RFC 3161 bis
Time-stamp Protocol

Denis Pinkas. Bull SAS
Lead editor of RFC 3161

Minneapolis - November 2008

Algorithm agility

Page 8 :

> **« The certificate identifier (ESSCertID) of the TSA certificate MUST be included as a signerInfo attribute inside a SigningCertificate attribute »**

- ESSCertID mandates the use of SHA-1.
- Other hash algorithms should be usable.
- There is the need to allow the use of ESSCertIDv2 defined in RFC 5035 and to maintain backwards compatibility.
- This change has been requested by ETSI TC ESI (**T**echnical **C**ommittee **E**lectronic **S**ignature & **I**nfrastructure)

Alignment with RFC 3628

- RFC 3628 “Policy Requirements for Time-Stamping Authorities”, is an Informational RFC, that makes the difference between a time-stamping unit (TSU) and a time-stamping authority (TSA).
- TSA: Time-Stamping Authority: authority which issues time-stamp tokens.
- TSU: Time-Stamping Unit: set of hardware and software which is managed as a unit and has a single time-stamp token signing key active at a time.
- The private key belongs to a TSU, rather than to a TSA which manages one or more TSUs.
- That distinction should be made within the document.
- Note: RFC 3628 is equivalent to ETSI TS 102 023 V 1.2.1 (2002-06).

Difference between a TSA and a TSS

- Page 5:

  If the TSA does not recognize the hash algorithm or knows that the hash algorithm is weak (a decision left to the discretion of each individual TSA), then the TSA SHOULD refuse to provide the time-stamp token by returning a pkiStatusInfo of 'bad_alg'.

- The answer is provided by the Time-Stamping *Service* (rather then the TSA, which is an administrative authority. Proposed rewording:

  If the TSS does not recognize the hash algorithm or knows that the hash algorithm is weak (a decision left to the discretion of each individual TSS), then the TSS SHOULD refuse to provide the time-stamp token by returning a pkiStatusInfo of 'bad_alg'.

Proposed definition for a TSS

- Time-Stamping Service (TSS):

  a service providing time-stamp tokens by means of one or more time-stamping units managed by one time-stamping authority.

ASN.1 module

- A new ASN.1 module which references the latest RFCs is anticipated.
- That module will keep the ASN.1 unchanged, unless ESSCerIDv2. is supported.
- The new module will include for information, the OID of the module that defines ESSCerIDv2 (RFC 5035).

New patent

- ETSI TC ESI has become aware of the following patent which should be added to the list:
  - # 7,047,404 Method and apparatus for self-authenticating digital records
  - Filing date: May 16, 2000
  - Issued: May 16, 2006
  - Inventors: Doonan, Wes; Wettlaufer, Albert J.; Lewis, Rone H.; Haber, Stuart A. (assignee) Surety LLC (Herndon, VA, US)
- However, it might be interesting to check whether this patent does not make use of information publicly available prior to the publication of ETSI ES 201 733 in year 2000.

References to ISO documents

- Informative references should be added to:
  - ISO 18 014-1 Time-stamping services – Part 1. Framework.
  - ISO 18 014-2 Time-stamping services – Part 2. Mechanisms producing independent tokens.
  - ISO18 014-3 Time-stamping services – Part 3. Mechanisms producing linked tokens.

Conclusion

- Permission is requested to the co-chairs to issue a draft document as:

  draft-ietf-pkix-rfc3161bis-00.txt