PKI ФОРУМ
РОССИЯ 2023

О ПРАВИЛАХ ВЗАИМНОГО ПРИЗНАНИЯ ЭЛЕКТРОННОЙ (ЦИФРОВОЙ) ПОДПИСИ

Харахордин Юрий Вадимович

Начальник отдела информационной безопасности Департамента информационных технологий Евразийской экономической комиссии

Санкт-Петербург, 13 сентября 2023 г.

ИСПОЛЬЗУЕМЫЕ НОРМАТИВНО-ПРАВОВЫЕ АКТЫ

- *Перечень сфер, требующих обеспечения признания электронной цифровой подписи (электронной подписи) в электронном документе и обеспечения юридической силы электронных документов при трансграничном взаимодействии хозяйствующих субъектов с органами государственной власти государств - членов Евразийского экономического союза*
  (Распоряжение Коллегии Комиссии от 25 января 2022 г. № 8)

- *Концепция трансграничного информационного взаимодействия*
  (Решение Евразийского межправительственного совета от 9 августа 2019 г. № 7)

- *Требования к созданию, развитию и функционированию трансграничного пространства доверия*
  (Решение Совета Евразийской экономической комиссии от 5 декабря 2018 № 96)

- *Стратегия развития трансграничного пространства доверия*
  (Решение Коллегии Комиссии от 27 сентября 2016 г. № 105)

- *Положение об обмене электронными документами при трансграничном взаимодействии органов государственной власти государств - членов Евразийского экономического союза между собой и с Евразийской экономической комиссией*
  (Решение Коллегии Комиссии от 28 сентября 2015 г. № 125)

- *Правила электронного обмена данными в интегрированной информационной системе внешней и взаимной торговли*
  (Решение Коллегии Комиссии от 27 января 2015 №5)

ИСПОЛЬЗУЕМЫЕ НОРМАТИВНО-ПРАВОВЫЕ АКТЫ

О Правилах признания электронной цифровой подписи (электронной подписи) в электронном документе и обеспечения юридической силы электронных документов при трансграничном информационном взаимодействии юридических лиц (хозяйствующих субъектов) с уполномоченными органами государств - членов Евразийского экономического союза и Евразийской экономической комиссией с использованием службы доверенной третьей стороны

(Решение Коллегии Комиссии от 22 августа2022 г. № 120)

КОНЦЕПЦИЯ ТРАНСГРАНИЧНОГО ИНФОРМАЦИОННОГО ВЗАИМОДЕЙСТВИЯ

«Государства члены Союза обеспечивают право субъектов электронного взаимодействия **пользоваться услугами доверенных третьих сторон**.»

«Юридические лица (хозяйствующие субъекты) государств-членов **вправе самостоятельно выбирать механизмы защиты электронных документов** с учетом требований законодательства государств-членов и международных договоров, а также оценки связанных с процессом электронного взаимодействия рисков и собственных предпочтений»

«Информационный обмен электронными документами между субъектами электронного взаимодействия, использующими разные механизмы защиты электронных документов, **могут обеспечиваться с использованием различных механизмов обеспечения информационного взаимодействия, в том числе доверенной третьей стороны**»

«Субъекты электронного **взаимодействия в рамках отношений типа B2B могут** применять механизмы обеспечения информационного взаимодействия, **предоставляемые на основе договоров операторами общей инфраструктуры документирования информации в электронном виде** государств-членов в соответствии с законодательством государств-членов»

«при реализации отношений типа B2G преимущественно следует использовать механизмы общей инфраструктуры документирования информации в электронном виде, предоставляемые операторами элементов трансграничного пространства доверия, включенными в перечень элементов общей инфраструктуры документирования информации в электронном виде, утверждаемый Евразийской экономической комиссией»

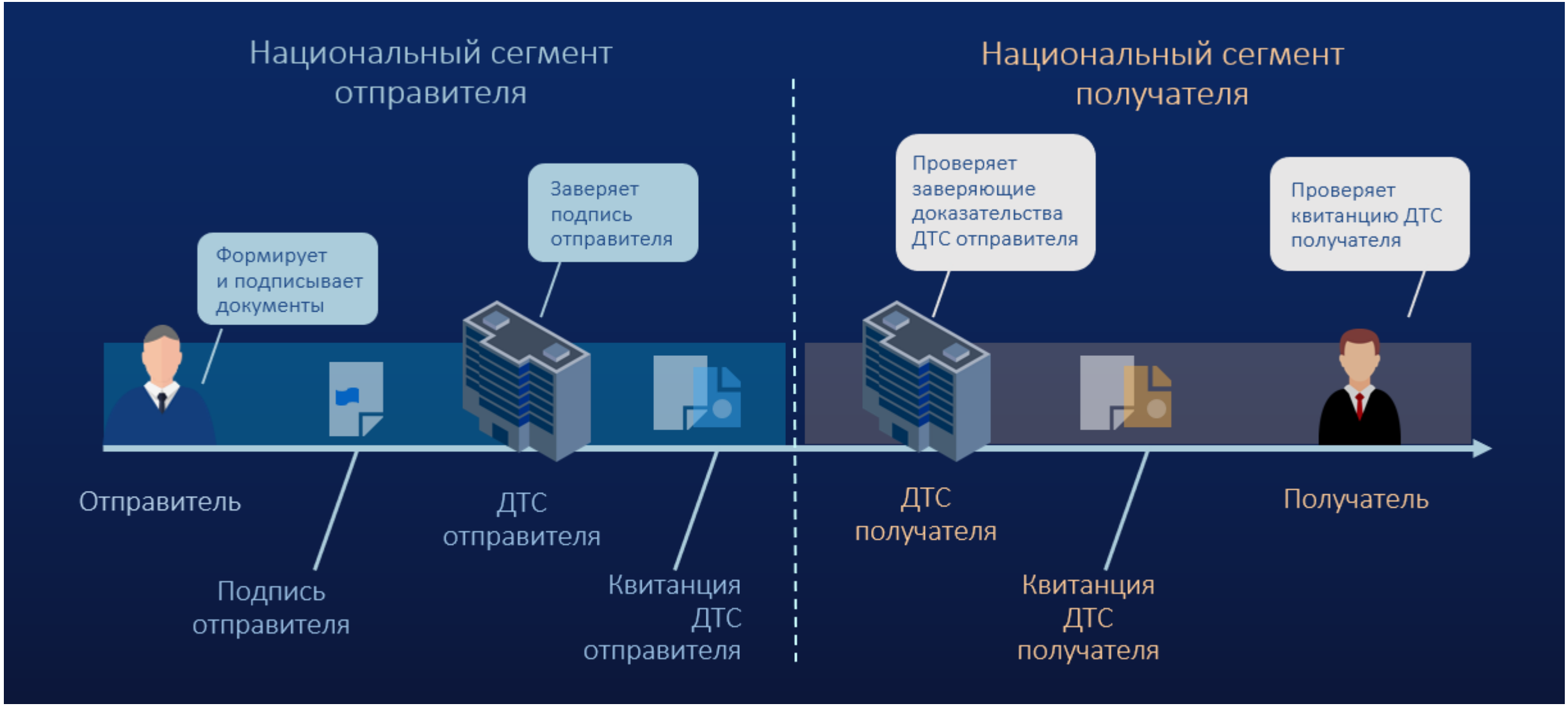
КОНЦЕПЦИЯ ТРАНСГРАНИЧНОГО ИНФОРМАЦИОННОГО ВЗАИМОДЕЙСТВИЯ: B2G

Механизмы обеспечения информационного взаимодействия в рамках отношений типа B2G :

- идентификация и аутентификация субъектов электронного взаимодействия (включая, при необходимости, управление сертификатами ключей проверки ЭЦП и предоставлению информации об их статусе);
- **создание и проверка ЭЦП, которой подписаны электронные документы, созданные субъектами электронного взаимодействия**;
- проверка статуса сертификатов ключей проверки ЭЦП;
- проверка полномочий субъектов электронного взаимодействия;
- предоставление меток времени;
- архивное хранение данных, в том числе электронных документов, проверки их подлинности по истечении заданного периода времени;
- передача данных, в том числе электронных документов, между субъектами электронного взаимодействия с достижением характеристик защиты передаваемых данных;
- **неотказуемость** - формирования (предоставления) для третьей стороны электронных доказательств выполнения субъектами электронного взаимодействия, участвующих в отношениях типа B2G, действий, в том числе подписания ЭЦП электронного документа и его передачи (получения);
- ведение и предоставление доступа к перечню элементов общей инфраструктуры документирования информации в электронном виде.

Указанные механизмы реализуются элементами трансграничного пространства доверия, которые должны соответствовать Требованиям к созданию, развитию и функционированию трансграничного пространства доверия

ТРАНСГРАНИЧНОЕ ИНФОРМАЦИОННОЕ ВЗАИМОДЕЙСТВИЕ В РАМКАХ ОТНОШЕНИЙ G2G



ПРОБЛЕМНЫЕ ВОПРОСЫ ПРИ ИСПОЛЬЗОВАНИИ ЭЛЕКТРОННЫХ ДОКУМЕНТОВ ПРИ B2G И B2B-ВЗАИМОДЕЙСТВИЯХ

Необходимо формировать особые требования к взаимодействию с сервисами ДТС для B2G и B2B при трансграничном взаимодействии

ПРАВИЛА ПРИЗНАНИЯ ЭЦП ДЛЯ B2G: ОБЩИЕ ПОДХОДЫ

«**Механизм признания ЭЦП** в электронном документе и обеспечения юридической силы электронных документов при трансграничном информационном взаимодействии **основывается на реализации задачи легализации** (подтверждения подлинности) электронных документов и ЭЦП юридических лиц (хозяйствующих субъектов), **выполняемой с использованием службы доверенной третьей стороны** в соответствии с настоящими Правилами»

«**Электронный документ, подлинность которого подтверждена квитанцией** доверенной третьей стороны с положительным результатом проверки, **признается** в юрисдикции уполномоченного органа государства-члена и Комиссии **равнозначным электронному документу, подписанному ЭЦП юридического лица (хозяйствующего субъекта)**»

«В рамках выполнения задачи легализации (подтверждения подлинности) электронных документов и ЭЦП юридических лиц (хозяйствующих субъектов) в фиксированный момент времени **доверенные третьи стороны**, сервисы которых входят в состав службы доверенной третьей стороны интегрированной информационной системы Союза (далее – интегрированная система), **во взаимодействии друг с другом осуществляют для уполномоченных органов государств-членов и Комиссии процедуру проверки ЭЦП юридических лиц (хозяйствующих субъектов) в электронных документах с формированием квитанции доверенной третьей стороны как результата такой проверки**»

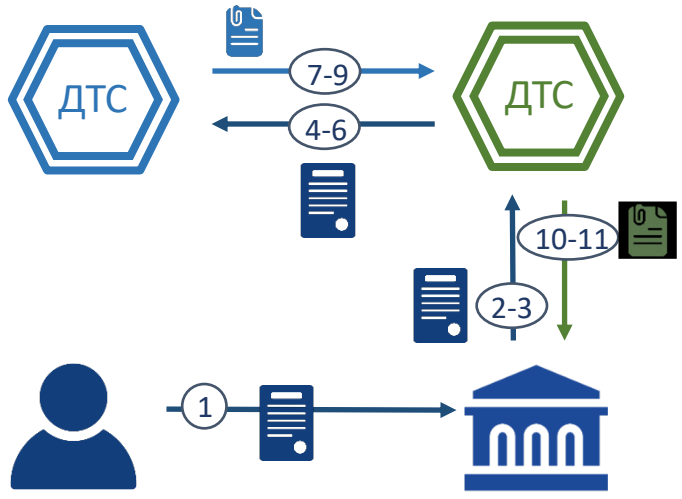
«Обеспечение юридической силы при трансграничном информационном взаимодействии … осуществляется посредством **применения к этим участникам единых требований к созданию, развитию и функционированию трансграничного пространства доверия, утверждаемых Комиссией**»

ОБЩИЕ ПОДХОДЫ К РЕАЛИЗАЦИИ ПРОЦЕДУРЫ ПРИЗНАНИЯ ЭЦП

Правила информационного взаимодействия и обработки данных доверенными третьими сторонами при проверке ЭЦП электронного документа

Упрощенная схема

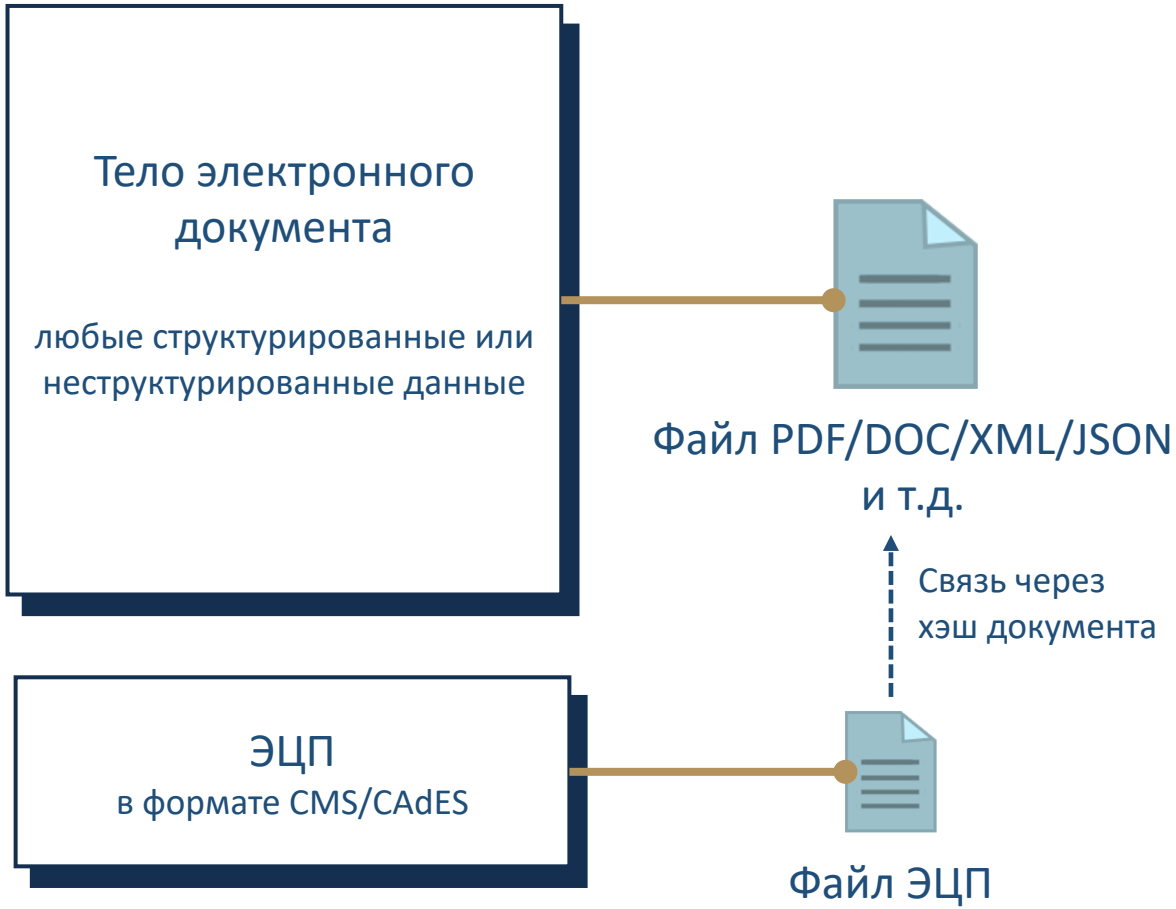
(взаимодействия 2-11 реально выполняются через интеграционную платформу)



Легенда:

- Электронный документ с ЭЦП отправителя
- Квитанция ДТС отправителя
- Квитанция ДТС получателя

СТРУКТУРА ЭЛЕКТРОННОГО ДОКУМЕНТА

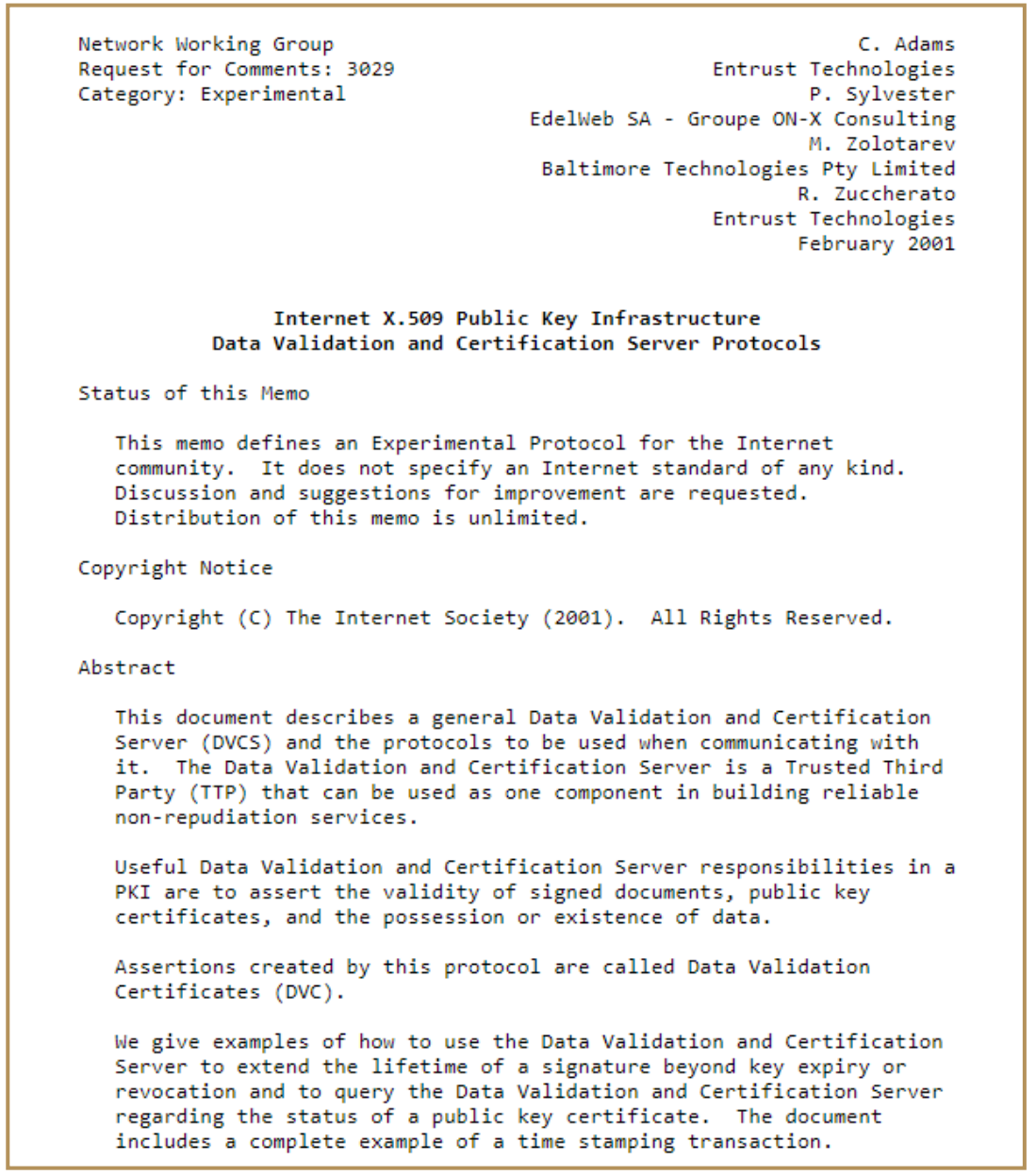


- Правилами регламентируется использование ЭЦП в формате CMS (RFC 5652) либо CAdES (RFC 5126)
- Тело электронного документа может представлять собой любой бинарный файл, содержащий структурированные или неструктурированные данные
- За счет использования на первом этапе ЭЦП в формате CMS/CAdES упрощается подача электронных документов хозяйствующих субъектов уполномоченным органам (предполагается, что будут использоваться в основном такие форматы ЭД как PDF/DOC, что позволит использовать уполномоченным органам такие документы «как есть» без необходимости дополнительных инструментов визуализации)
- В рамках дальнейших работ планируется регламентировать механизмы проверки ЭЦП в иных форматах (например XMLDSIG/XAdES, PAdES и проч.)

СТАНДАРТ DVCS КАК ТЕХНОЛОГИЧЕСКАЯ ОСНОВА

Internet X.509 Public Key Infrastructure
Data Validation and Certification Server Protocols

- В качестве технологического стандарта для реализации взаимодействия уполномоченных органов с ДТС, а также ДТС между собой, используется стандарт DVCS
- Стандарт DVCS регламентирует процессы проверок ЭЦП, созданных в двоичном формате (CMS)
- В рамках работ по написанию проекта Правил было произведено исследование стандарта DVCS на предмет возможности его использования для схемы взаимодействия, регламентируемую Правилами
- Результаты исследования показали принципиальную возможность использования стандарта DVCS
- Сформулированы требования по заполнению полей DVCS-запросов и квитанций для условий реализации B2G-взаимодействия в рамках Союза, которые легли в основу приложения № 2 к Правилам



Network Working Group
Request for Comments: 3029
Category: Experimental

C. Adams
Entrust Technologies
P. Sylvester
EdelWeb SA - Groupe ON-X Consulting
M. Zolotarev
Baltimore Technologies Pty Limited
R. Zuccherato
Entrust Technologies
February 2001

Internet X.509 Public Key Infrastructure
Data Validation and Certification Server Protocols

Status of this Memo

This memo defines an Experimental Protocol for the Internet community. It does not specify an Internet standard of any kind. Discussion and suggestions for improvement are requested. Distribution of this memo is unlimited.

Copyright Notice

Abstract

This document describes a general Data Validation and Certification Server (DVCS) and the protocols to be used when communicating with it. The Data Validation and Certification Server is a Trusted Third Party (TTP) that can be used as one component in building reliable non-repudiation services.

Useful Data Validation and Certification Server responsibilities in a PKI are to assert the validity of signed documents, public key certificates, and the possession or existence of data.

Assertions created by this protocol are called Data Validation Certificates (DVC).

We give examples of how to use the Data Validation and Certification Server to extend the lifetime of a signature beyond key expiry or revocation and to query the Data Validation and Certification Server regarding the status of a public key certificate. The document includes a complete example of a time stamping transaction.

ДАЛЬНЕЙШИЕ ДЕЙСТВИЯ

Модернизация ДТС Комиссии и экспортного варианта ДТС для B2G взаимодействия

Разработка и утверждение Архитектуры 2 этапа развития Трансграничного пространства доверия

Разработка и утверждение Требований к созданию, развитию и функционированию трансграничного пространства доверия для B2G взаимодействия

Разработка и утверждение Порядка разрешения конфликтных ситуаций при трансграничном обмене электронными документами

Регламентация механизмов проверки ЭЦП в иных форматах (например XMLDSIG/XAdES, PAdES и тому подобные

СПАСИБО ЗА ВНИМАНИЕ !