Ежегодная международная научно-практическая конференция
«РусКрипто’2021»

Разработка проекта МР «Доверенная третья сторона. Протокол сервера проверки и удостоверения данных»

Драло Мария Павловна
ООО «Газинформсервис»
Dralo-M@gaz-is.ru

Предпосылки разработки проекта МР

1. **Международное право**

- Директива 1999/93/ЕС Европейского парламента и Совета ЕС О правовых основах регулирования электронных подписей в сообществе
- Регламент (ЕС) N 910/2014 Европейского Парламента и Совета ЕС Об электронной идентификации и удостоверительных сервисах для электронных транзакций на внутреннем рынке и об отмене Директивы 1999/93/ЕС
- Договор о Евразийском экономическом союзе

2. **Национальное право:**

- стратегия развития информационного общества в РФ на 2017-2030 годы
- программа «Цифровая экономика Российской Федерации»

Основания разработки стандарта

18 апреля 2018 г.

Протокол №23
Заседания технического комитета по стандартизации
“Криптографическая защита информации” (ТК26)

2.8 Включить разработку документа «Протокол проверки сертификатов и подписанных документов» в план работы РГ с целью дальнейшего утверждения его в качестве методических рекомендаций. О ходе работ доложить на осеннем заседании ТК 26.

(отв. РГ СКАиП, срок – ноябрь 2019 г.)

Цель разработки

Унификация подходов к реализации процессов и механизмов, связанных с осуществлением процедур проверки электронных подписей, стандартизированных на уровне протокола для решения поставленных задач:

- Проверки электронной подписи
- Проверки действительности сертификатов ключей проверки электронной подписи
- Удостоверения обладания данными
- Предоставления результатов выполненных задач

Российская нормативная платформа

Международные договоры и соглашения РФ

Договор о ЕАЭС, Рамочное соглашение об упрощении процедур трансграничной безбумажной торговли в Азиатско-Тихоокеанском регионе

Федеральные законы РФ, Указы Президента, Постановления Правительства

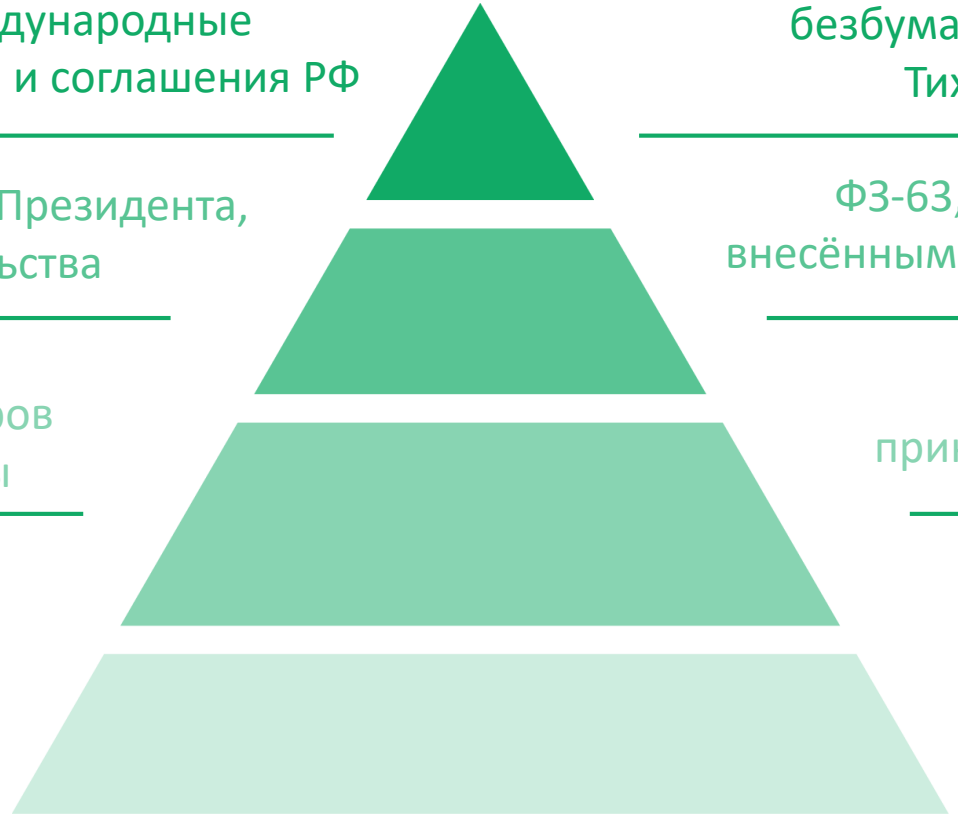
ФЗ-63, с поправками, внесёнными ФЗ-476, ПП № 2101

Требования регуляторов и подзаконные акты

Приказ ФСБ РФ № 556, приказы Минцифры РФ № 641 и № 642

Международные и национальные стандарты (RFC 3029, x.842)

Проект МР протокола сервера проверки и удостоверения данных



Анализ международной практики

В качестве основы для разработки отечественного стандарта протокола сервера проверки и удостоверения данных был проведен сравнительный анализ следующих протоколов:

- Data Validation and Certification Server Protocols (DVCS)
- OASIS Digital Signature Service (DSS)
- XML Key Management Specification (XKMS)

Основные параметры сравнения протоколов

Виды обрабатываемых запросов

Используемый транспортный протокол

Обрабатываемый формат подписанной структуры

Сложность реализации

Производительность

Поддержка множественной ЭП

DVCS

OASIS DSS

XKMS

Применимость для работы с иностранными СКЗИ

Возможность проверки ЭП хеш-значения от ЭД

Юридическая значимость результата работы протокола

Поддержка штампов времени

Возможности стандартов и требования ФЗ-63

ФЗ-63	DVCS	Oasis DSS	XKMS
Проверка ЭП ЭД	+	+	+
Проверка статуса СКП ЭП	+	+	+
Поддержка работы со штампом времени	+	+	–
Возможность формирования квитанций	+	–	–

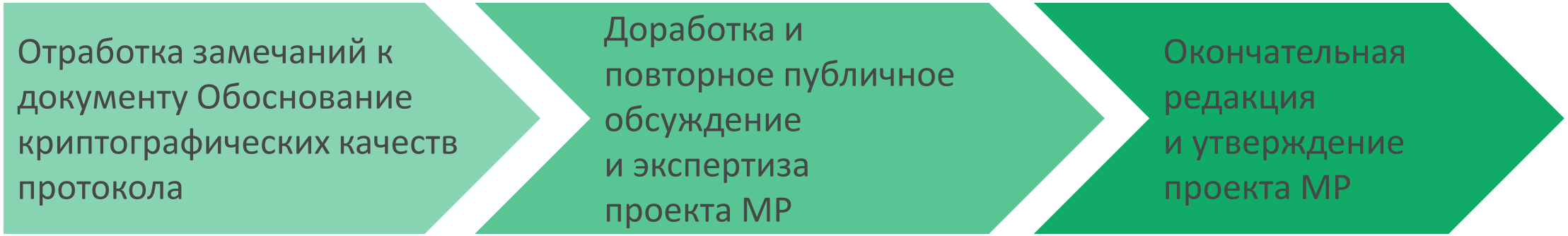
Протокол сервера проверки и удостоверения данных

- Описание протокола
- Термины и определения
- Функции, реализуемые протоколом: CPD, CCPD, VSD и VPKC
- Сценарии использования протокола
- Функциональные требования к протоколу
- Трансграничное взаимодействие
- Описание общих типов данных, используемых для работы протокола
- Описание запросов на проверку
- Описание ответов
- Описание протоколов безопасности и транспортного взаимодействия
- Патентная информация

Сопутствующие документы

- Модель угроз протокола сервера проверки и удостоверения данных
- Криптографическое исследование. Обоснование криптографических качеств протокола

Дорожная карта разработки проекта МР



апрель 2021 **май-август 2021** **сентябрь 2021**

Вопросы

Контактная информация

Электронная почта:

Dralo-M@gaz-is.ru

Телефон:

+7 812 677-20-53

Facebook:

https://www.facebook.com/GAZINFORMSERVICE/

Сайт:

www.gaz-is.ru