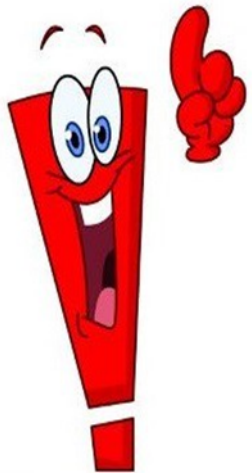
Цель

Пользователям Союзного государства:

- удобно
- безопасно/надежно (рассмотрим подробнее)
- не дорого



Безопасно/надежно

Эквивалентный уровень безопасности:

- Что он означает (и проблема не столько в правильной проверке, сколько в безопасности подписания)
- Близкие термины и их определения
- Эквивалентные требования к средствам ЭЦП
- Эквивалентные требования к услугам по распространению ключей проверки подписи
- Эквивалентные методы/способы/принципы оценки соответствия указанным выше требованиям
- …

Гармонизация терминов и определений

ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

ПРЕДВАРИТЕЛЬНЫЙ НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

пнет 799— 2022

Информационные технологии

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Термины и определения

ГОСУДАРСТВЕННЫЙ СТАНДАРТ РЕСПУБЛИКИ БЕЛАРУСЬ

СТБ 34.101.69-2014

Информационные технологии и безопасность

КРИПТОЛОГИЯ

Термины и определения

Эквивалентные требования к средствам ЭЦП

- Алгоритмы (выработки и проверки подписи; хэширования; генерации параметров; генерации ключей; …)
- Форматы (подписанных сообщений; СОК; СОС; …)
- Протоколы (OCSP; …)
- Требования к среде эксплуатации

Эквивалентные требования к услугам по распространению ключей проверки подписи

- ❑ К политике УЦ
- ❑ К системному ПО
- ❑ К криптографическому ПО
- ❑ К физической защите
- ❑ По защите информации
- ❑ К ответственности за качество услуг
- ❑ К локальным нормативным правовым актам УЦ
- ❑ …

Как достичь

Два варианта:

1. Гармонизация действующих нормативных и правовых документов
2. Разработка и принятие единых нормативных и правовых документов, на основе имеющихся

Далее – реализация на практике.

Гармонизация в правовой сфере. Некоторые аспекты

- В Беларуси (РБ): ЭД и ЭЦП. В России (РФ): ЭП.
- В РБ нет ответственности УЦ
- …..

Иностранный ЭД в РБ

- Есть регулятор (ОАЦ)
- Есть оператор проверки подлинности иностранных ЭД (НЦЭУ)
- В Законе об ЭД и ЭЦП есть о признании иностранных СОК, но нет о юридической силе подлинных иностранных ЭД

Иностранный сертификат в РБ

Статья 30. Признание иностранного сертификата открытого ключа

- ❑ Доверие к СОК через международный договор
- ❑ Также можно доверять СОК, выданному иностранным УЦ, аккредитованным в ГосСУОК РБ

Но:

- ✓ как иностранный УЦ будет соответствовать требованиям для аккредитации, если согласно ним должны использоваться сертифицированные в РБ средства ЭЦП?
- ✓ Кто будет его клиентами по этой услуге – только те кто использует сертифицированные в РБ средства ЭЦП.
- ✓ А как лица РФ в массовом порядке могут приобрести такие средства?

О проверке электронных подписей

- Обыденная
- В рамках споров (независимая)
- Важных ЭД (это обыденная? независимая? или отдельная процедура?)

Об услугах проверки электронных подписей

Две возможности:

- Проверить ЭП самостоятельно (на данный момент для иностранных, в т.ч. Союзных, исключена)

- Воспользоваться услугой по проверке подписи

О применении доверенных сторон

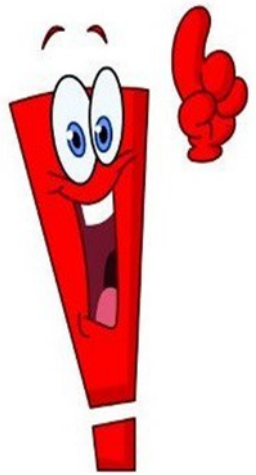
Доверенные стороны (организации), оказывающие услуги по:

- Распространению ключей проверки подписи - УЦ
- По проверке ЭП - ДТС
- Облачной подписи, проверке, генерации и управлению ключами – облачная ЭЦП

Объединение доверенных сторон

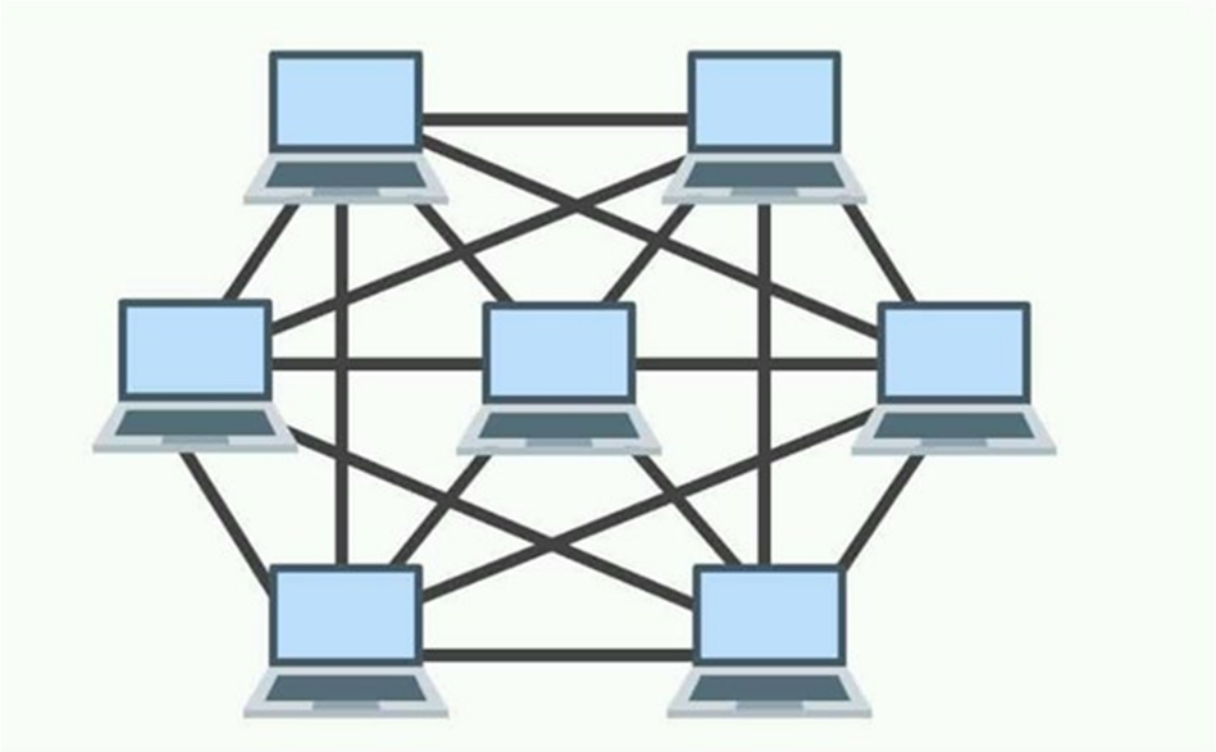
Организация, оказывающая услуги по:

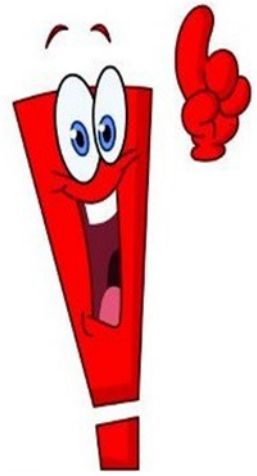
- Распространению ключей проверки подписи - УЦ
- По проверке ЭП - ДТС
- Облачной подписи, проверке, генерации и управлению ключами – облачная ЭЦП



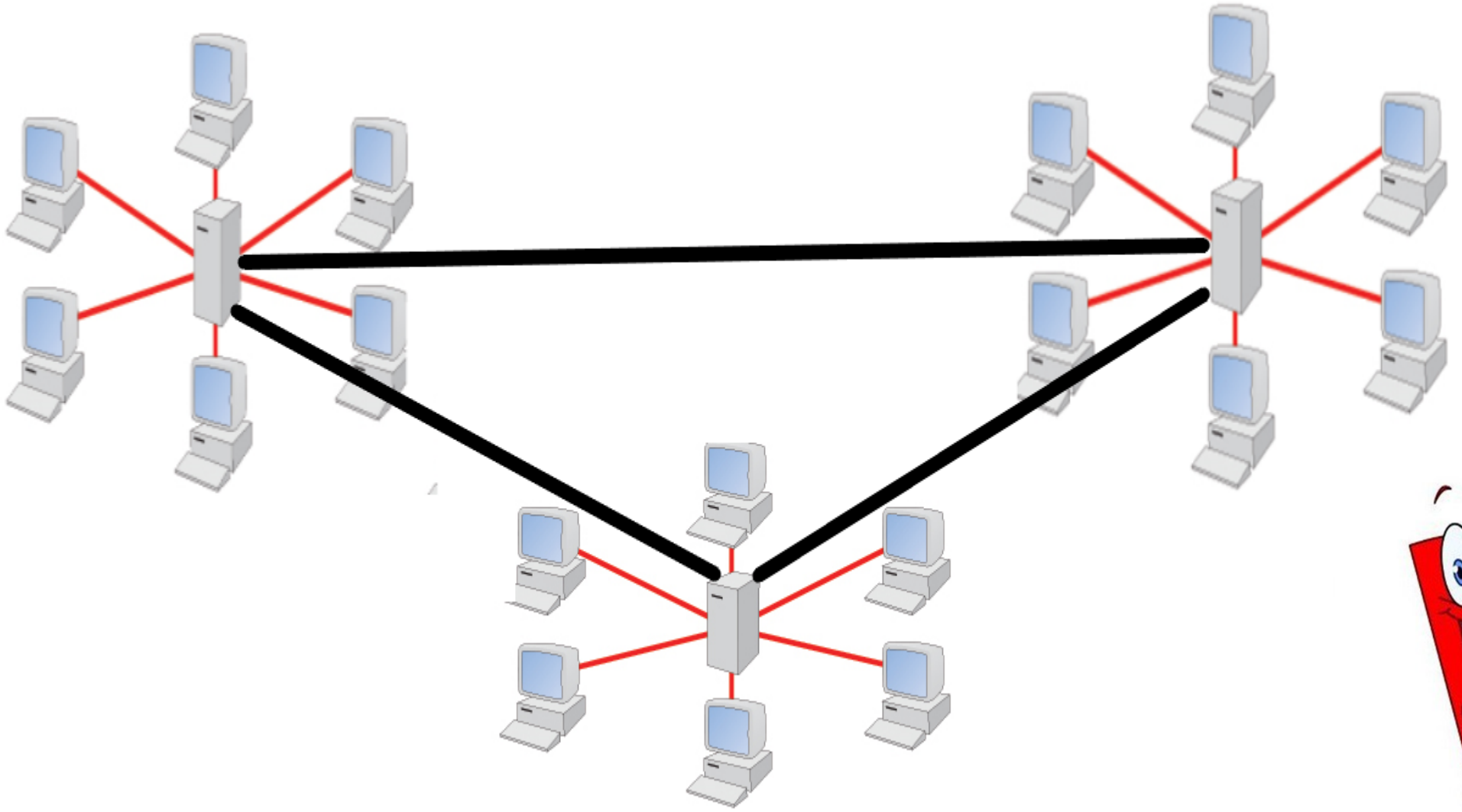
Изменение модели открытого взаимодействия

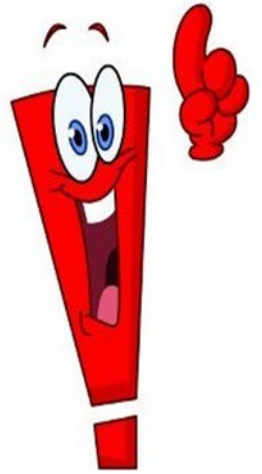
ISO/IEC 9594-8:2020 Information technology — **Open systems interconnection** — Part 8: The Directory: Public-key and attribute certificate frameworks





Изменение модели открытого взаимодействия





Ввоз/вывоз средств ЭЦП в Союзном государстве

- Пересмотр целей ограничений с учетом реалей
- Как применяется шифрование в средствах ЭЦП
- Связь между средствами ЭЦП и шифрования в средствах КЗИ:
  - ЭД открытый
  - ЭД конфиденциальный

LWO

В ритме инноваций

lwo.by
contact@lwo.by

+375 17 334 10 02
+375 17 334 28 27

ул. Кропоткина, д. 91, Минск
Республика Беларусь, 220002