**Часові штемпелі - Time Stamp Protocol (TSP)**

Timestamp – часовий штемпель, підтверджує наявність документу в певний момент часу (коли був створний документ ми не знаємо, лише можемо підтвердити наявність)

Нова третя довірена сторона TTP: TSP-сервер (TSA) – уповноважена інстанція для видачі часових штемпелів. Стандарти: R

FC 3161, ISO/IEC - 1.2002

A picture containing text, blackboard

Description automatically generatedОсосбливості:

1. принципово анонімний
2. TSA абороняється зберігати ідентичні дані користувачів
3. TSA може лише видавати часові штемпелі (позначається у Extended Key Usage)

Запит: Time Stamp Request = SEQ {

* version INTEGER v1,
* messageImprint SEQ{
* hashAlg AlgId, hashedMessage OCTET STRING} – геш документа, має форму сіквенса і складається з алгоритму і геша,
* reqPolicy OID OPT, користувач може попросити сервер використовувати певну політику
* nonce OCTET STRIG OPT, користувач може використовувати нонси для захисту від атак
* certReq BOOLEAN DEFAULT FALSE, користувач може заросити сертифікат разом з часом,
* extensions [0] Extensions OPT

}

reqPolicy може передбачати відості про сфери використання таких штампелів і може фіксувати наявність доступу до аудиу

Відповідь: Time Stamp Response = SEQ {

* Status PKIStatusInfo – Статус,
* timeStampToken ContentInfo OPT, - власне часовий штемпель, включається якщо попереднє поле = 1 або 0. Тип: Signed Data, контент: TSTokenInfo, id: 1.2.840.1.9.16.1.4

}

Signed Data:

* Використовується сертифікація за S/MIME ( розширення ESS certificateID)
* сертифікат TSA включається у поле certs

TSTokenInfo= SEQ{

* Version INTEGER,
* Policy OID,
* messageImprint – копія із запиту гешу докумнта,
* serialNumber INTEGER -довжина 0...2^160-1
* genTime GenerilizedTime,
* ordering BOOLEAN OPT – якщл правда, то усі видані часові штемпи нумеруються хронологічно,
* accuracy Accuracy OPT,
* nonce INTEGER OPT - із запиту якщо є
* tsa [0] GeneralName OPT

}

**Розширені електроні підписи CMS Advanced Signatures (CAdES)**

RFC 5126

ETSI TS 101 733

1. BES(basic electronic sign) – бащовий тип без зайвих выдомомстей + часовий штемпелы на даны на якы ставиться пыдпис (Content Time Stamp) + ESS Signing Certificate v2
2. EPES (explicit policy abased ES) – BES + Signing policy теж базовий

Сфери використання таких типів – онлайн перевірка.

Розширені типи:

1. T = BES + Signature TimeStamp
2. C = T + посилання на усі необхідні сертфікати і посилання на усі необхідні CBC/OCBP – відп.
3. X Long = C + усі необхідні відомості про статус

X type 1 = C + часовий штепмепь на C

X type 2 = C + часовий штемпель на атрибути

X long Type ½

1. A = X Long Type ½ + часовий штемпель на увесь документ

Постановка підпису із відтермінування (retention period)

A blackboard with white writing

Description automatically generated with low confidence