



*Конвергенция единого окна и
трансграничного пространства
доверия - технологическая основа
глобальных цепочек поставок*

Кирюшкин Сергей Анатольевич
ООО "Газинформсервис"
Kiryushkin-S@gaz-is.ru

» Что хотелось бы обсудить:

1

ТПД: какие успехи?

2

ТПД и единое окно: точки конвергенции

3

Мировой опыт ТПД и ЕО и что из него следует

4

Инициатива “снизу”

» ЕО и ТПД: определения

- «Единое окно» (ЕО) определяется как механизм, позволяющий сторонам, участвующим в торговых и транспортных операциях, **представлять стандартизованную информацию и документы с использованием единого пропускного канала в целях выполнения всех регулирующих требований**, касающихся импорта, экспорта и транзита. Если информация имеет электронный формат, то отдельные элементы данных должны представляться только один раз.

СЕФАКТ ООН, РЕКОМЕНДАЦИЯ № 33 Создание «единого окна» для повышения эффективности обмена информацией между торговыми компаниями и государственными органами

» ЕО и ТПД: определения

- "трансграничное пространство доверия" - совокупность правовых, организационных и технических условий, согласованных государствами-членами **с целью обеспечения доверия при межгосударственном обмене данными и электронными документами между уполномоченными органами**

Протокол об информационно-коммуникационных технологиях и информационном взаимодействии в рамках Евразийского экономического союза, Приложение № 3 к Договору о Евразийском экономическом союзе.



Модель «покупка-перевозка-оплата» СЕФАКТ ООН



Перспективы ТПД

- | | | |
|--------------------|-----------------|------------------------|
| 1. Argentina | 21. Greece | 41. Philippines |
| 2. Armenia | 22. Hong Kong | 42. Poland |
| 3. Austria | 23. Hungary | 43. Portugal |
| 4. Azerbaijan | 24. India | 44. Republic of Cyprus |
| 5. Belarus | 25. Indonesia | 45. Republic of Korea |
| 6. Belgium | 26. Ireland | 46. Romania |
| 7. Bermuda | 27. Israel | 47. Russian Federation |
| 8. Brazil | 28. Italy | 48. Singapore |
| 9. Bulgaria | 29. Japan | 49. Slovakia |
| 10. Chile | 30. Kazakhstan | 50. Slovenia |
| 11. China | 31. Kyrgyzstan | 51. South Africa |
| 12. Colombia | 32. Latvia | 52. Spain |
| 13. Croatia | 33. Lithuania | 53. Sweden |
| 14. Czech Republic | 34. Luxembourg | 54. Switzerland |
| 15. Denmark | 35. Malaysia | 55. Taiwan |
| 16. Estonia | 36. Malta | 56. Turkey |
| 17. Finland | 37. Mexico | 57. United Kingdom |
| 18. France | 38. Netherlands | 58. Uzbekistan |
| 19. Georgia | 39. Norway | |
| 20. Germany | 40. Peru | |

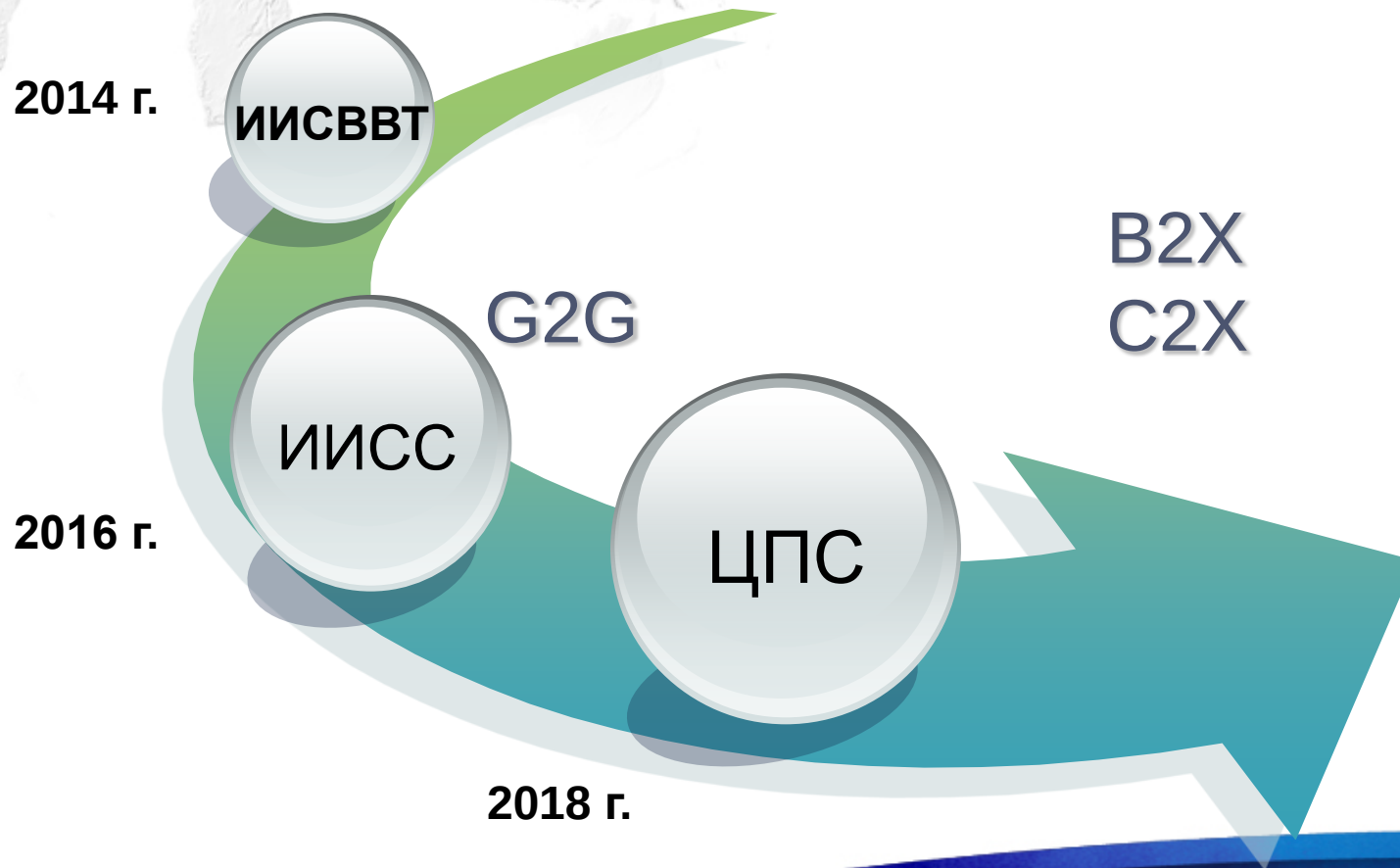
На основе:

- Общее руководство по законодательству в области ЭП: краткое изложение законодательства и исполнимости по странам/© Adobe Systems Incorporated 2016.
- Глобальный индекс кибербезопасности и профили по киберблагополучию. Отчет. Исследовательская группа ABI Reserch по заказу группы кибербезопасности МСЭ. Апрель 2015 г.

» Где и как ТПД работает практически



ТВД в ЕАЭС в рамках ИИСС



ТВД и ЕО в ЕС в проекте Реррол

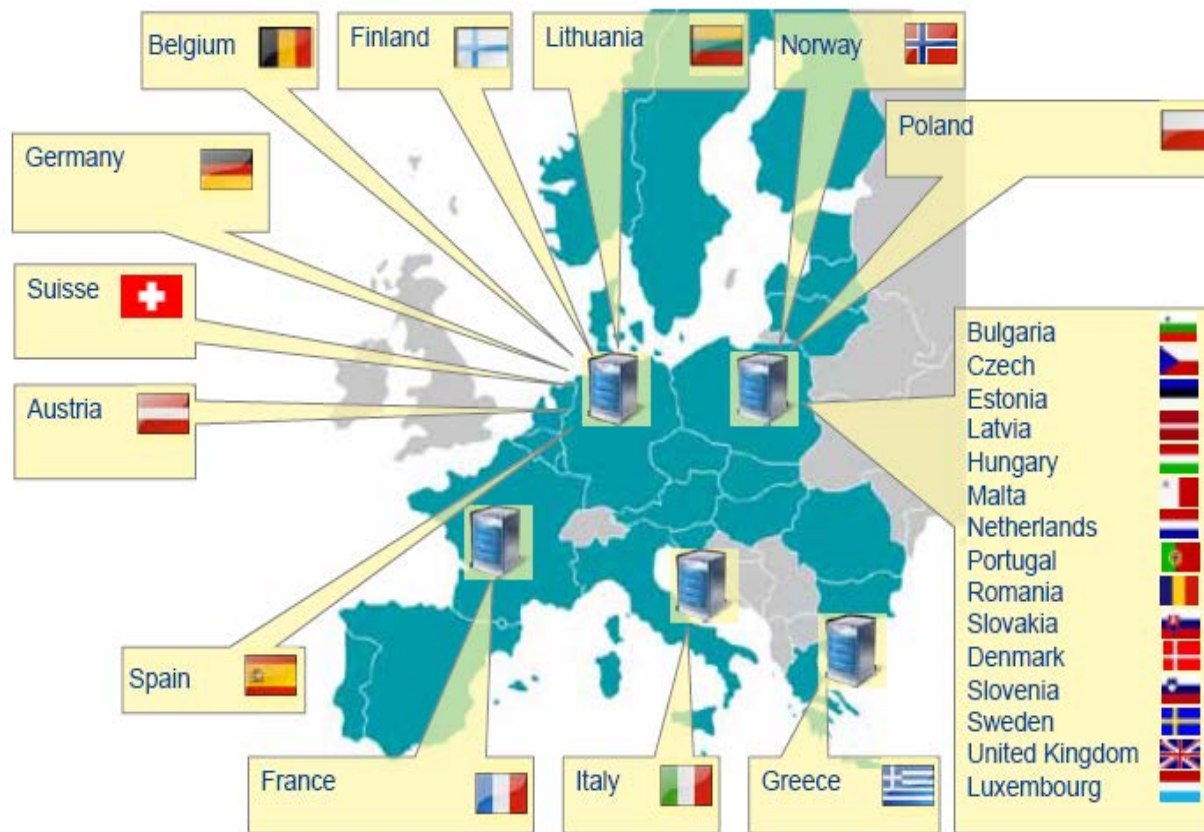


Figure 4: Full Coverage of PEPPOL e-signature Validation Infrastructure

ТПД и ЕО в ЕС в проекте Perpol



ТВД и ЕО в ЕС в проекте Perpol

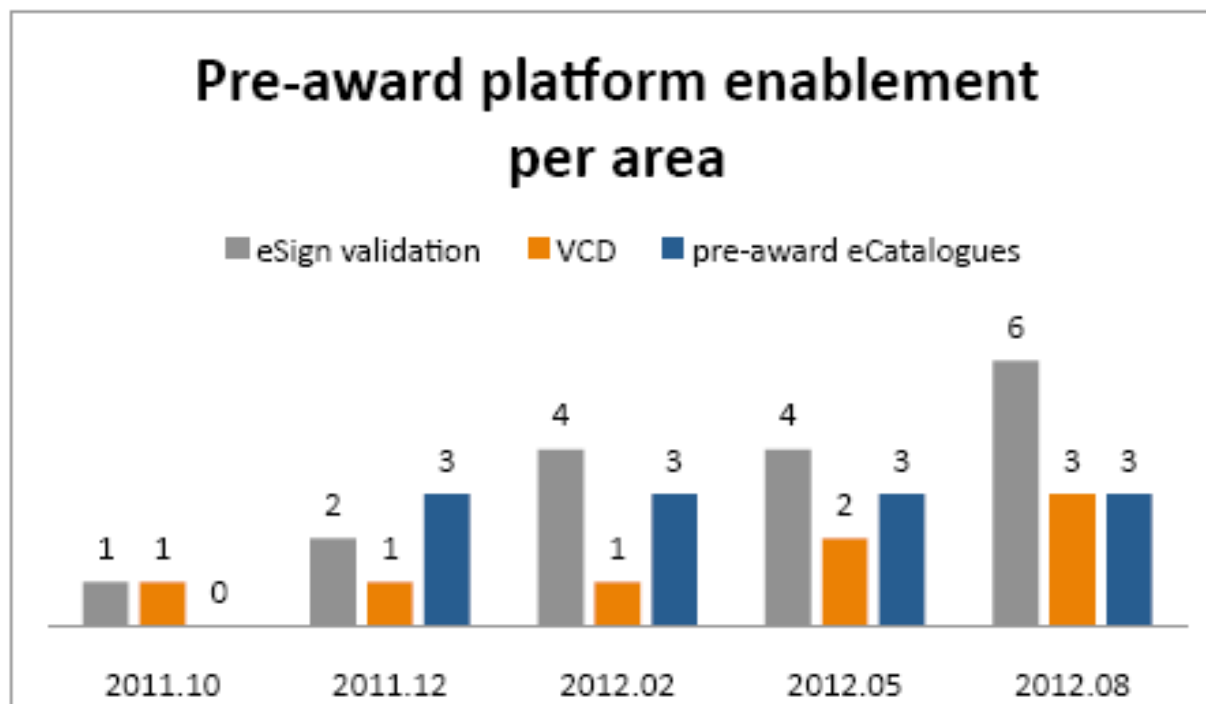


Figure 11: Pre-award platform enablement



FRAMEWORK AGREEMENT ON FACILITATION OF CROSS-BORDER PAPERLESS TRADE IN ASIA AND THE PACIFIC

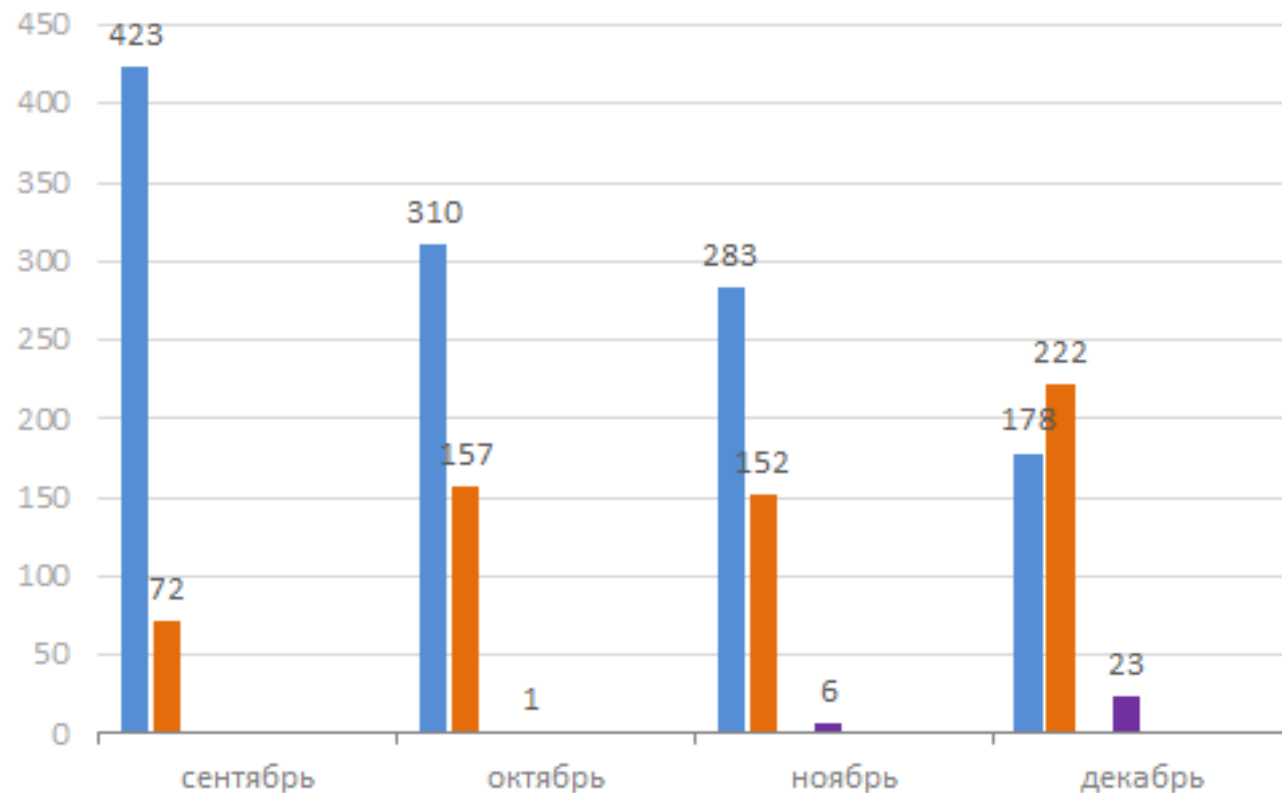
РАМОЧНОЕ СОГЛАШЕНИЕ ОБ УПРОЩЕНИИ ПРОЦЕДУР ТРАНСГРАНИЧНОЙ БЕЗБУМАЖНОЙ ТОРГОВЛИ В АЗИАТСКО- ТИХООКЕАНСКОМ РЕГИОНЕ

» ТПД и ЕО в ЭСКАТО ООН

Статья 1 Цель

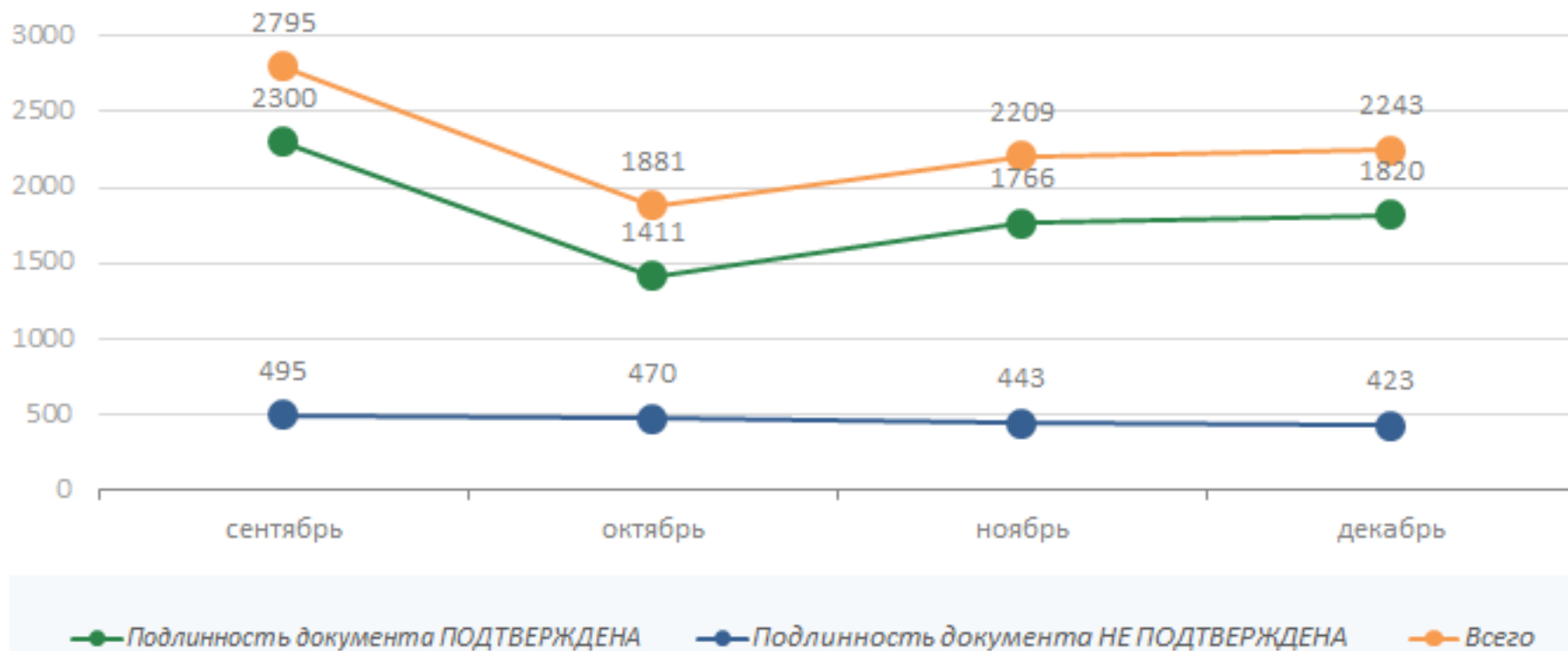
Целью настоящего рамочного соглашения является содействие развитию безбумажной трансграничной торговли посредством **создания условий для взаимного признания документов и данных о торговле в электронной форме** и обмена ими, а также посредством содействия повышению операционной совместимости национальных и субрегиональных систем «единого окна» и/или других систем безбумажной торговли в целях повышения эффективности и транспарентности международных торговых сделок и обеспечения более строгого соблюдения нормативных требований.

Результаты практической работы ДТС на корпоративной торговой площадке



- Просрочен сертификат
- Сертификат выпущен неквалифицированным УЦ
- Не настроено рабочее место
- Сертифика отозван по OCSP
- Время OCSP и TSP не синхронизировано
- Ошибка получения точек распространения OCSP
- Получение CRL недействителен по времени
- Подпись математически некорректна

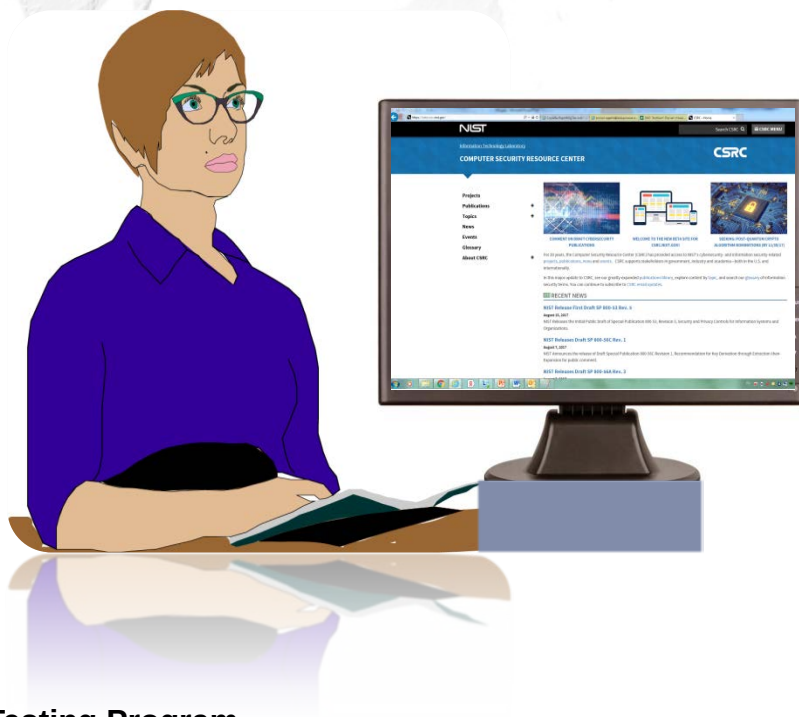
» Результаты практической работы ДТС на корпоративной торговой площадке





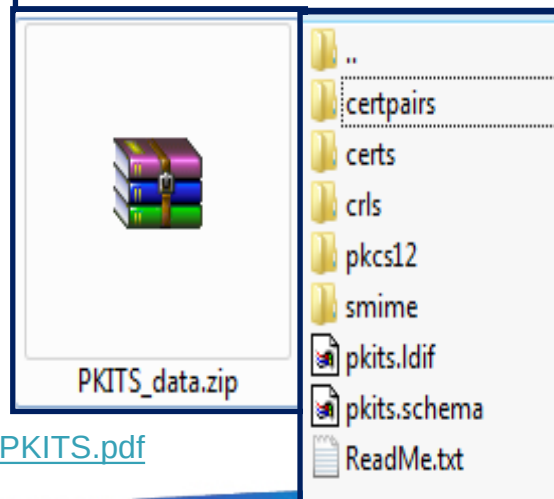
КЗИ, Суздаль 2018

Соответствие средств ЭП 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



Соответствие средств ЭП международным рекомендациям

4 Certification Path Validation Tests.....
4.1 Signature Verification.....
4.2 Validity Periods.....
4.3 Verifying Name Chaining.....
4.4 Basic Certificate Revocation Tests.....
4.5 Verifying Paths with Self-Issued Certificates.....
4.6 Verifying Basic Constraints.....
4.7 Key Usage.....
4.8 Certificate Policies.....
4.9 Require Explicit Policy.....
4.10 Policy Mappings.....
4.11 Inhibit Policy Mapping.....
4.12 Inhibit Any Policy.....
4.13 Name Constraints.....
4.14 Distribution Points.....
4.15 Delta-CRLs.....
4.16 Private Certificate Extensions.....

Public Key Interoperability
Test Suite (PKITS)
Certification Path Validation

» Независимое экспертное исследование средств ЭП

Тест российских средств электронной подписи и шифрования документов



Александр Панасенко

Главный-редактор Anti-Malware.ru

Сравнения

Корпорации

Admin-PKI

File-PRO

Litoria Desktop

...

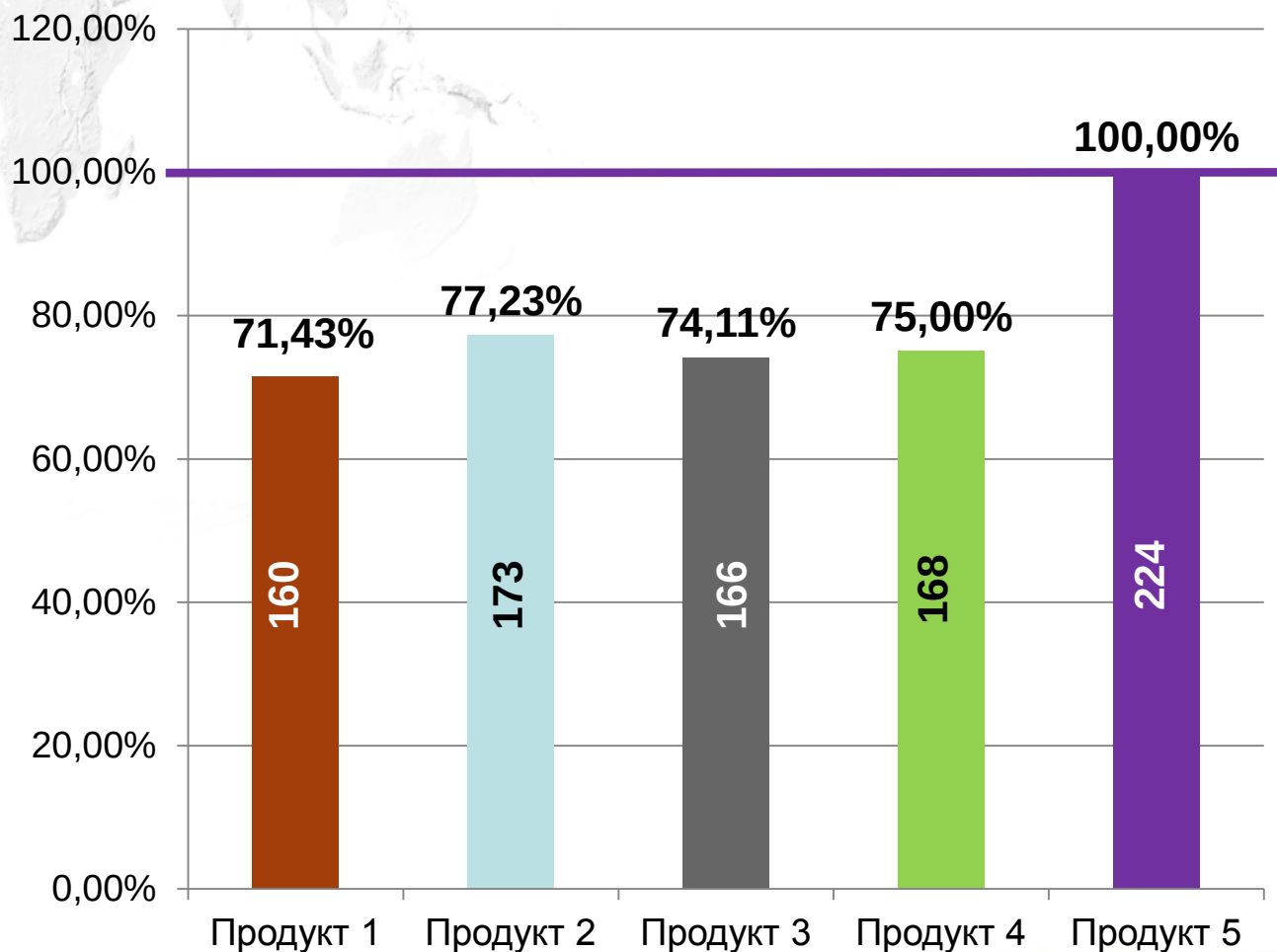


Для того чтобы признать электронный документ равным с юридической точки зрения бумажному с подписью и печатью, необходима электронная подпись, а безопасная отправка чувствительных данных должна быть обеспечена посредством их шифрования. Но несмотря на то, что государство всячески пропагандирует переход 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 средств ЭП





Итоги независимого исследования средств ЭП

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					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»				
-	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									

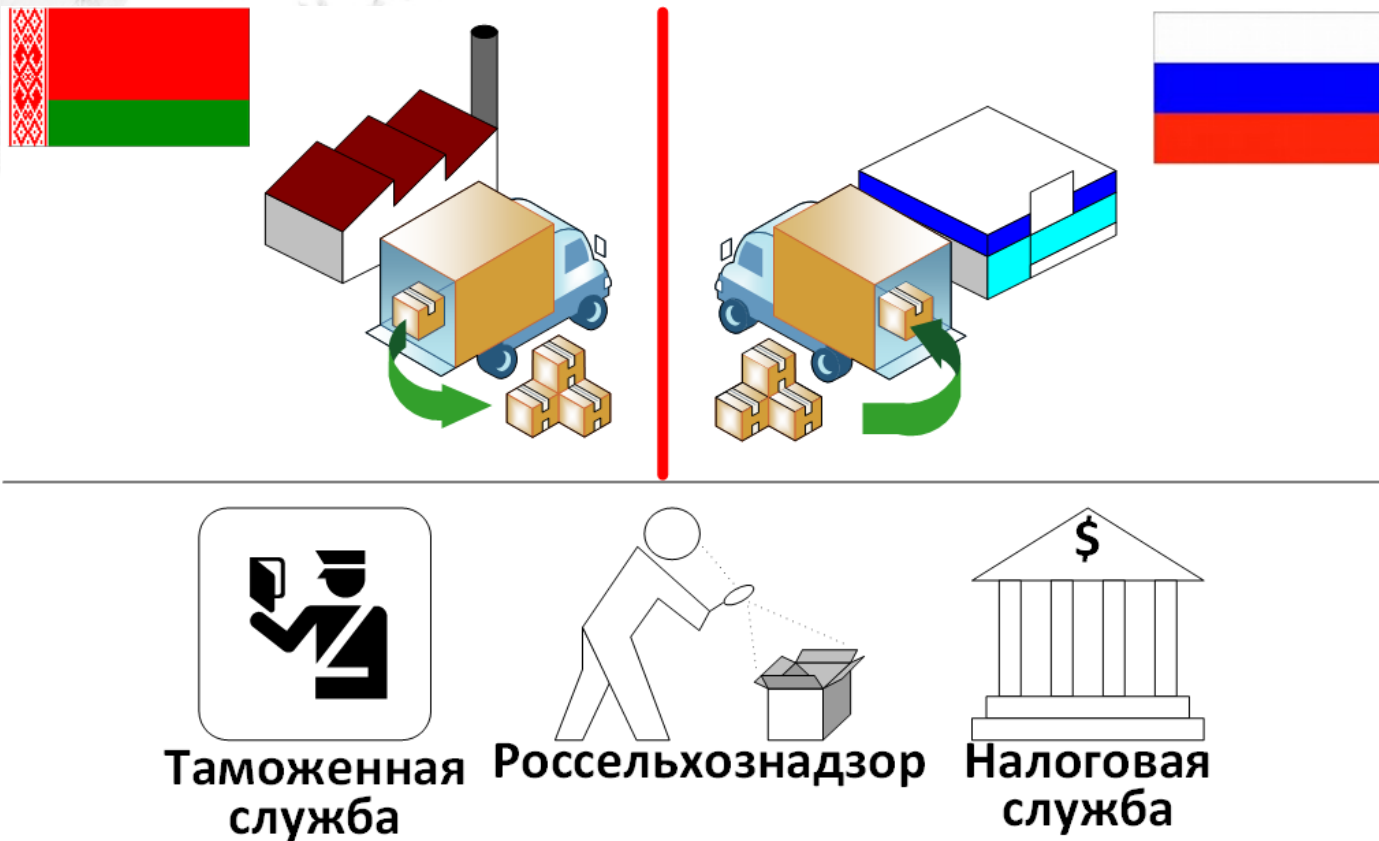


Итоги независимого исследования средств ЭП

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

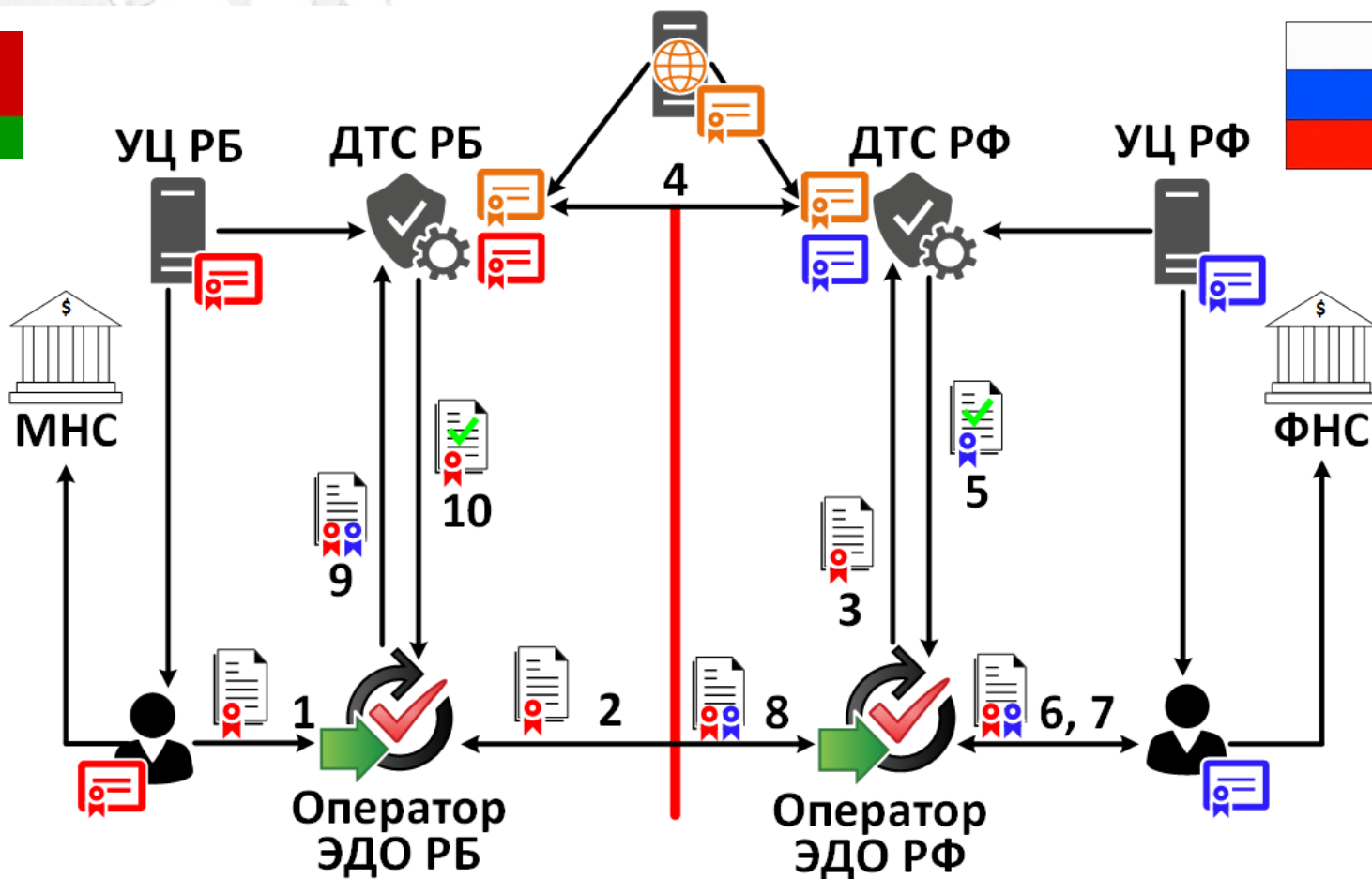
Инициатива “снизу”

КЗИ, Суздаль 2018



Инициатива “снизу”

КЗИ, Суздаль 2018



» В качестве вывода: рецепт успеха

Политическая воля

Централизованное управление
внедрением ТПД и ЕО

Взаимодействие бизнеса и власти

**Практическое
внедрение
интероперабельных
ЕО**

КЗИ, Суздаль 2018

Спасибо за внимание!

Кирюшкин Сергей Анатольевич
ООО “Газинформсервис”
Kiryushkin-S@gaz-is.ru
www.gaz-is.ru