GIS ГАЗИНФОРМ СЕРВИС

конференция РусКрипто

18-21 марта 2025 г.
Солнечногорск

Правильная проверка электронной подписи, в том числе иностранной и архивной

Кирюшкин Сергей Анатольевич, к.т.н.
Советник генерального директора – начальник удостоверяющего центра
ООО “Газинформсервис”
kiryushkin-s@gaz-is.ru
www.gaz-is.ru

Рассматриваемые вопросы:

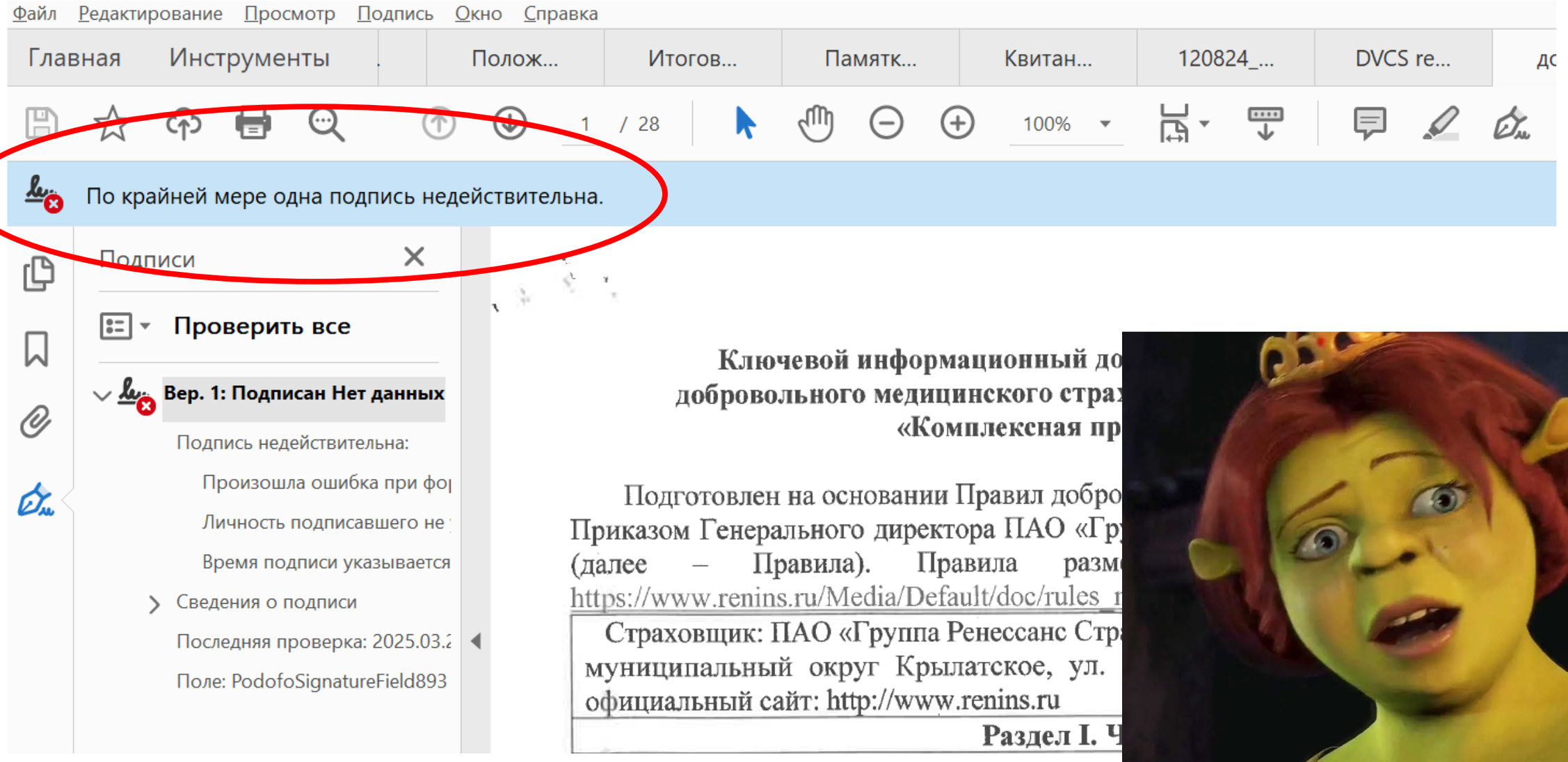
1. Кому нужна правильная проверка подписи?
2. Проверка архивной электронной подписи
3. Проверка иностранной подписи
4. Требования реального заказчика к процедуре проверки подписи

GIS ГАЗИНФОРМ СЕРВИС

Как мне правильно проверить электронную подпись?

GIS ГАЗИНФОРМ СЕРВИС

Качество и надежность проверки электронной подписи



GIS ГАЗИНФОРМ СЕРВИС

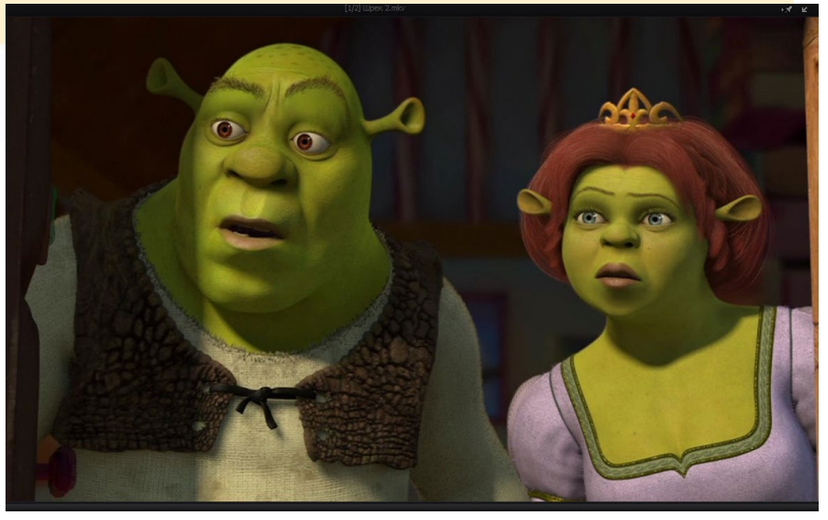
Качество и надежность проверки электронной подписи

Проверка квалифицированной ЭП | Проверка УНЭП | Проверка сертификата

‹ Назад

Отчет о проверке квалифицированной электронной подписи

java.lang.RuntimeException: Ошибка при выводе очередной строки для PDF-документа



GIS ГАЗИНФОРМ СЕРВИС

Качество и надежность проверки электронной подписи

Подпись ДЕЙСТВИТЕЛЬНА

Подписи:

1. Статус подписи: 0

Электронная подпись верна (CAdES-BES)

Статус сертификата подписи: 7

Один из сертификатов цепочки аннулирован

Проверка действительности цепочки квалифицированных сертификатов

Кто проверяет подпись согласно 63-ФЗ:

Согласно положениям 63-ФЗ проверку ЭП осуществляют три сущности:

1) средства электронной подписи (ст. 2, п.9);
2) удостоверяющий центр (ст.13 часть 1 п.9);
3) доверенная третья сторона (ст.2 п.17, ст. 18.1 часть 1)

Проверка ЭП в уполномоченной организации – Validation Authority ДТС

О "портале регулятора" или каких-то других порталах 63-ФЗ ничего не говорит.

Статья 11. Признание квалифицированной электронной подписи

Квалифицированная электронная подпись признается действительной до тех пор, пока решением суда не установлено иное, при одновременном соблюдении следующих условий:

Что надо проверить, при проверке ЭП?

1) квалифицированный сертификат создан и выдан аккредитованным удостоверяющим центром, аккредитация которого действительна на день выдачи указанного сертификата;

Доверие к TSL

e-trust.gosuslugi.ru/check/sign

Gmail YouTube Карты DeepL Translate – С... Новая вкладка

госуслуги

Портал уполномоченного федерального органа в сфере использования электронной подписи

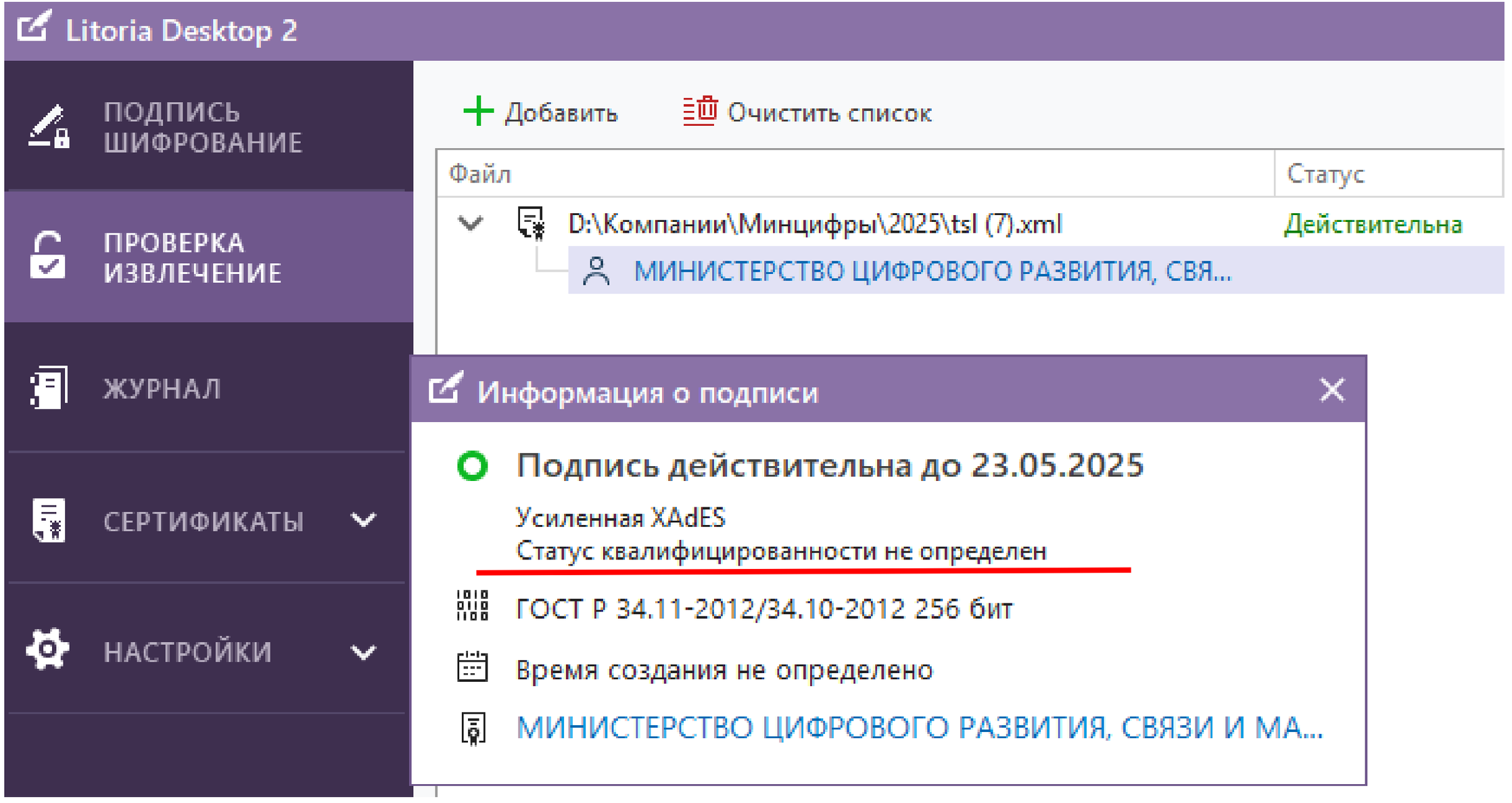
Портал предоставляет сервисы проверки электронной подписи (ЭП) и машиночитаемой доверенности (МЧД), получения реестра аккредитованных удостоверяющих центров (АУЦ) и корневых сертификатов головного удостоверяющего центра (ГУЦ)

Скачать TSL

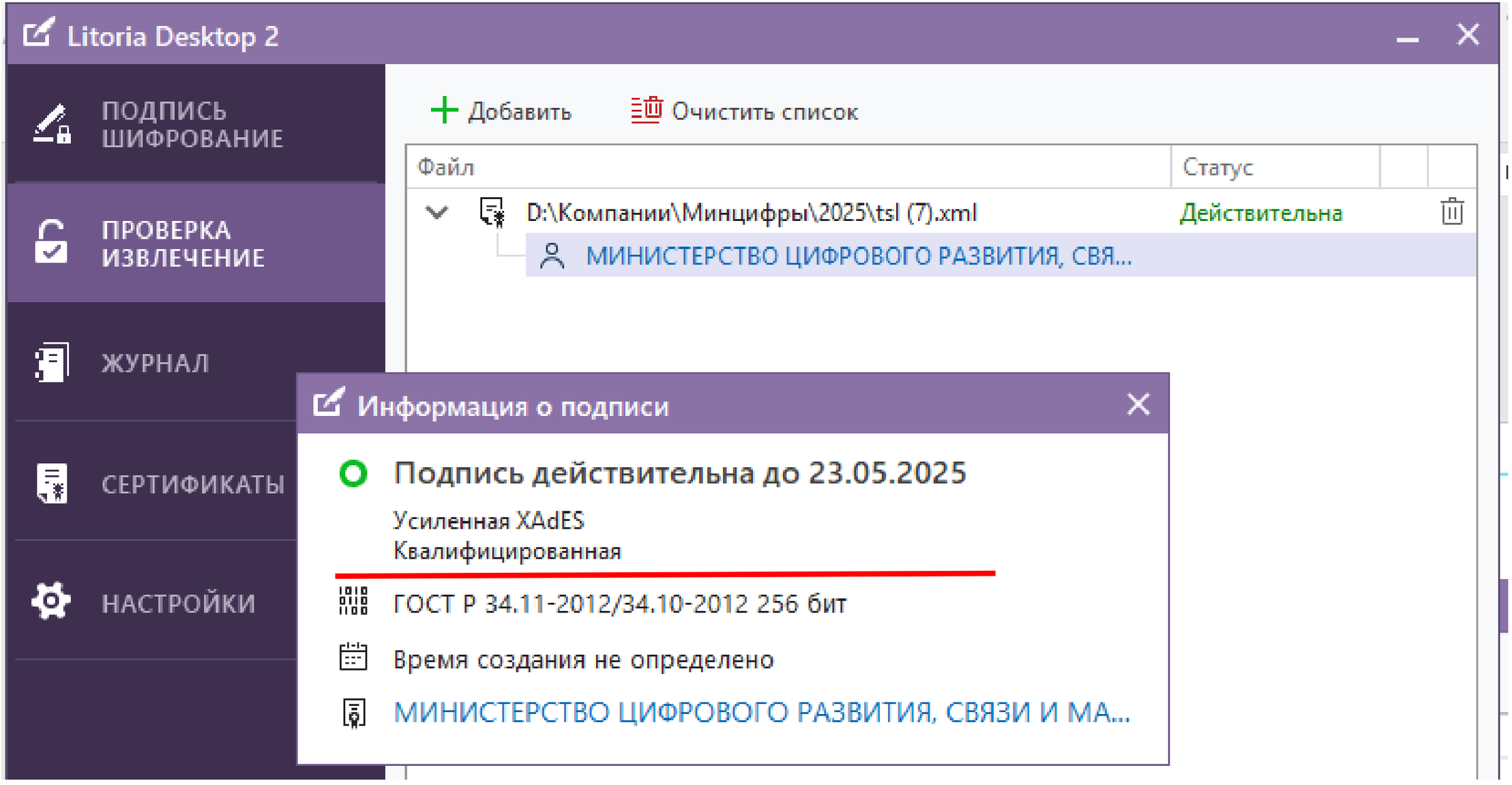
Проверка ЭП | Проверка МЧД | Реестры | Мониторинг АУЦ

Проверка квалифицированной ЭП | Проверка УНЭП | Проверка сертификата

Доверие к TSL



Доверие к TSL



Что надо проверить, при проверке ЭП?

2) квалифицированный сертификат действителен на момент подписания электронного документа (при наличии достоверной информации о моменте подписания электронного документа) или на день проверки действительности указанного сертификата, если момент подписания электронного документа не определен;

Public Key Interoperability Test Suite (PKITS) Certification Path Validation

RFC 5280
224 теста

GIS ГАЗИНФОРМ СЕРВИС

Используете ли вы в своих системах ЭДО электронную подпись с меткой времени?

Ответили: 97 Пропустили: 0

ВАРИАНТЫ ОТВЕТА		ОТВЕТЫ	
Да, мы используем в системе электронного документооборота электронную подпись с меткой времени		13,40 %	13
Нет, не используем. Знаем о метке времени, но ее применение не обязательно.		15,46 %	15
Нет, не используем. Знаем о метке времени, но это усложняет систему		6,19 %	6
Хотели бы использовать, но не знаем, как это реализовать		12,37 %	12
Я не знаю, используем ли мы метку времени		46,39 %	45
Другое (укажите)	Ответы	6,19 %	6
ВСЕГО			97

Опрос Елены Ткаченко, руководителя экспертного совета «Электронные документы – эффективная экономика»

Требования к атрибутам поля Subject. stateOrProvinceName, localityName, streetAddress

stateOrProvinceName (наименование штата или области)

Приказ ФСБ России № 795: «В качестве значения данного атрибута имени следует использовать текстовую строку, содержащую наименование соответствующего субъекта Российской Федерации»

Приложение N 2
к Требованиям (п. 32)

Список изменяющих документов
(в ред. Приказа ФСБ России от 29.01.2021 N 31)

ОБЩИЙ ВИД КВАЛИФИЦИРОВАННОГО СЕРТИФИКАТА
НА БУМАЖНОМ НОСИТЕЛЕ ДЛЯ ВЛАДЕЛЬЦА - ЮРИДИЧЕСКОГО ЛИЦА

```
Номер квалифицированного сертификата: <serialNumber>
Действие квалифицированного сертификата: с <notBefore>
                                          по <notAfter>

        Сведения о владельце квалифицированного сертификата

Наименование юридического лица: <commonName>
Основной государственный регистрационный номер: <OGRN>
Идентификационный номер налогоплательщика: <INNLE>
Место нахождения юридического лица: <countryName>,
<stateOrProvinceName>, <localityName>, <streetAddress>
* Уполномоченный представитель юридического лица: <title> <surname>
<givenName>
Тип идентификации при выдаче сертификата: <identificationKind>
```

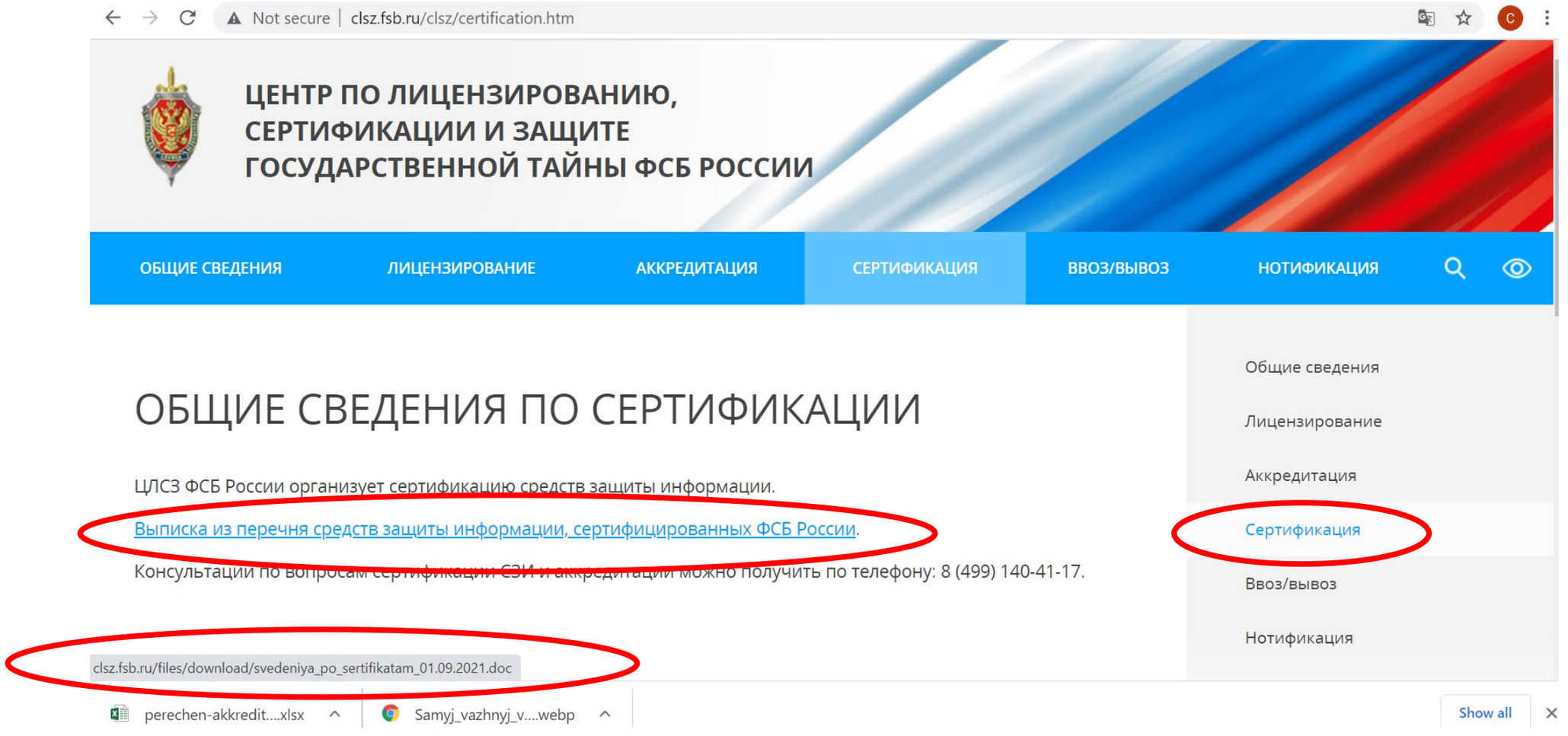
Что надо проверить, при проверке ЭП?

2.1) срок действия ключа электронной подписи, указанный в квалифицированном сертификате в соответствии с пунктом 9 части 2 статьи 17 настоящего Федерального закона, не истек на момент подписания электронного документа (при наличии достоверной информации о моменте подписания электронного документа) или на день проверки квалифицированной электронной подписи, созданной с использованием данного ключа электронной подписи, если момент подписания электронного документа не определен;

Что надо проверить, при проверке ЭП?

3) имеется положительный результат проверки принадлежности владельцу квалифицированного сертификата квалифицированной электронной подписи, с помощью которой подписан электронный документ, и подтверждено отсутствие изменений, внесенных в этот документ после его подписания. **При этом проверка осуществляется с использованием средств электронной подписи, имеющих подтверждение соответствия требованиям, установленным в соответствии с настоящим Федеральным законом,** и с использованием квалифицированного сертификата лица, подписавшего электронный документ

Что надо проверить, при проверке ЭП?

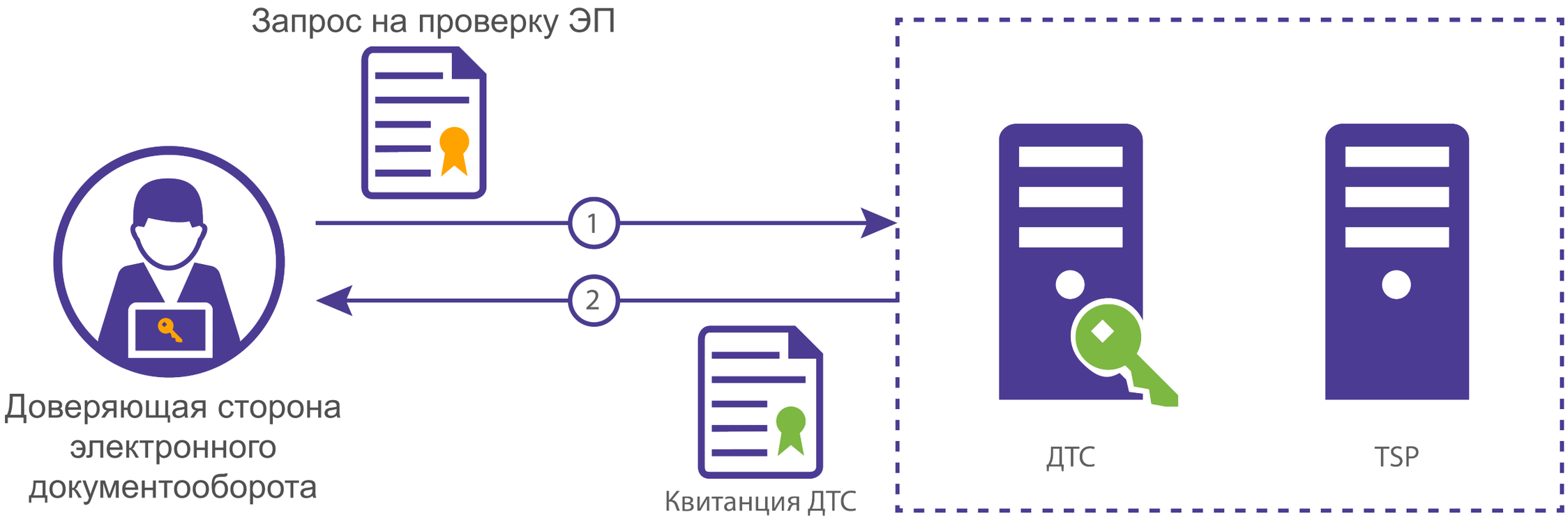


Статья 18.1. Доверенная третья сторона

1. Доверенная третья сторона оказывает услуги:

1. **по подтверждению действительности электронных подписей**, используемых при подписании электронного документа, в том числе установлению **фактов того, что соответствующие сертификаты действительны на определенный момент времени**, созданы и выданы аккредитованными удостоверяющими центрами, аккредитация которых действительна на день выдачи этих сертификатов;
2. **по проверке соответствия** всех квалифицированных сертификатов, используемых при подписании электронного документа, **требованиям, установленным настоящим Федеральным законом** и иными принимаемыми в соответствии с ним нормативными правовыми актами;
3. по **проверке полномочий участников** электронного взаимодействия;
4. **по созданию и подписанию** квалифицированной электронной подписью доверенной третьей стороны **квитанции с результатом проверки** квалифицированной электронной подписи в электронном документе с достоверной информацией о моменте ее подписания;
5. **по хранению данных, в том числе документированию выполняемых доверенной третьей стороной операций.**

Правильная проверка подписи в Validation Authority ДТС



GIS ГАЗИНФОРМ СЕРВИС

Дополнительные материалы:

Особенности проверки цепочки сертификатов в соответствии с требованиями руководящих документов

Екатерина Ермина, ведущий инженер, Газинформсервис

Выступление на PKI-Форуме в 2022 году

https://pki-forum.ru/files/files/5_4_Eremina.pdf

GIS ГАЗИНФОРМ СЕРВИС

Нормативное регулирование в области архивного хранения ЭД

Законопроект

№ 1173189-7

О внесении изменений в Федеральный закон "Об информации, информационных технологиях и о защите информации" и отдельные законодательные акты Российской Федерации
(в части использования и хранения электронных документов)

Рассмотрение Советом Государственной Думы законопроекта, представленного ответственным комитетом

21.02.2022 — исключить комитет из числа соисполнителей (Комитет Государственной Думы по труду, социальной политике и делам ветеранов)

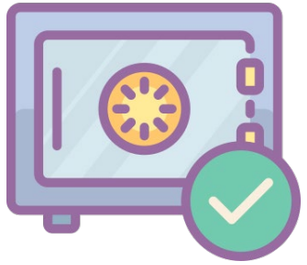
04.04.2022 — внести законопроект на рассмотрение Государственной Думы (06.04.2022)

Рассмотрение законопроекта Государственной Думой

06.04.2022 — принять законопроект в первом чтении; представить поправки к законопроекту (Срок представления поправок в тридцатидневный срок со дня принятия постановления; 05.05.2022)

GIS ГАЗИНФОРМ СЕРВИС

Подходы к обеспечению свойств целостности, аутентичности и юридической значимости ЭД при длительном хранении



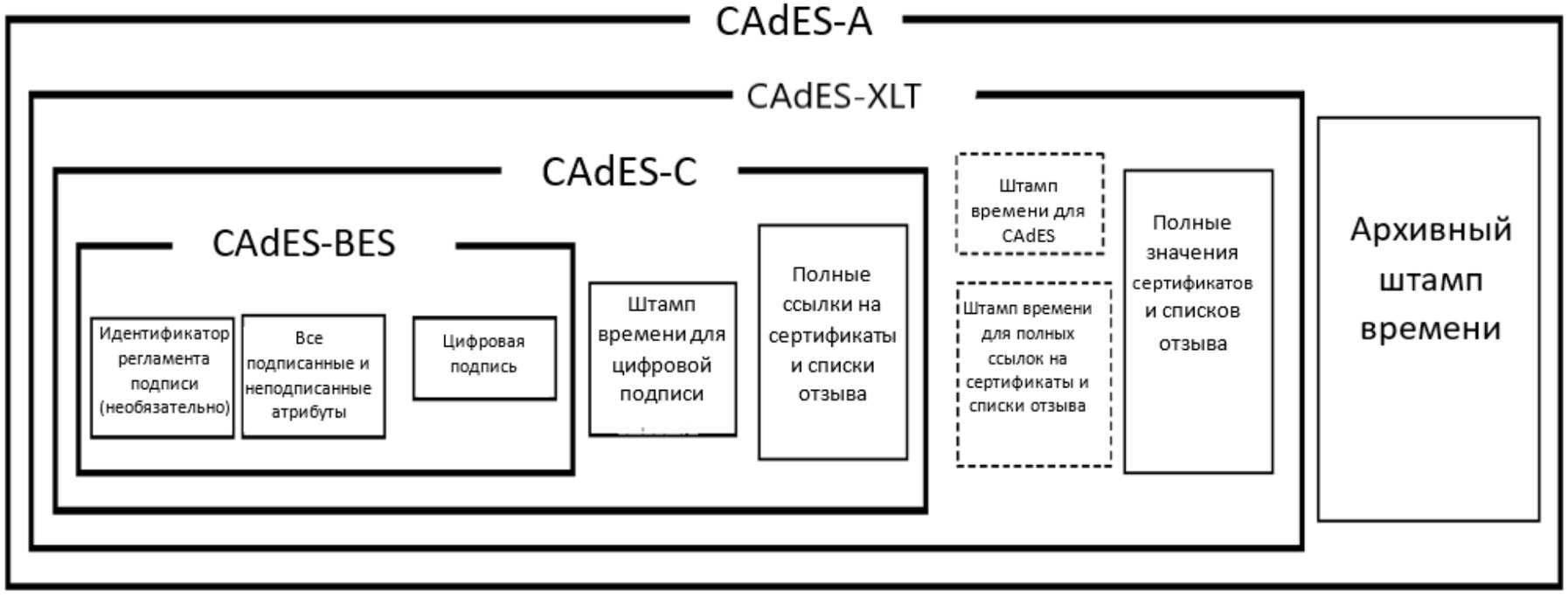
I. Игнорирование первичной ЭП и обеспечение свойств ЭД на уровне всего архива;

II. Использование архивных форматов ЭД с ЭП

III. Использование сервиса валидации электронной подписи

Использование архивных форматов ЭД на примере CAdES

ЭП в формате CAdES-BES преобразуется до формата CAdES-XLT (усовершенствованная ЭП) **путем расширения содержания атрибутов**: штампы времени, доказательства событий проверки всех ЭП и сертификатов из цепочки сертификации



ЭП остаётся верна до тех пор, пока действителен СКП ЭП сервиса штампов времени. Затем ЭП преобразовывается в архивную ЭП формата CADES-A

GIS ГАЗИНФОРМ СЕРВИС

Дополнительные материалы:

PKI-Форум 2024, **Сессия 5.**
Электронные архивы с ЭП. Усовершенствованные форматы ЭП

https://vkvideo.ru/video-212085506_456239282?ref_domain=pki-forum.ru

GIS ГАЗИНФОРМ СЕРВИС

Проверка иностранной ЭП средствами, встроенными в Adobe Acrobat

По крайней мере одна подпись недействительна.

Панель "Подпись"

文件ID: SHCAfdaebd9dfe0e473a80b847282f1a4189
企业名称：上海市数字证书认证中心有限公司
企业统一社会信用代码：91310000631291289X
签署时间：2024年09月18日 12时20分

经办人姓名：刘锟

AGREEMENT № 10674/IAC on the procedure for interaction during mutual validation of electronic signatures	**СОГЛАШЕНИЕ № 10674/ИАС о порядке взаимодействия при взаимной проверке электронной подписи**
St. Petersburg, Shanghai “___” _____ 2024	Санкт-Петербург, Шанхай «___» _____ 2024 г.

GIS ГАЗИНФОРМ СЕРВИС

Проверка иностранной ЭП средствами Validation Authority ДТС

Детальная информация о сертификате 1

Статус проверки электронной подписи: ДЕЙСТВИТЕЛЬНА

Сертификат ключа проверки электронной подписи:

刘镪

Издатель
SHECA G2

Алгоритм открытого ключа
RSA

Серийный номер
24E16955FACF5C0375786CE5EAF7031A

Время действия
18 сентября 2024 г. 2:18:07 UTC по 18 сентября 2025 г. 15:59:59 UTC

Комментарий к подписи: Нет комментария

Тип подписи подробно: Усиленная, Неквалифицированная, PAdES

Время создания: 18 сентября 2024 г. 4:19:31 UTC

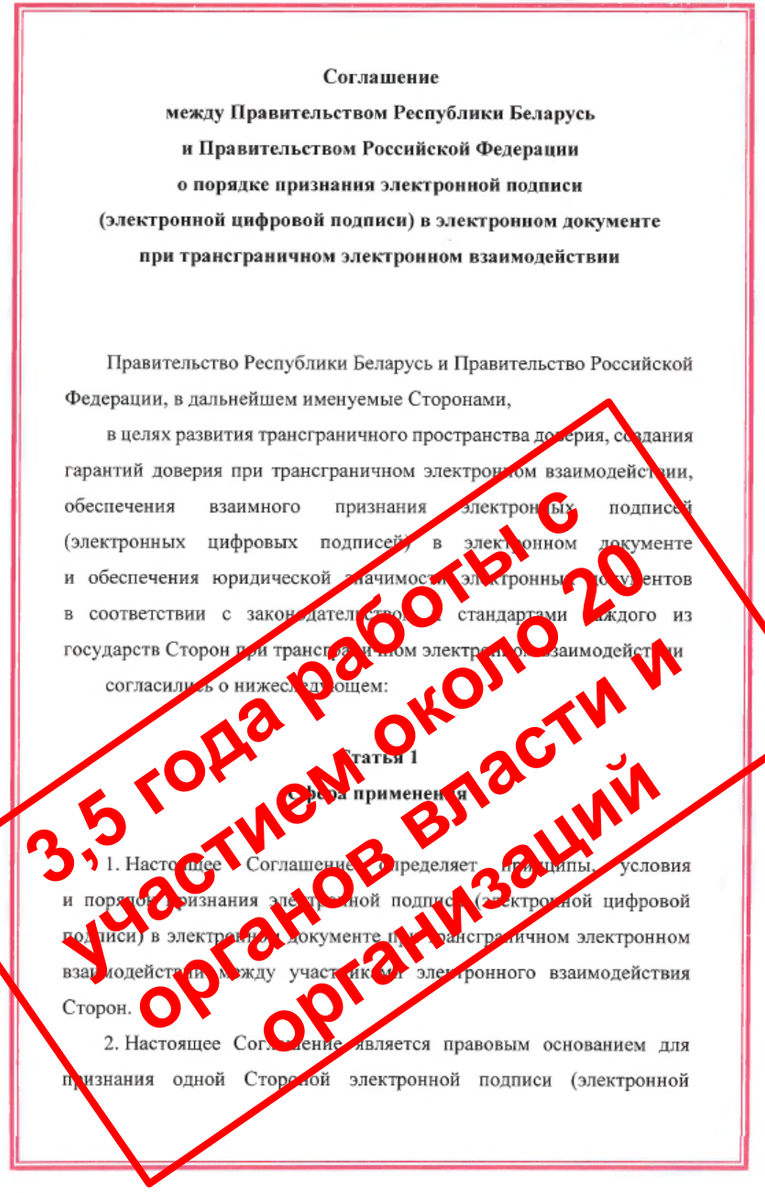
GIS ГАЗИНФОРМ СЕРВИС

Правовая основа признания иностранных ЭП

Армения Об электронном документе и ЭЦП от 14.12.2004 ст.15	**Беларусь** Закон от 28.12.2009 113-З, ст. 30	**Казахстан** Закон РК от 07.01.2003 года N 370, ст. 13	**Кыргызстан** Закон КР от 19.07.2017 № 128 ст. 7, 13 ч.1 п.9, ч.9	**Россия** ФЗ №63-ФЗ от 06.04.2011, ст. 7	**Узбекистан** ЗРУ №793, от 12.10.22, ст.28
Международный договор	Международный договор			Международный договор	Международный договор
	Признание иностранного сертификата открытого ключа ДТС	Установление отношений доверия с иностранным УЦ или иностранной ДТС	Договор между участниками взаимодействия	Соглашение между участниками взаимодействия	Подтверждение подлинности иностранной ЭЦП ДТС

GIS ГАЗИНФОРМ СЕРВИС

Прецедент международного договора о ВПИЭП



Соглашение
между Правительством Республики Беларусь
и Правительством Российской Федерации
о порядке признания электронной подписи
(электронной цифровой подписи) в электронном документе
при трансграничном электронном взаимодействии

Правительство Республики Беларусь и Правительство Российской Федерации, в дальнейшем именуемые Сторонами,

в целях развития трансграничного пространства доверия, создания гарантий доверия при трансграничном электронном взаимодействии, обеспечения взаимного признания электронных подписей (электронных цифровых подписей) в электронном документе и обеспечения юридической значимости электронных документов в соответствии с законодательством и стандартами каждого из государств Сторон при трансграничном электронном взаимодействии

согласились о нижеследующем:

Статья 1

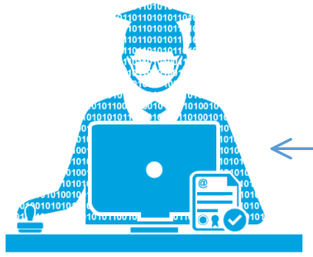
Сфера применения

1. Настоящее Соглашение определяет принципы, условия и порядок признания электронной подписи (электронной цифровой подписи) в электронном документе при трансграничном электронном взаимодействии между участниками электронного взаимодействия Сторон.

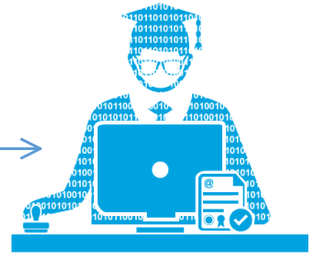
2. Настоящее Соглашение является правовым основанием для признания одной Стороной электронной подписи (электронной

3,5 года работы с участием около 20 органов власти и организаций

На основе соглашения между участниками



Соглашение о взаимодействии ДТС **(СВДТС)**



АДТС (СПЭП АУЦ)

Договор на услуги ДТС (СПЭП АУЦ) **(ДУ)**

АДТС (СПЭП АУЦ)

Договор на услуги ДТС (СПЭП АУЦ) **(ДУ)**

1) ДУ должен в описании услуги должен содержать формулировку, что осуществляется проверка на соответствие условий СВП.
2) При этом СВП заключается между неограниченным количеством участников, оперативно. А ДУ может быть заключен ранее, для любого взаимодействия.
3) Логично в ДУ указать, что он распространяется только на взаимодействие, которое описывает порядок признания, в соответствии с ДУ.
4) Тогда в СВП нужно будет указать формулировку, что порядок признания в соответствии с ДУ № ___ от_____

Конечный пользователь

Соглашение о взаимном признании ЭЦП (ЭП) **(СВП)**

Конечный пользователь

GIS ГАЗИНФОРМ СЕРВИС

С какими странами реализуем этот подх

Организация Объединенных Наций

Комиссия Организации Объединенных Наций по праву международной торговли

Комиссия Организации Объединенных Наций по праву международной торговли

Типовой закон ЮНСИТРАЛ об электронных подписях (2001 год)

Дата принятия: 5 июля 2001 года

Цель

Типовой закон об электронных подписях (ТЗЭП) имеет целью сделать возможным и облегчить

Дополнительные ресурсы

- Текст

Типовой закон UNCITRAL об ЭП (MLES)

Статья 12. Признание иностранных сертификатов и электронных подписей

1. Страна выдачи сертификата ЭП, страна подписания ЭД **не влияют на юридическую силу ЭП;**

2, 3. Иностранный сертификат и ЭП равнозначны отечественному, **если обеспечивают эквивалентный уровень надежности (ЭУН)**;

4. При определении ЭУН следует учитывать международные стандарты и любые другие соответствующие факторы;

5. Независимо от п.п.2,3,4, если стороны договорились, этого достаточно для трансграничного признания

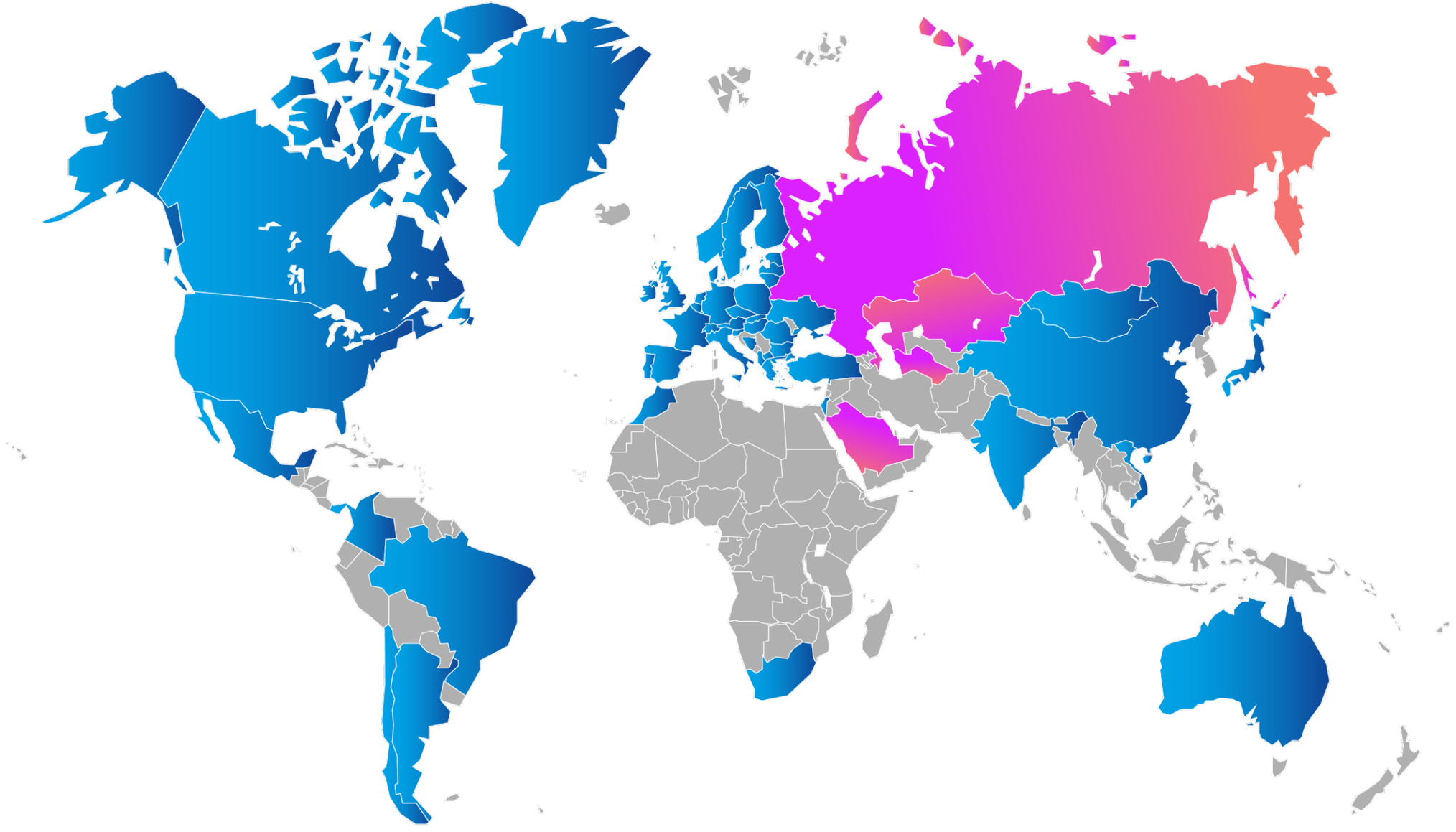
GIS ГАЗИНФОРМ СЕРВИС

Страны с MLES-подобным законодательством

1.	Австралия	19.	Грузия	37.	Люксембург	55.	Таиланд
2.	Австрия	20.	Дания	38.	Макао	56.	Таджикистан
3.	Азербайджан	21.	Израиль	39.	Малайзия	57.	Тайвань
4.	Алжир	22.	Индия	40.	Мальта	58.	Туркменистан
5.	Аргентина	23.	Индонезия	41.	Мексика	59.	Турция
6.	Армения	24.	Иран	42.	Монголия	60.	Узбекистан
7.	Бангладеш	25.	Ирландия	43.	Молдавия	61.	Украина
8.	Беларусь	26.	Испания	44.	Нидерланды	62.	Филиппины
9.	Бельгия	27.	Италия	45.	Норвегия	63.	Финляндия
10.	Бермудские острова	28.	Казахстан	46.	Перу	64.	Франция
11.	Болгария	29.	Канада	47.	Польша	65.	Хорватия
12.	Бразилия	30.	Кипр	48.	Португалия	66.	Чехия
13.	Великобритания	31.	Киргизия	49.	Россия	67.	Чили
14.	Венгрия	32.	КНР	50.	Румыния	68.	Швейцария
15.	Вьетнам	33.	Колумбия	51.	Сингапур	69.	Швеция
16.	Германия	34.	Корея	52.	Словакия	70.	Эстония
17.	Греция	35.	Латвия	53.	Словения	71.	ЮАР
18.	Гонконг	36.	Литва	54.	США	72.	Япония

GIS ГАЗИНФОРМ СЕРВИС

Страны с MLES-подобным законодательством



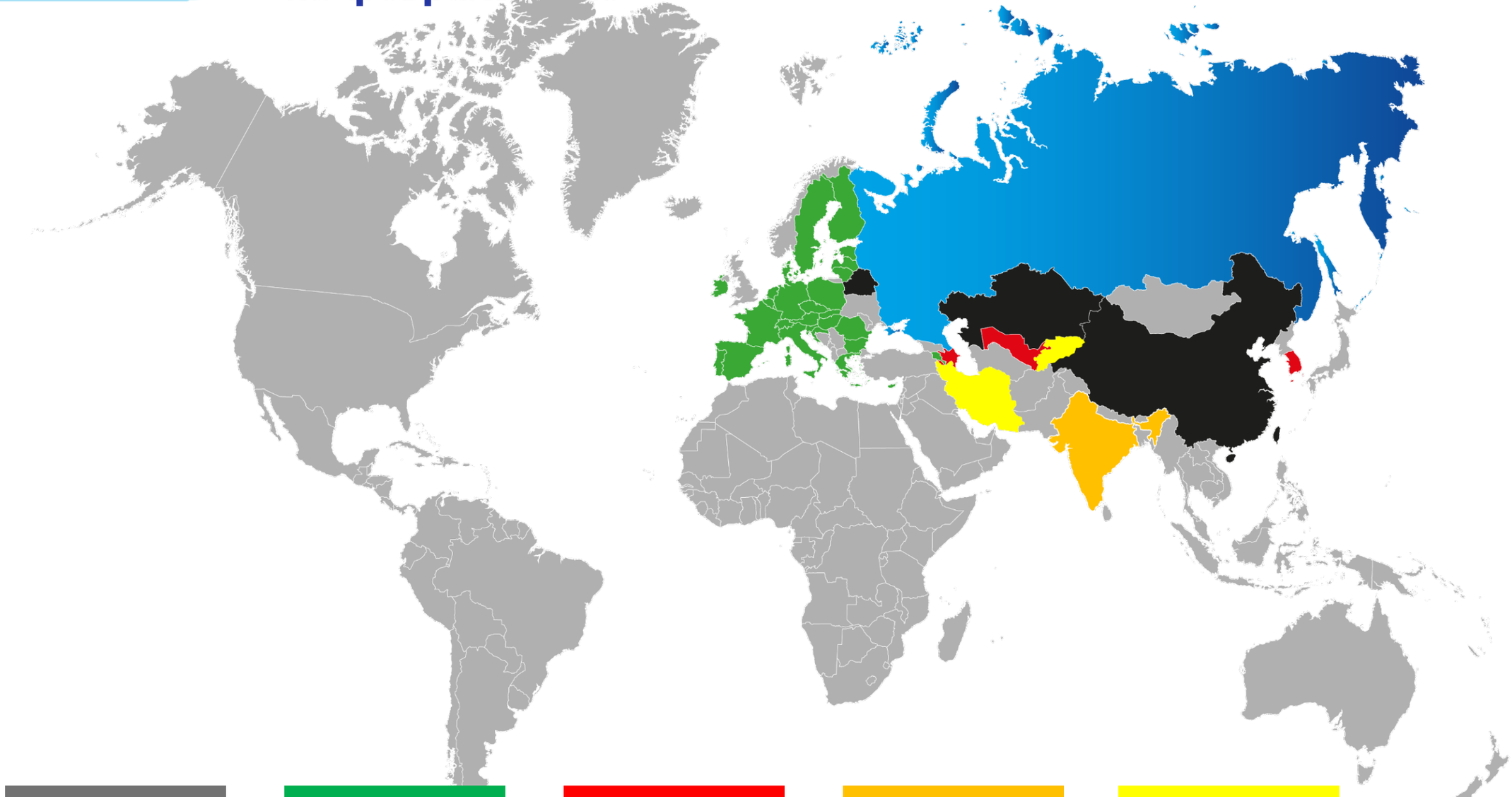
GIS ГАЗИНФОРМ СЕРВИС

Карта трансграничного пространства доверия (ТПД) уровня B2B РФ на февраль 2025

№	Фаза развития ТПД между РФ и	Описание фазы	Условная нумерация фаз
1.	Беларусью	Промышленная эксплуатация	1
2.	Казахстаном	Промышленная эксплуатация	1
3.	Китаем	Промышленная эксплуатация	1
4.	Арменией	Пилотный проект	3
5.	ЕС	Пилотные проекты	3
6.	Азербайджаном	Тестирование	4
7.	Республикой Корея	Тестирование	4
8.	Узбекистаном	Тестирование	4
9.	Индией	Подготовка к тестированию	5
10.	Кыргызстаном	Переговоры	6
11.	Ираном	Переговоры	6

GIS ГАЗИНФОРМ СЕРВИС

Карта трансграничного пространства доверия (ТПД) уровня B2B РФ на февраль 2025



GIS ГАЗИНФОРМ СЕРВИС

Дополнительные материалы:

PKI-Форум 2024, **Сессия 2.**
Трансграничное признание иностранной ЭП

https://vkvideo.ru/video-212085506_456239279?ref_domain=pki-forum.ru

GIS ГАЗИНФОРМ СЕРВИС

Требования реальных клиентов к любому сервису доверия, в том числе – Validation Authority ДТС

1. понятно, что конкретно "под капотом" у оператора сервиса
2. в соответствии с какими требованиями выполняется проверка
3. SLA
4. ясность и однозначность результата проверки (в т.ч. квитанция соответствует потребностям Заказчика)
5. реализация возможности дополнительных проверок
6. возмещения ущерба при ошибках 1 и 2 рода
7. государственный контроль оператора сервиса
8. *независимый аудит оператора сервиса*

конференция РусКрипто

18-21 марта 2025 г.
Солнечногорск

GIS ГАЗИНФОРМ СЕРВИС

Спасибо за внимание!

Кирюшкин Сергей Анатольевич, к.т.н.
Советник генерального директора – начальник удостоверяющего центра
ООО “Газинформсервис”
kiryushkin-s@gaz-is.ru
www.gaz-is.ru