PKI-FORUM
РОССИЯ

О работах ТК 26 по форматам подписи и сопутствующим протоколам

Павел Смирнов

Станислав Смышляев

Компания КриптоПро

КРИПТОПРО

Предпосылки работ по стандартизации

- Отсутствие нормативно-правовых актов, определяющих механизмы и процедуры формирования и проверки ЭП
- Несовместимость средств ЭП друг с другом
- Несоответствие процедур проверки цепочек сертификатов в отечественных средствах ЭП международным стандартам
  - https://www.anti-malware.ru/compare/test_russian_digital_signature_and_encryption_documents
  - Доклад Станкевич Т. «Стандартизация и унификация процессов формирования и проверки электронной подписи» на PKI Forum 2017

Пробелы в техническом регулировании

- Проверка статуса сертификата ключа проверки ЭП
- Проверка статусов сертификатов ключей проверки ЭП по цепочке до доверенного корневого сертификата
- Протокол штампов времени (TSP)
- Протокол проверки статуса сертификата в режиме реального времени (OCSP)
- Формат подписанных данных в документах XML (XMLDSig)
- Форматы расширенных представлений подписанных документов (CAdES, PAdES, XAdES)
- Протокол проверки сертификатов и подписанных документов

Решения ТК 26

- XX заседание (ноябрь 2017г.)
  - Провести изучение вопроса о потребностях в разработке документов по стандартизации процедур формирования и проверки ЭП сертификатов.
- XXI заседание (апрель 2018г.)
  - Разработка документов представляется важной, однако не хватает базовых документов по протокольным решениям и форматам. В план работ РГ включить: XMLDSig, TSP, OCSP.

План РГ

- XMLDSig – в 2018 году сформировать проект документа в ТК 26
- OCSP, TSP – в 2019 году сформировать проект документов в ТК 26
- Протокол проверки сертификатов и подписанных документов – в 2019 году сформировать проект документа в ТК 26

О ходе работ

- XMLDSig – готовится под руководством экспертов КриптоПро, первая редакция будет рассмотрена на осеннем заседании РГ
- OCSP, TSP – готовится под руководством экспертов КриптоПро, первая редакция планируется к рассмотрению на заседании РГ весной 2019г.
- Протокол проверки сертификатов и подписанных документов – готовится под руководством экспертов Газинформсервис, планируется к рассмотрению на заседании РГ весной 2019г.

СПАСИБО ЗА ВНИМАНИЕ!

КРИПТО-ПРО – ключевое слово в защите информации

http://www.cryptopro.ru
spv@cryptopro.ru
svs@cryptopro.ru
Тел./факс:
+7 (495) 995-48-20