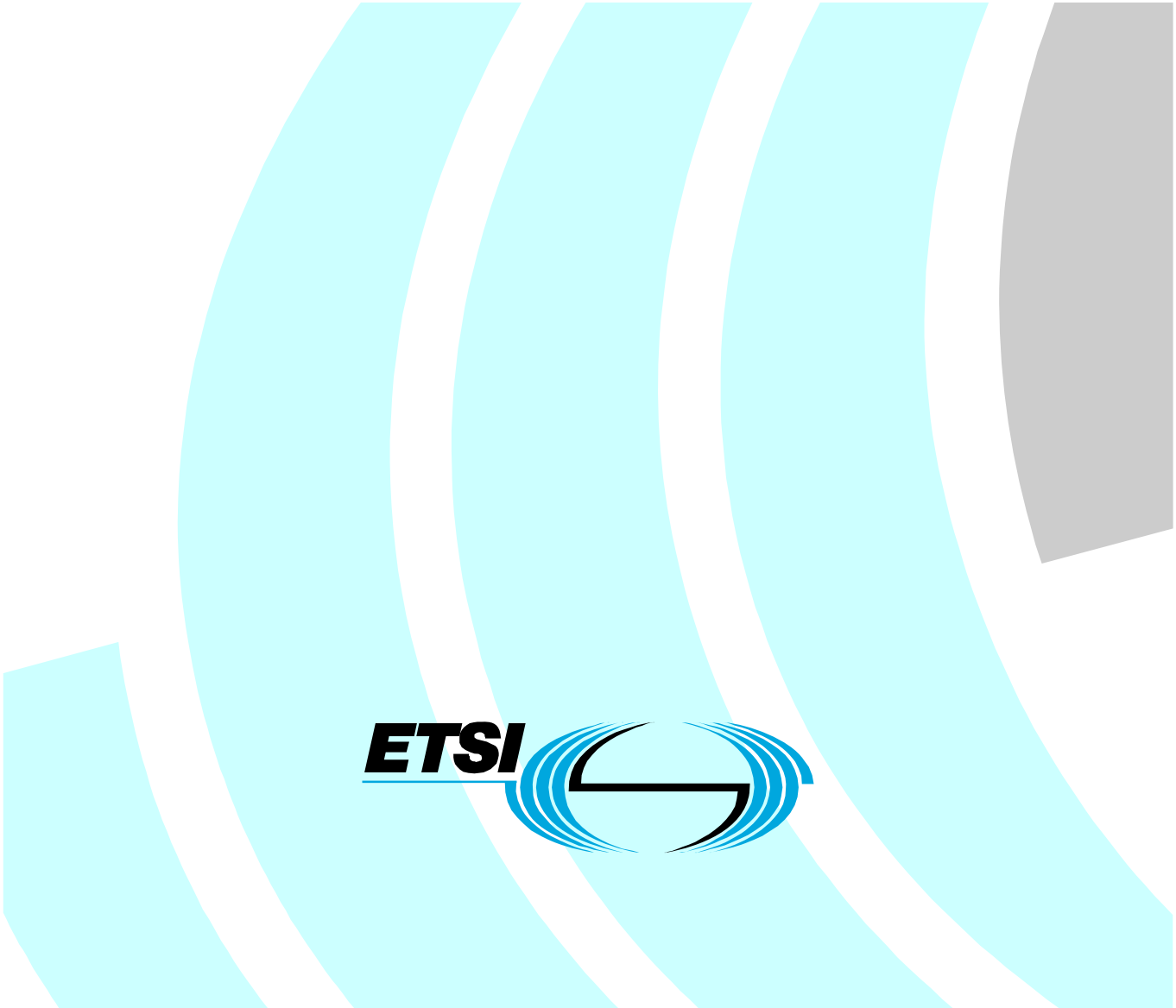
ETSI TS 101 861 V1.4.1 (2011-07)

Technical Specification

Electronic Signatures and Infrastructures (ESI); Time stamping profile



Reference
RTS/ESI-000110

Keywords
electronic signature, IP, security

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://ipr.etsi.org).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Technical Specification (TS) has been produced by ETSI Technical Committee Electronic Signatures and Infrastructures (ESI).

Background

Time Stamping is critical for electronic signatures in order to know whether the digital signature was affixed during the validity period of the certificate. To this respect, electronic signatures must be time stamped during the life time of the corresponding certificate.

A Time Stamp Protocol (TSP) has been defined by the IETF. The present document limits the number of options by placing some additional constraints.

1 Scope

The present document is based on the Time Stamp Protocol (TSP) from RFC 3161 [1] including optional ESSCertIDv2 update in RFC 5816 [9].

It defines what a Time Stamping client must support and what a Time Stamping Server must support.

2 References

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

NOTE: While any hyperlinks included in this clause were valid at the time of publication ETSI cannot guarantee their long term validity.

2.1 Normative references

The following referenced documents are necessary for the application of the present document.

[1] IETF RFC 3161: "Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)".

[2] Void.

[3] Void.

[4] Void.

[5] Void.

[6] Void.

[7] ISO 9594-6: "Information technology - Open Systems Interconnection - The Directory: Selected attribute types".

[8] ITU-T Recommendation X.520: "Information technology - Open Systems Interconnection - The Directory: Selected attribute types".

[9] IETF RFC 5816: "ESSCertIDV2 update to RFC 3161".

[10] ETSI TS 102 176-1: "Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms".

NOTE 1: It is recommended that the latest version of TS 102 176-1 is applied to new systems.

NOTE 2: References to specific algorithms changed to TS 102 176-1.

2.2 Informative references

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] ETSI TS 102 023: "Electronic Signatures and Infrastructures (ESI); Policy requirements for time-stamping authorities".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

time-stamping unit: set of hardware and software which is managed as a unit and has a single time-stamping signing key active at a time

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

HTTP	HyperText Transfer Protocol
TSA	Time Stamping Authority
TSP	Time Stamp Protocol

4 Requirements for a TSP client

4.1 Void

4.2 Profile for the format of the request

4.2.1 Parameters to be supported

The following requirement applies: no extension field shall be present.

4.2.2 Hash Algorithms to be used

Hash algorithms supported for the time-stamp data shall be as specified in clause A.8 of TS 102 176-1 [10]. This should take into account the expected duration of the time-stamp and recommended hash functions versus time given in clause 9.2 of TS 102 176-1 [10].

NOTE: In the case of old time-stamps that were applied at a time when use of other algorithms were accepted then implementations may raise a warning to users and may indicate that the time-stamp remains valid even if the algorithms is no longer considered acceptable.

4.3 Profile for the format of the response

4.3.1 Parameters to be supported

The following requirements apply:

- the accuracy field must be supported and understood;
- the nonce parameter must be supported;
- no extension is required to be supported.

NOTE: A TSA may not support ordering hence clients should not depend on the ordering of time-stamps.

4.3.2 Algorithms to be supported

Time-stamp token signature algorithms to be supported shall be as specified in clause A.8 of TS 102 176-1 [10].

NOTE: In the case of old time-stamps that were applied at a time when use of other algorithms were accepted then implementations may raise a warning to users and may indicate that the time-stamp remains valid even if the algorithms is no longer considered acceptable.

4.3.3 Key lengths to be supported

Signature algorithm key lengths for the selected signature algorithm should be supported as recommended in clause 9.3 of TS 102 176-1 [10].

5 Requirements for a TSP server

5.1 Profile for the format of the request

5.1.1 Parameters to be supported

The following requirements apply:

- the nonce must be supported;
- certReq must be supported;
- no extension is required to be supported.

5.1.2 Algorithms to be supported

Hash algorithms for the time-stamp data to be supported shall be as specified in clause A.8 of TS 102 176-1 [10]. This should take into account the expected duration of the time-stamp and recommended hash functions versus time given in clause 9.2 of TS 102 176-1 [10].

NOTE: In the case of old time-stamps that were applied at a time when use of other algorithms were accepted then implementations may raise a warning to users and may indicate that the time-stamp remains valid even if the algorithms is no longer considered acceptable.

5.2 Profile for the format of the response

5.2.1 Parameters to be supported

The following requirements apply:

- a genTime parameter limited to represent time with one second is required;
- a minimum accuracy of one second is required;
- an ordering parameter missing or set to false is required;
- no extension is required to be generated;
- no extension shall be critical.

5.2.2 Structure for the name of the issuing TSP server

The name of the issuing TSP server shall contain an appropriate subset of the following attributes (defined in ISO 9594-6 [7] and ITU-T Recommendation X.520 [8]):

- countryName;
- stateOrProvinceName;
- organizationName;
- commonName.

The countryName, when applicable, identifies the name of the country where the TSA is established (which is not necessarily the name of the country where the time-stamping unit is located).

The stateOrProvinceName is an optional component that identifies a geographical subdivision in which the TSA is established.

The organizationName shall be present. It identifies the TSA responsible for managing the time-stamping unit. That name should be an officially registered name of the TSA.

The commonName shall be present. It specifies an identifier for the time-stamping unit. Within the TSA, the attribute commonName uniquely identifies the time-stamping unit used.

5.2.3 Algorithms to be supported

Time-stamp token signature algorithms shall be supported as specified in clause A.8 of TS 102 176-1 [10].

NOTE: In the case of old time-stamps that were applied at a time when use of other algorithms were accepted then implementations may raise a warning to users and may indicate that the time-stamp remains valid even if the algorithms is no longer considered acceptable.

5.2.4 Key lengths be supported

It is recommended that key length for the selected signature algorithm is as recommended in clause 9.3 of TS 102 176-1 [10].

5.2.5 TSA Certificates

It is recommended that certificates issued for TSA are as specified in clauses A.9 and A.10 of TS 102 176-1 [10].

5.2.6 TSA Certificate Identifier

The TSA certificate identifier must be present in the TSA signature as specified in RFC 3161 [1] (ESSCertID) or RFC 5816 [9] (ESSCertID or ESSCerIDv2).

6 Profiles for the transport protocols to be supported

One on-line protocol and one store and forward protocol must be supported for every Time Stamping Authority (TSA).

Among the four protocols that are defined in the RFC 3161 [1], the following protocol should be supported:

- the Time Stamp Protocol via HTTP (section 3.4 from the RFC 3161 [1]).

7 Object identifiers of the cryptographic algorithms

Object identifiers for the recommended hashing and signature algorithms are specified in annex F of TS 102 176-1 [10].

Annex A (informative): Structure for the policy field

When the TSA conforms to TS 102 023 [i.1], then the policy field from the TSTInfo structure should contain the identifier for the baseline time-stamp policy defined in the present document, which is:

```
itu-t(0) identified-organization(4) etsi(0) time-stamp-policy(02023)
policy-identifiers(1) baseline-ts-policy (1)
```

If this identifier is not included, a TSA may define its own policy which enhances this policy.

Annex B (informative): Bibliography

- Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.
- IETF RFC 2459: "Internet X.509 Public Key Infrastructure Certificate and CRL Profile".
- IETF RFC 2630: "Cryptographic Message Syntax".
- FIPS Publication 186: "Digital Signature Standard (DSS)".
- H. Dobbertin, A. Bosselaers, B. Preneel: "RIPEMD-160, a strengthened version of RIPEMD", Fast Software Encryption, LNCS 1039, D.Gollmann, Ed., Springer-Verlag, 1996, pp. 71-82.
- A. Menezes, P. van Oorschot, S. Vanstone: "Handbook of Applied Cryptography", CRC press.
- A. Bosselaers, H. Dobbertin, B. Preneel: "The RIPEMD-160 cryptographic hash function", Dr. Dobb's Journal, Vol. 22, No. 1, January 1997, pp. 24-28.
- B. Preneel, A. Bosselaers, H. Dobbertin: "The cryptographic hash function RIPEMD-160", CryptoBytes, Vol. 3, No. 2, 1997, pp. 9-14.

History

Document history		
V1.1.1	September 2001	Publication
V1.2.1	March 2002	Publication
V1.3.1	January 2006	Publication
V1.4.1	July 2011	Publication