Российские стандартизированные решения в области криптографической защиты информации

28.03.2024

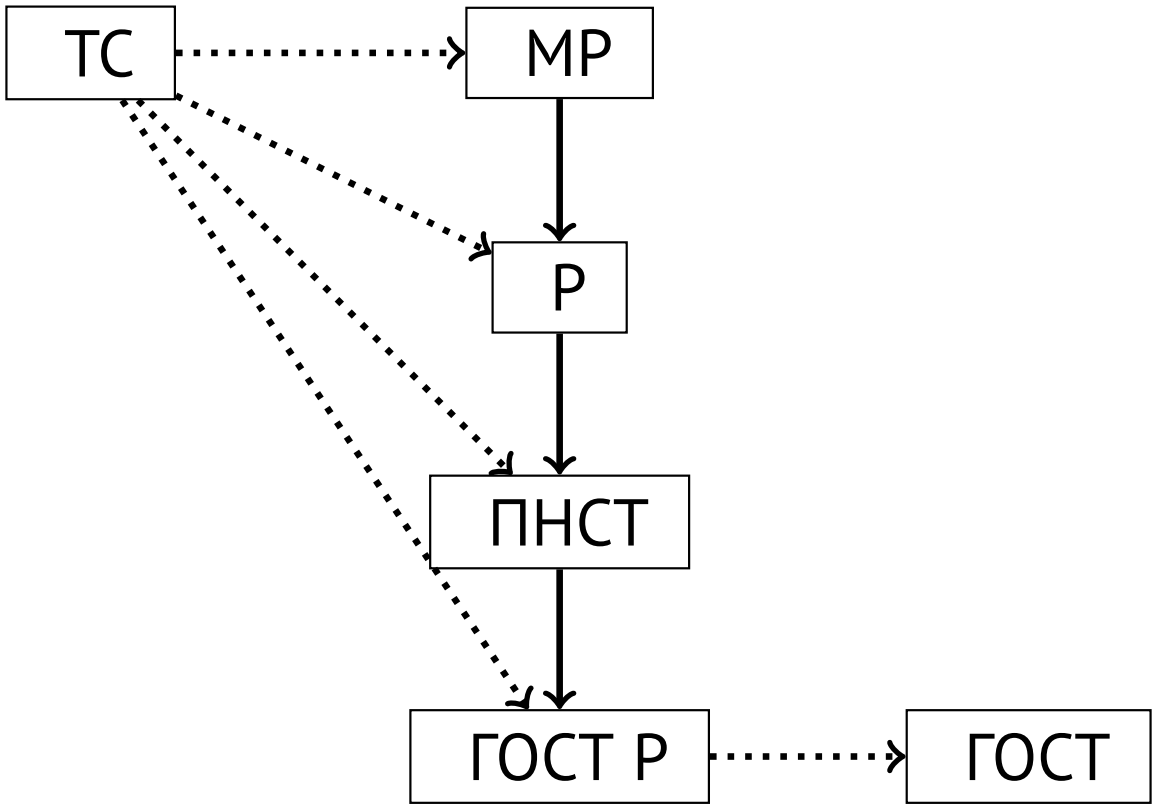
Национальная система стандартизации Российской Федерации в области КЗИ

В области КЗИ ведущую роль играет

Технический комитет по стандартизации № 26 «Криптографическая защита информации»

- Выявление потребностей промышленности и разработчиков
- Формирование требований и перечня функциональных возможностей разрабатываемого решения, удовлетворяющего потребностям производителей и разработчиков при реализации проекта
- Унификация разрабатываемых решений
- Разработка стандартизированного решения, удовлетворяющего потребностям

Иерархия документов по стандартизации в области КЗИ



ТК 26 **разработано > 90 документов** по стандартизации в области КЗИ (начиная с 2017 г.)

Стандартизированные решения Российской Федерации в области КЗИ

Фундаментом российской системы стандартизации являются следующие криптографические примитивы:

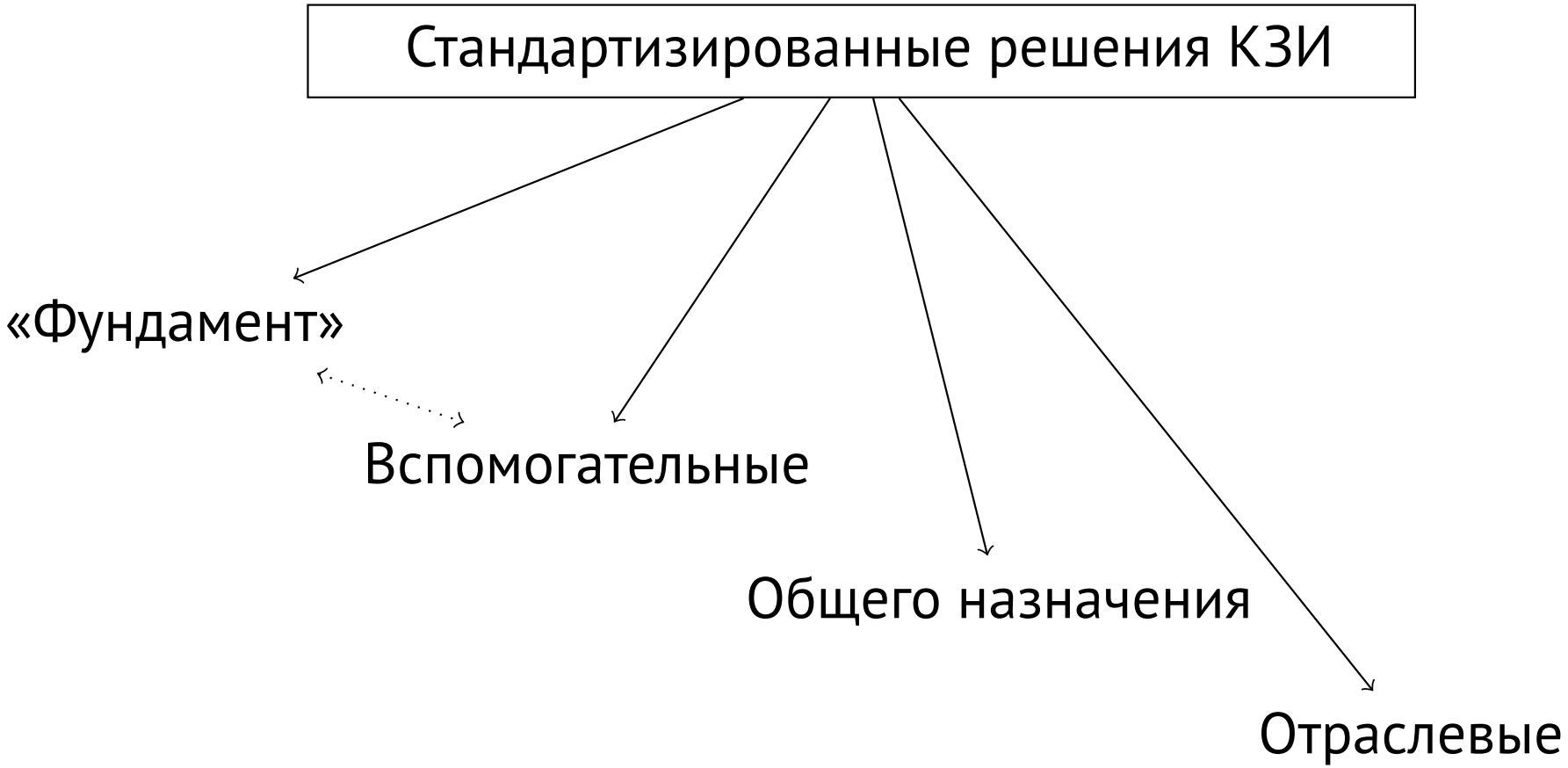
- Блочные шифры **«Кузнечик»** (128, 256 бит) и **«Магма»** (64, 256 бит)
- Режимы работы блочных шифров (**ECB**, **CBC**, **CFB**, **OFB**, **CTR**, **MAC**, **MGM**, **CTR-ACPKM**)
- Функция хэширования **«Стрибог»** (256, 512 бит)
- Электронная подпись (512 или 1024 бита)

Стандартизированные решения Российской Федерации в области КЗИ

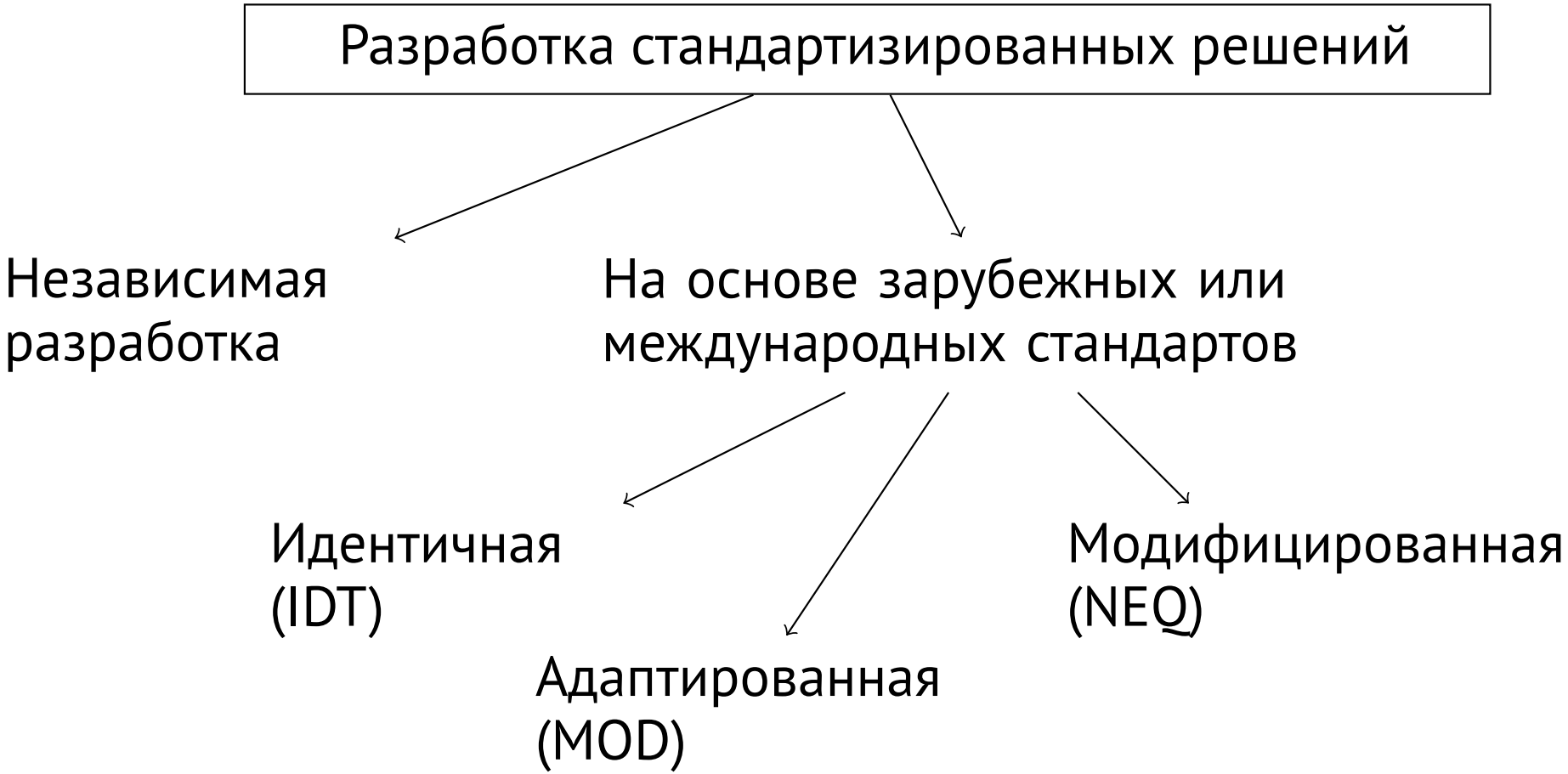
Вспомогательные документы, которые описывают:

- Различные функции на базе х.ф. «Стрибог» (развертка ключей, HMAC, PRF, KDF ...)
- Экспорт и импорт ключей, согласование ключей (VKO)
- Параметры и форматы представления эллиптических кривых (оптимизация вычислений)
- Форматы передачи защищенных сообщений, представления данных и контейнеры (CMS, x.509, PKCS)

Стандартизированные решения Российской Федерации в области КЗИ



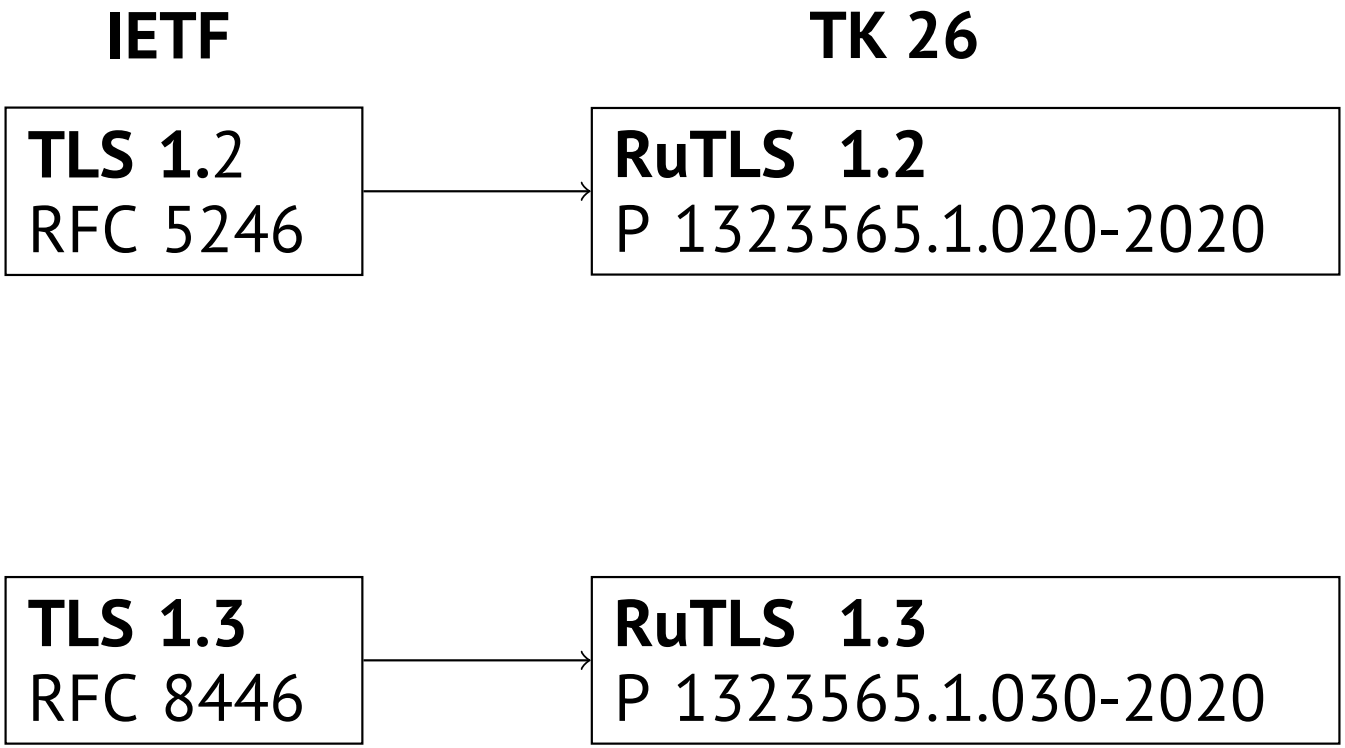
Разработка стандартов в области КЗИ



Разработка стандартов в области КЗИ

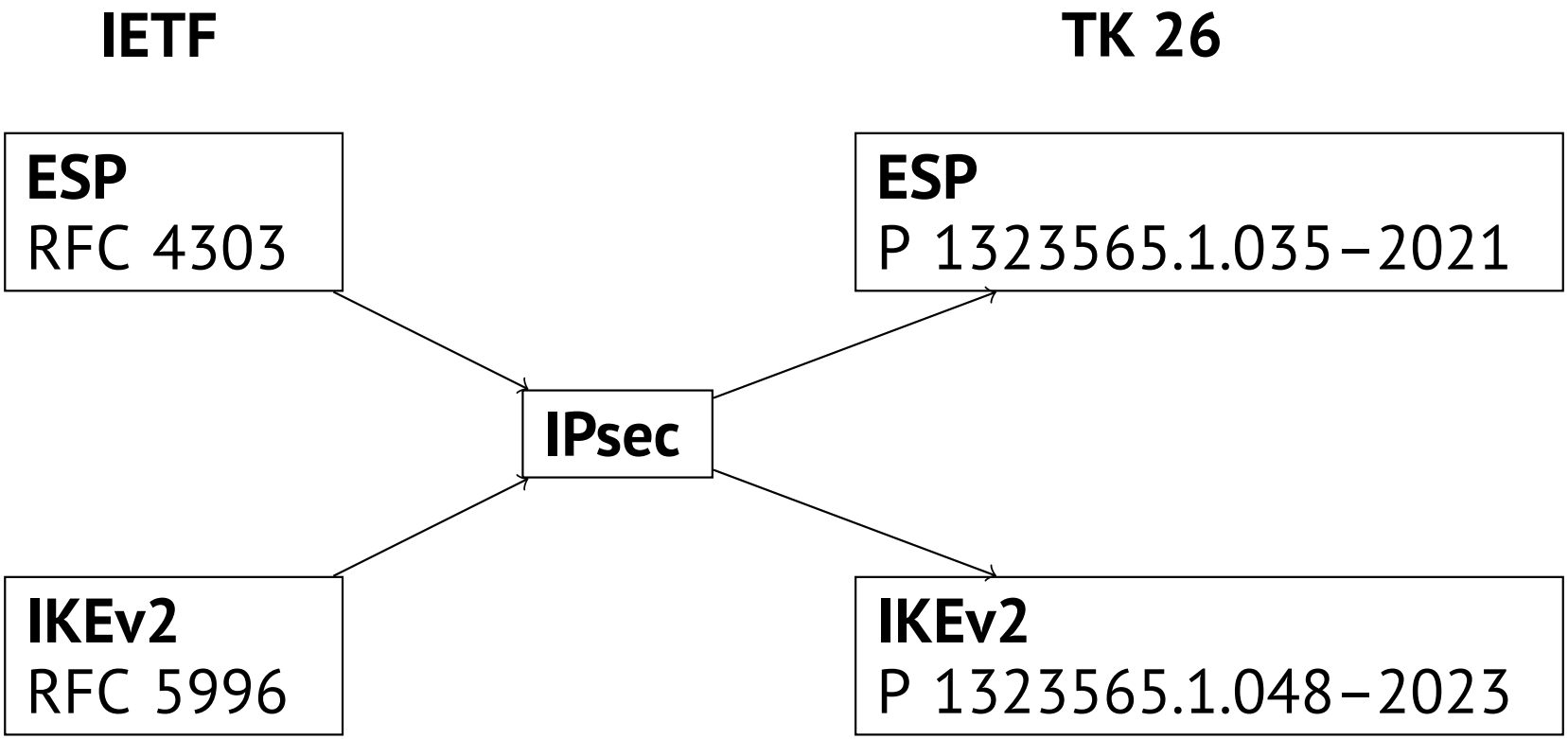
Решения общего назначения

Решения общего назначения. Протокол TLS



* идентификаторы для всех наборов российских криптографических примитивов организацией IANA внесены в реестр (RFC 9189, RFC 9367).

Решения общего назначения. Семейство протоколов IPsec



* идентификаторы для всех наборов российских криптографических примитивов организацией IANA внесены в реестр (RFC 9227).

Решения общего назначения. Протокол IPlir

Протокол **IPlir** - **Р 1323565.1.034–2020**. Некоторые особенности протокола IPlir:

- Позволяет обеспечить конфиденциальность и целостность данных
- Назначение - построение туннелей
- Нет механизма генерации ключей, ключевой материал поставляется извне (Master key)
- Простая ключевая система для формирования внутренних ключей на базе блочного шифра
- Работает на 3 уровне ISO. Представляет собой структуру данных для инкапсуляции IP-пакетов
- Использует блочные шифры **Магма & MGM**, **Кузнечик & MAC**

Решения общего назначения. Протокол SESPAKE

Протокол **SESPAKE** - **Р 50.1.115–2016** (Security Evaluated Standardized Password Authenticated Key Exchange) - протокол выработки общего ключа с аутентификацией на основе пароля при взаимодействии клиент-сервер.

Протокол использует:

- PBKDF2 $\leftarrow$ HMAC $\leftarrow$ «Стрибог»
- Электронную подпись, х.ф. «Стрибог»

Решения общего назначения. Протокол SESPAKE

Некоторые особенности архитектуры протокола SESPAKE:

- Предусмотрена защита от атак оффлайн перебора пароля
- Нет критерия для проведения перебора пароля
- Несимметричность протокола (использование различных математических операций на стороне клиента и сервера)
- В архитектуре протокола SESPAKE заложен накопленный опыт проектирования протоколов данного класса
- Обеспечивает защиту от всех классов атак, характерных для данного класса протоколов
- Экспортирует полученный ключ (ключевой материал).

Разработка стандартов в области КЗИ

Отраслевые решения

Отраслевые. IoT & IIoT. Протокол CRISP

Протокол **CRISP - Р 1323565.1.029–2019** (CRyptographic Industrial Security Protocol) - неинтерактивный, бессессионный протокол, предназначенный для обеспечения безопасной передачи данных в автоматизированных системах управления, промышленных сетях, системах сбора информации и при M2M-взаимодействии.

Протокол использует:

- **Магма & MAC & CTR**

Отраслевые. IoT & IIoT. Протокол CRISP

Некоторые особенности протокола CRISP:

- Используется совместно с любым транспортным телекоммуникационным протоколом
- CRISP - надстройка для обеспечения безопасности данных
- Обеспечивает конфиденциальность и целостность данных, аутентификацию источника и защиту от повтора
- Использует предварительно распределенные ключи (PSK)
- Минимальный размер сообщения (8 байт)
- Ключевая система на базе блочного шифра в режиме MAC

Отраслевые. ЖКХ. Протокол DLMS

Протокол **DLMS** - **Р 1323565.1.032-2020**. Применяется при организации защищенного обмена данными между системами сбора данных (клиент) и измерительными устройствами (сервер). Данный протокол позволяет обеспечить:

- Конфиденциальность
- Целостность
- Аутентификацию источника данных

Отраслевые. Автотранспорт. Протокол Тахограф

Протокол **«Тахограф»** - **Р 1323565.1.018-2018**. Данный протокол определяет криптографические механизмы аутентификации, регистрации и хранения контрольных данных, в том числе ключевой информации для электронной подписи, в контрольных устройствах для автотранспорта.

Отраслевые. PKI-инфраструктура. Различные элементы

Разработан необходимый набор элементов для развертывания полноценной PKI-инфраструктуры на базе российских криптографических примитивов:

- Электронная подпись **ГОСТ Р 34.10-2012**
- Использование российских криптографических алгоритмов в сертификатах формата x.509, списке отозванных сертификатов CRL и запросе на сертификат PKCS #10 - **Р 1323565.1.023–2022**
- Протокол штампов времени (TSP) - **Р 1323565.1.044–2022**
- Протокол получения актуальных статусов сертификатов (OCSP) - **МР 26.2.004-2023**

Перспективные направления деятельности ТК 26

- Квантовое распределение ключей (системы выработки и распределения ключей, СВРК)
  - канал СВРК-СКЗИ (Протокол **ProtoQa**, Р 1323565.1.046–2023)
  - канал между узлами СВРК
- Постквантовые схемы
  - Коды, исправляющие ошибки
  - Криптография на решётках
  - Изогении эллиптическими кривых
- Новые криптографические примитивы
  - Подпись вслепую (BSign)
  - Доказательства с нулевым разглашением (ZKP)
  - Распределенные безопасные вычисления (MPC)
  - …

Спасибо за внимание