

Практика признания квалифицированной электронной подписи

Алексей Иванов
Управление криптографической защиты





ПЛАН ДОКЛАДА:



1

Инструменты проверок квалифицированной электронной подписи:

- Требования к средствам ЭП и к проверкам КЭП.
- Сравнение решений, преимущества и недостатки.

2

Проблемы участников информационного взаимодействия

3

Выводы и предложения





1. ИНСТРУМЕНТЫ ПРОВЕРОК КЭП:



Федеральный закон
№ 63-ФЗ «Об электронной
подписи»



Использовать средства ЭП, имеющих подтверждение соответствия требованиям 63-ФЗ:

- п.4 ч.1 ст.10 63-ФЗ: обязательство использовать для проверки КЭП средства электронной подписи, имеющих подтверждение соответствия требованиям, установленным в соответствии с 63-ФЗ.
- п.3 ст.11 63-ФЗ: проверка КЭП осуществляется с использованием средств электронной подписи, имеющих подтверждение соответствия требованиям, установленным в соответствии с 63-ФЗ.



Прибегать к услугам проверки КЭП (при необходимости):

1. Аккредитованного УЦ (п.9, ч.1 ст.13 63-ФЗ);
2. Доверенной третьей стороны (п.1-2, ч.1 ст.18.1 63-ФЗ).

* Судебная экспертиза.

ТРЕБОВАНИЯ К ПРОВЕРКЕ КЭП:



Федеральный закон
№ 63-ФЗ «Об электронной
подписи»



Статья 11. Признание квалифицированной ЭП. Совокупность условий:

- 1) сертификат КЭП выдан аккредитованным УЦ,
* аккредитация которого действительна на день выдачи сертификата;
- 2) сертификат действителен:
 - **на момент подписания документа (при наличии метки времени)**
 - или на день проверки сертификата (если нет метки времени)
- 2.1) срок действия ключа ЭП не истек:
 - **на момент подписания документа (при наличии метки времени)**
 - или на день проверки КЭП (если нет метки времени)
- 3) имеется:
 - а) подтверждение принадлежности владельцу сертификата КЭП,
 - б) подтверждение отсутствия изменений в документе,**проверено с помощью сертифицированных ФСБ средств ЭП.**



Статья 12. Средства электронной подписи.

ДОСТУПНЫЕ ИНСТРУМЕНТЫ:



СРЕДСТВА ЭЛЕКТРОННОЙ ПОДПИСИ:

01

имеющих подтверждение
соответствия требованиям
63-ФЗ



02

имеющих подтверждение соответствия
требованиям приказа ФСБ России от
27.12.2011 г. № 796

SIGN.ME
JINN CLIENT LITORIA DESKTOP 2
КРИПТОПРО CSP
VIPNET PKI CLIENT ЛИРССЛ-CSP
БИКРИПТ **КРИПТОАРМ ГОСТ**
КРИПТОПРО SVS

03

ПУБЛИЧНЫЕ СЕРВИСЫ*

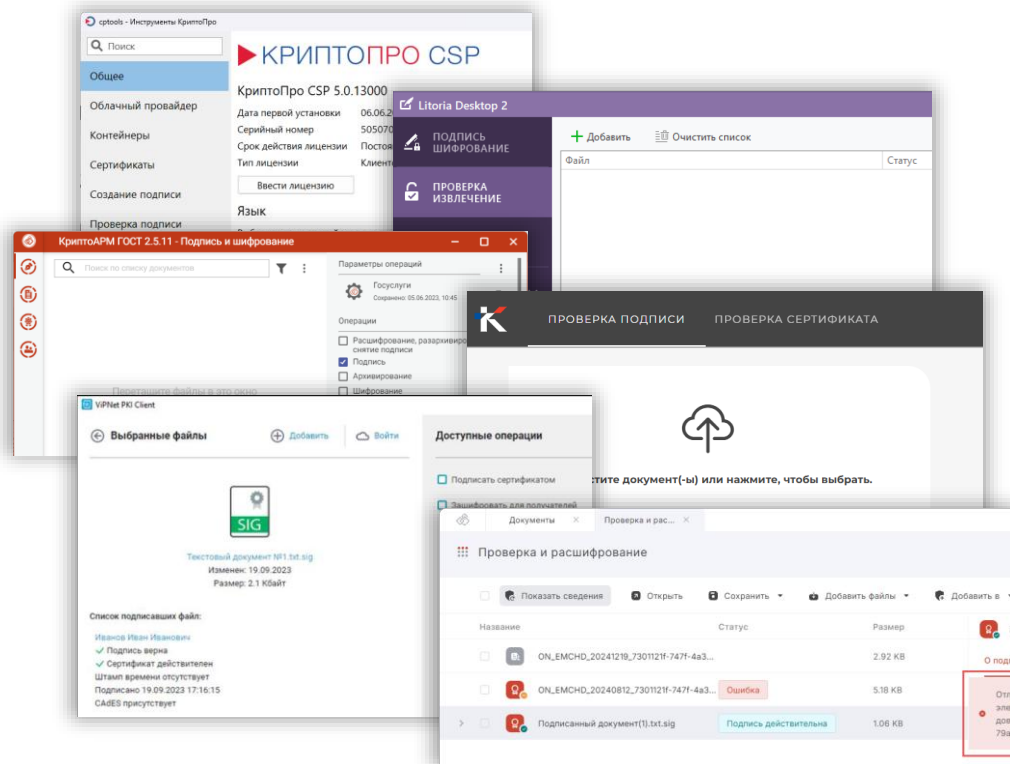
**ПОРТАЛ УФО
(ГОСУСЛУГИ)**

LITORIA DVCS SABY CRYPTO
ПОРТАЛ ФНС
КОНТУР.КРИПТО

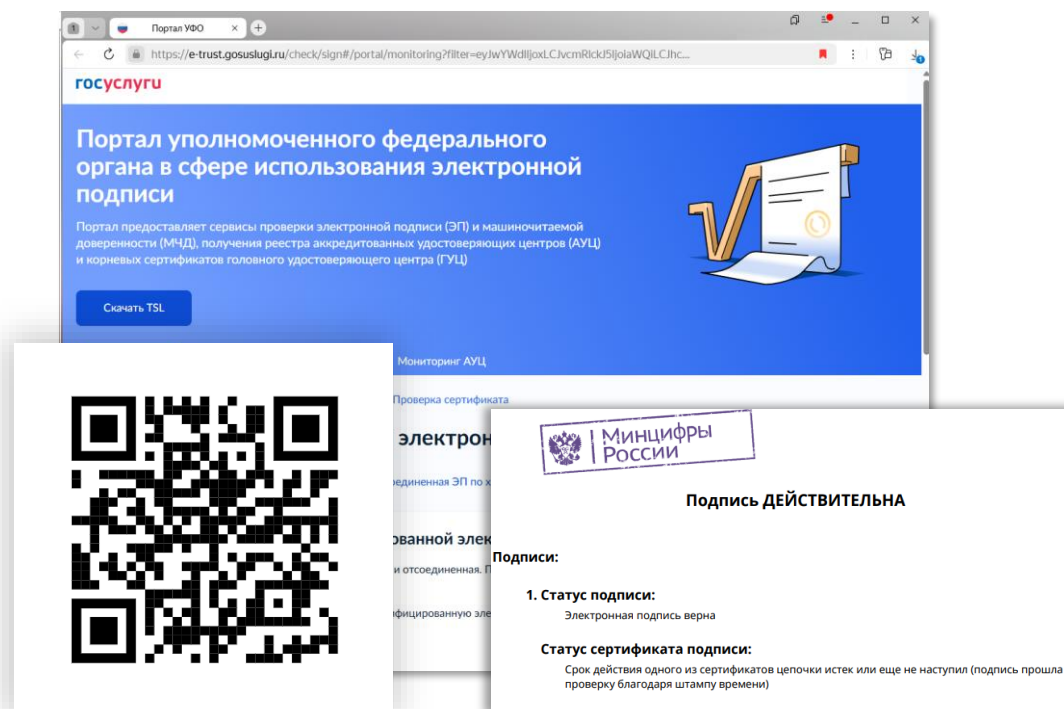
СРАВНЕНИЕ ИНСТРУМЕНТОВ:



СРЕДСТВА ЭП:



ПОРТАЛ УФО (ГОСУСЛУГИ)



<https://e-trust.gosuslugi.ru/check/sign>



СРАВНЕНИЕ ИНСТРУМЕНТОВ:



	СРЕДСТВА ЭП	ПОРТАЛ УФО
ПРЕИМУЩЕСТВА	Сертификаты ФСБ по соответствию требованиям приказа ФСБ России № 796	Проверяет по условиям ст. 11 63-ФЗ*
НЕДОСТАТКИ	Не реализованы проверка условий п.2, п.2.1 ст.11 63-ФЗ в случаях: <ul style="list-style-type: none">• истечения сертификата КЭП;• истечении срока действия ключа ЭП.	Отсутствуют сведения средств ЭП

РАСХОЖДЕНИЕ В РЕЗУЛЬТАТАХ ПРОВЕРОК УКЭП:



СЦЕНАРИЙ	СРЕДСТВА ЭП	ПОРТАЛ УФО
Сертификат - истёк Ключ ЭП - истёк Метка времени - есть	 ОТРИЦАТЕЛЬНЫЙ	 ПОЛОЖИТЕЛЬНЫЙ
Сертификат - действителен Ключ ЭП - истёк Метки времени - нет	 ПОЛОЖИТЕЛЬНЫЙ	 ОТРИЦАТЕЛЬНЫЙ



ИТОГИ СРАВНЕНИЙ:



1. **Портал УФО** проверяет УКЭП согласно условиям ст.11 63-ФЗ, при этом отсутствуют сведения применяемых средств ЭП (п.3 ст.11 63-ФЗ).
2. **Средства ЭП** формирует результаты отличные от условий п.2, п.2.1 ст.11 63-ФЗ при истечении срока действия сертификата и ключа ЭП.
3. Широкое распространение средств ЭП создает риски корректной проверки УКЭП.
4. Отсутствуют готовые инструменты проверки УКЭП под ключ.



2. ПРОБЛЕМЫ УЧАСТНИКОВ



- 01** Невозможность самостоятельной оценки сценария проверки УКЭП.
- 02** Отсутствие единого централизованного инструмента проверки УКЭП.
- 03** Неопределенность статуса УКЭП, подтверждающего его юридическую значимость.
- 04** Разбор расхождений в результатах проверки УКЭП.

Спорные сценарии проверок УКЭП:



Сертификат - **действителен**
Ключ ЭП - **истёк**
Метки времени - **нет**



Сертификат - **истёк**
Ключ ЭП - **истёк**
Метка времени - **есть**



Сертификат - **истёк**
Метка времени - **нет**



УКЭП В МЧД – ГОЛОВНАЯ БОЛЬ



01

ОСОБЕННОСТИ МЧД:

- МЧД выпускается ~ на 3-5 лет.
- Срок УКЭП (МЧД) ~1 год.
- Истечение УКЭП не аннулирует МЧД.
- ФНС выдала >7 млн УКЭП ЮЛ/ИП за 2 года.

02

ПРОБЛЕМЫ:

- истек сертификат УКЭП в МЧД;
- средство ЭП - подпись недействительна;
- не возможно подтвердить юридическую значимость УКЭП (МЧД)
- не возможно подтвердить результат проверки УКЭП для работы с МЧД (р.2 ПП РФ №223).

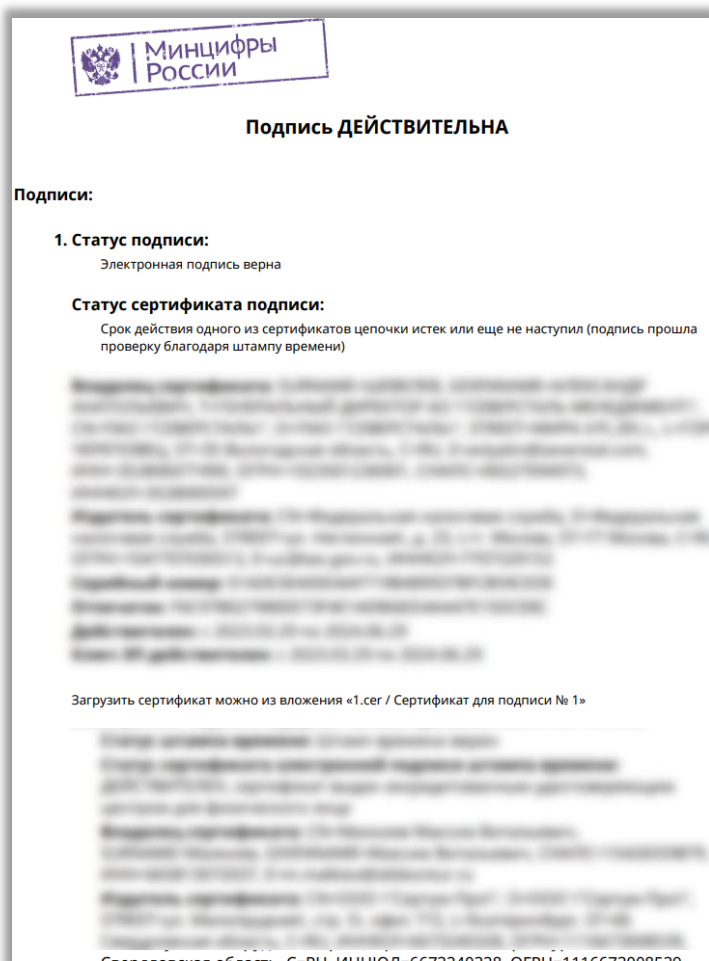
03

ВАРИАНТЫ РЕШЕНИЯ:

1. Проверять на момент действия УКЭП и фиксировать результат проверки протоколом.
2. При истечении срока действия УКЭП (МЧД) - использовать протокол успешной проверки для дальнейших заключений сделок
3. При истечении срока действия УКЭП (МЧД) - переподписать УКЭП под МЧД с меткой времени (негатив, потеря клиента).
4. Проверять МЧД на портале УФО с фиксацией результата проверки.



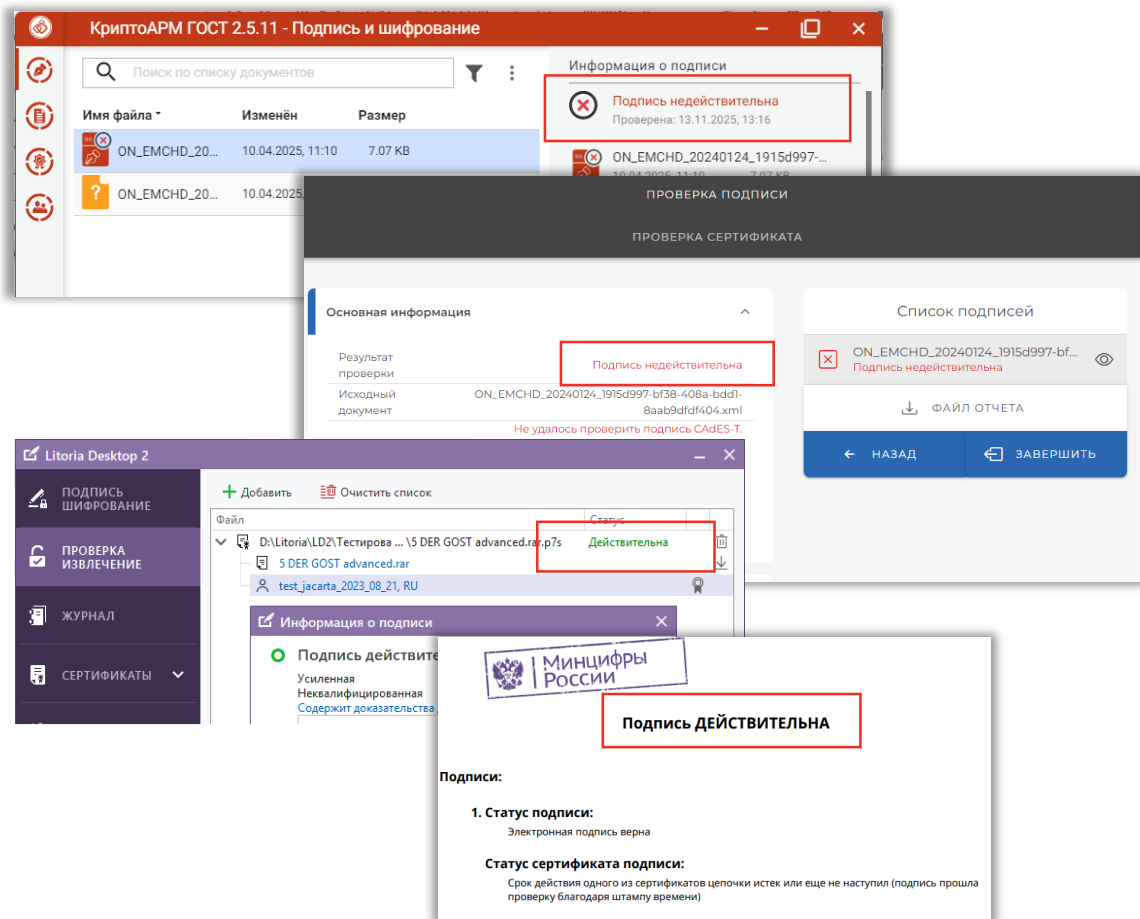
ПРОТОКОЛ ПРОВЕРКИ УКЭП



ПРЕИМУЩЕСТВА:

1. Подтверждает факт проверки УКЭП.
2. Закрепляет правомерность принятых решений.
3. Сокращает время для экспертной оценки УКЭП.
4. Сокращает риски приема документа при истечении УКЭП.
5. Документальное подтверждение в суде.

ОЖИДАНИЯ УЧАСТНИКОВ:



УЧАСТНИКУ НУЖЕН:

1. Результат проверки УКЭП:

- действительна
- недействительна

2. Подтверждение проверки УКЭП:

- протокол проверки подписи.



ВЫВОДЫ И ПРЕДЛОЖЕНИЯ



01

Отсутствие готовых решений проверок УКЭП под ключ

Решение:

- Бизнесу потребуется внедрять собственные инструменты проверок УКЭП, в том числе проведения оценки влияния СКЗИ.
- АУЦ/ДТС предлагается развивать публичные (доступные) сервисы с моментальным получением результата.
- Вендорам предлагается внедрять новые инструменты проверок.

02

Широкое распространение УКЭП без меток времени

Решение:

- Повышение осведомлённости, формирование культуры и новых привычек.
- Минимизация риска через формирование протокола проверки УКЭП.

03

Наличие расхождения в результатах проверки ЭП

Решение:

- Формирование единого доверия к инструментам проверкам ЭП.



СПАСИБО ЗА ВНИМАНИЕ

конференция
РусКрипто

Алексей Иванов

**Управление
криптографической защиты**

Альфа Банк

+7 (926) 531-55-05
iaa@alfabank.ru

