RFC 3161 bis
Time-stamp Protocol
draft-ietf-pkix-rfc3161-01.txt

Denis Pinkas. Bull SAS.
Lead editor of RFC 3161

San Francisco - March 23, 2009

Status

A draft has been issued in February 2009.
Major differences from RFC 3161 [RFC3161] are summarized below:

- The use of hash function different from SHA1 [SHA1] for CertID is allowed through the support of RFC 5035 [ESSV2].

- A difference between a time-stamping unit (TSU) and a TSA (time-stamping authority) has been introduced in order to align with RFC 3628 (alias ETSI TS 102 023 : « Policy requirements for Time-Stamping Authorities ».

- Time-Stamping Authorities manage Time-Stamping Units (TSUs), but do not issue Time-Stamp Tokens (TSTs) which are signed by TSUs.

- A difference between a Time-Stamping Service and a Time-Stamping Unit has been introduced. A client talks to a service, i.e., a Time-Stamping Service, not a TSU nor a TSA. A time-stamping service may support more than one time-stamping unit.

- As a consequence, the DN of the TSU certificate is structured to allow the separation of the DN of the TSA. The CN component of the DN identifies the TSU managed by that TSA.

- A new normative ASN1 module has been added to refer to the ASN.1 modules from the latest RFCs. Since the ASN.1 is unchanged when ESSCertV2 is unused, the previous module has been kept for information.

- Informative references to ISO 18014-1 [ISO18014-1], ISO 18014-2 [ISO18014-2] and ISO 18014-3 [ISO18014-3] have been added.

Comments received: essCertIDv2

- Stefan first said that ESSCertID was not needed, but then : “as essCertIDv2 is standardized and has been a focus for EU work in relation to time stamps, it is probably reasonable to allow essCertIDv2 to be used with RFC 3161 time stamps ».

- Stefan noticed that there is the need to find two collisions (one on the certificate on one on ESSCertID) to change, without noticing it, the TSU certificate.

- I suggest that Stefan provides some text in the security considerations section on this issue.

Comments received: diff. between TSA, TSU & TSS

- There are different opinions:
  - Some support it, some don't.

- The difference between TSA & TSU became needed when ETSI wrote the policy document on Time-Stamping Authorities:
  - An authority manages the time-stamping units. Certificates from TSUs can be revoked. A Time-Stamping Authority is never revoked, since it has no certificate of its own. Creating a new TSU certificate is no problem.

- The difference between TSA and TSS highlights the fact that a client talks to a port and will receive:
  - an error, unsigned, from the TSS (Time-Stamping Service), or
  - a TST signed by one TSU. The right TSU may be selected from the reqPolicy field, or among a set of TSUs for performance reasons.

The ways to progress

- There are two possible paths forwards:
  - to issue an RFC that replaces RFC 3161, or
  - to issue an update to RFC 3161.

- If it would be an update, Stefan proposed to :
  - add the option to use essCertIDv2, AND
  - to include an informational Annex explaining the basic difference in terminology between RFC 3161 and RFC 3628.

    Most importantly this informational text would explain that TSU in the policy document corresponds to TSA in the protocol.

Comments received: co-authors names

- The previous co-editors have been contacted, but declined to participate to the writing and to the discussions on the list about RFC 3161bis.
- Should their names remain as co-editors (without e-mail addresses), or
  should their names be mentioned in the acknowledgment section (with their permission) ?