/проверка сертификата с IdentificationKind (тип идентификации будущего владельца сертификата) | нет | да | нет возможности создавать запросы на сертификат из GUI; проверка сертификата - да | да | нет | Не получена демо-сборка | да |

# Сравнительный анализ средств ЭП

| | Средство ЭП1 | Средство ЭП2 | Средство ЭП3 | Средство ЭП4 | Средство ЭП5 | Средство ЭП6 | Средство ЭП7 |
|---|---|---|---|---|---|---|---|
| Работа с МЧД | | | | | | | |
| - Проверка пакета документов с МЧД | Проверка ЭП на ЭД и проверка ЭП (CMS, XMLDSig) на МЧД | Проверка ЭП на ЭД и проверка ЭП (CMS) на МЧД | Проверка ЭП на ЭД и проверка ЭП (CMS) на МЧД | Проверка ЭП на ЭД и проверка ЭП (CMS, XMLDSig) на МЧД | Проверка ЭП на ЭД и проверка ЭП (CMS) на МЧД | Не предоставлена демо | Проверка ЭП (CMS) на МЧД |
| - Формирование пакета документов с МЧД | За рамками функциональности продукта | Архив, содержащий ЭД, файл подписи, файл МЧД, ЭП МЧД | За рамками функциональности продукта | За рамками функциональности продукта | За рамками функциональности продукта | Не предоставлена демо | За рамками функциональности продукта |
| - Создание МЧД | Нет | Нет | Нет | Нет | Нет | Не предоставлена демо | Нет |
| - Подписание МЧД | Отделённая подпись CMS для XML; XMLDSig | Отделённая подпись CMS для XML | Отделённая подпись CMS для XML | Отделённая подпись CMS для XML; XMLDSig | Отделённая подпись CMS для XML | Не предоставлена демо | Отделённая подпись CMS для XML |
| - Проверка ЭП на МЧД | Проверка ЭП на ЭД и проверка ЭП (CMS, XMLDSig) на МЧД | Проверка ЭП на ЭД и проверка ЭП (CMS) на МЧД | Проверка ЭП на ЭД и проверка ЭП (CMS) на МЧД | Проверка ЭП на ЭД и проверка ЭП (CMS, XMLDSig) на МЧД | Проверка ЭП на ЭД и проверка ЭП (CMS) на МЧД | Не предоставлена демо | Проверка ЭП (CMS) на МЧД |

# Сравнительный анализ средств ЭП

| | Средство ЭП1 | Средство ЭП2 | Средство ЭП3 | Средство ЭП4 | Средство ЭП5 | Средство ЭП6 | Средство ЭП7 |
|---|---|---|---|---|---|---|---|
| Поддерживаемые форматы документов | все форматы для подписи CAdES; pdf - PAdES; xml - XAdES | все форматы для подписи CAdES | все форматы для подписи CAdES | все форматы для подписи CAdES; xml - XMLDsig | txt, .xml, .pdf, .odt, .doc, .docx для подписи CMS | Не получена демо-сборка | все форматы для подписи CAdES |
| Форматы ЭП | | | | | | | |
| CAdES | CAdES-BES, CAdES-T, CAdES-X Long Type1, CAdES-A | CAdES-BES, CAdES-T, CAdES-X Long Type1, CAdES-A | CAdES-BES | CAdES-BES, CAdES-T | CMS | Не получена демо-сборка | CAdES-BES, CAdES-T, CAdES-X Long Type 1 |
| XAdES | да | нет | нет | XMLDSIG | XAdES-BES | Не получена демо-сборка | нет |
| PAdES | да | нет | нет | нет | Нет | Не получена демо-сборка | нет |
| Содержит в своем составе криптопровайдер, реализующий алгоритмы ГОСТ | нет | нет | да | да | да | Не получена демо-сборка | да |
| Поддержка криптопровайдера, реализующий зарубежные криптографические алгоритмы | да | да | да | нет | нет | Не получена демо-сборка | нет |

# Сравнительный анализ средств ЭП

| | Средство ЭП1 | Средство ЭП2 | Средство ЭП3 | Средство ЭП4 | Средство ЭП5 | Средство ЭП6 | Средство ЭП7 |
|---|---|---|---|---|---|---|---|
| Функция уничтожения ключей (в соответствии с редакцией 63ФЗ от 04.08.2023) | нет | нет | нет | да | нет | нет | нет |
| Отличительная особенность | Поддержка функциональности клиента Доверенной третьей стороны, есть ПАК ДТС | 1. поддержка функциональности работы с МЧД, формирования пакета документов, заверенных квалифицированной ЭП с МЧД<br>2. Почтовый клиент, реализующий стандарт S\MIME | 1. не требует расходов на закупку средства ЭП, пользовательский интерфейс является надстройкой над криптопровайдером;<br>2. необходимый и достаточный набор функций средства ЭП реализован в пользовательском GUI, без излишеств | Единый клиент для работы с ключами ЭП и реализации сценариев работы с ЭП, не требующий установки дополнительных компонентов | Формирование ЭП происходит только в доверенной среде; генерация ключей электронной подписи формата PKCS#15 | Не получена демо-сборка | Квалифицированная ЭП, которая всегда под рукой (в командировке, в отпуске, в транспорте), в мобильном телефоне для формирования ЭП с любого устройства |

# Выводы

# Ключевые выводы

## 100%

Рассматриваемых средств ЭП выполняют требования российского законодательства

## 10,5%

Максимальный процент отклонений в логике проверки статуса сертификата (по методике NIST) средством ЭП от эталонных

# Ключевые выводы

- Доказано разночтение в проверках цепочки сертификатов разными средствами ЭП
- Ряд прикладного ПО, в т.ч. почтовые клиенты, платформы операторов ЭДО реализуют ЭП, а значит выполняют проверки статусов сертификатов
- В логике обработки сертификатов прикладным ПО также могут быть выявлены расхождения

# МЧД
## ключевые выводы

- Будут иметь разную логику обработки полномочий  компаниями, пользователями, вендорами пока не появится четкого регламента

- Проверка ЭП на МЧД (а, следовательно, и действительности сертификата и его цепочки) будет выполняться с разными результатами действительности пока не появится четкого регламента*

**Вывод сделан на основе проведенных тестов и обнаруженных разночтений*

# Ключевые выводы

Нам нужны регламенты и рекомендации в подходах к проверкам статусов сертификатов и цепочки сертификатов,  а также полномочий, указанных в МЧД

Будем ВКонтакте!

# Спасибо за внимание!

Татьяна Станкевич