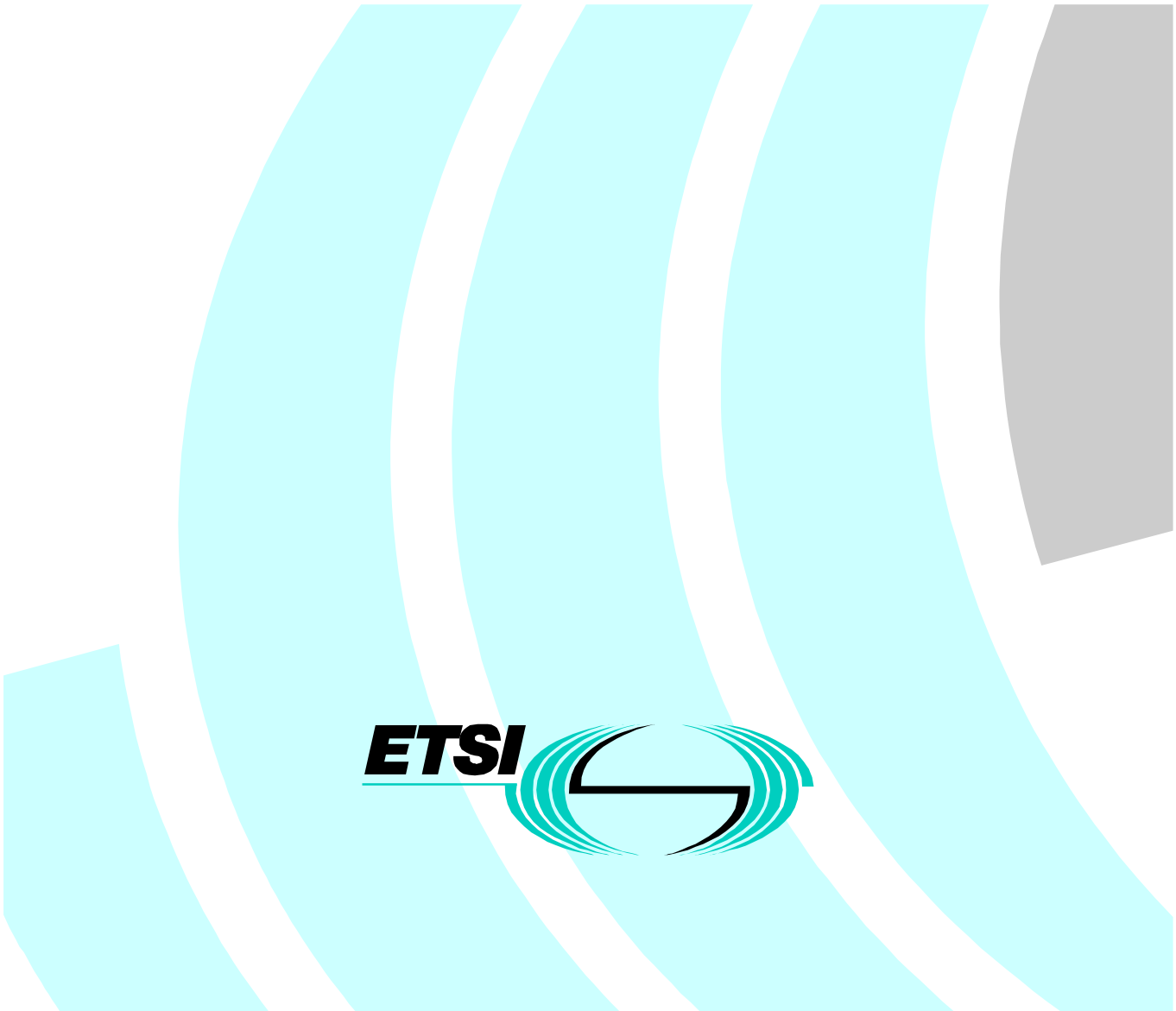
ETSI TS 101 861 V1.1.1 (2001-08)

Technical Specification

Time stamping profile



Reference
DTS/SEC-004004

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

Important notice

Individual copies of the present document can be downloaded from:
http://www.etsi.org

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at http://www.etsi.org/tb/status/

If you find errors in the present document, send your comment to:
editor@etsi.fr

Copyright Notification

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://www.etsi.org/ipr).

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 Security (SEC).

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 has been defined by the IETF. The present document limits the number of options by placing some additional constraints.

1 Scope

This profile is based on the Time Stamp Protocol (TSP) from the IETF, RFC 3161 [1].

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

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication and/or edition number or version number) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies.

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

[2] FIPS Publication 180-1 (1995): "Secure Hash Standard".

[3] RFC 2313 (1998): "PKCS 1: RSA Encryption Version 1.5" - B. Kaliski.

[4] RFC 1321 (1992): "The MD5 Message-Digest Algorithm" - R. Rivest.

[5] RFC 2437: "PKCS #1: RSA Cryptography Specifications, Version 2.0".

[6] ISO/IEC 10118-3: "Information technology - Security techniques - Hash-functions - Part 3: Dedicated hash-functions", International Organization for Standardization, Geneva, Switzerland.

3 Definitions, symbols and abbreviations

3.1 Definitions

No specific definition is made in the present document.

3.2 Symbols

No specific symbol is used in the present document.

3.3 Abbreviations

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

DSA	Digital Signature Algorithm. A signature algorithm used in conjunction with SHA-1
HTTP	HyperText Transfer Protocol
MD5	Message Digest 5. A one way hash function that provides an 128 bits output
PKCS	Public Key Cryptographic Standards. Standards published by RSA, Labs
RIPEMD-160	Race Integrity Primitives Evaluation Message Digest 160. A one way hash function that provides a 160 bits output
RSA	Rivest Shamir Adleman . An algorithm usable either for signature or encryption
SHA-1	Secure Hash Function 1. A one way hash function that provides a 160 bits output

4 Requirements for a TSP client

4.1 Profile for the format of the request

4.1.1 Parameters to be supported

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

4.1.2 Algorithms to be used

The following hash algorithms may be used to hash the information to be time-stamped: SHA-1, MD5, RIPEMD-160. It is recommended to use either SHA-1 or RIPEMD-160.

4.2 Profile for the format of the response

4.2.1 Parameters to be supported

The following requirements apply:

- the accuracy field must be supported and understood,
- the ordering parameter either missing or set to FALSE must be supported,
- the nonce parameter must be supported,
- no extension is required to be supported.

4.2.2 Algorithms to be supported

The following signature algorithm must be supported:

- SHA-1 with RSA.

4.2.3 Key lengths to be supported

For the RSA algorithm, key lengths of 1 024 bits must be supported. Key lengths of 2 048 bits should be supported.

For the DSA algorithm, the larger of the two primes, p and q, shall be at least 1 024 bits.

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

The following hash algorithms must be recognized: SHA-1, MD5, RIPEMD-160.

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 Algorithms to be supported

The following hash algorithms must be supported: SHA-1, MD5, RIPEMD-160.

The following signature algorithm must be supported:

- SHA1 with RSA.

The signature algorithm with SHA-1 and the RSA encryption algorithm is implemented using the padding and encoding conventions described in RFC 2313 [3].

5.2.3 Key lengths be supported

For the RSA algorithm, key lengths of 1024 bits must be supported. Key lengths of 2048 bits may be supported.

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.

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

7.1 Hash algorithms

7.1.1 SHA-1

The SHA-1 digest algorithm is defined in FIPS Pub 180-1 [2]. The algorithm identifier for SHA-1 is:

```
sha-1 OBJECT IDENTIFIER ::= { iso(1) identified-organization(3) oiw(14) secsig(3) algorithm(2) 26 }
```

The AlgorithmIdentifier parameters field is optional. If present, the parameters field shall contain an ASN.1 NULL.

Implementations should accept SHA-1 AlgorithmIdentifiers with absent parameters as well as NULL parameters.

Implementations should generate SHA-1 AlgorithmIdentifiers with NULL parameters.

7.1.2 MD5

The MD5 digest algorithm is defined in RFC 1321 [4]. The algorithm identifier for MD5 is:

```
md5 OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) digestAlgorithm(2) 5 }
```

The AlgorithmIdentifier parameters field shall be present, and the parameters field shall contain NULL.

Implementations may accept the MD5 AlgorithmIdentifiers with absent parameters as well as NULL parameters.

7.1.3 RIPEMD-160

The RIPEMD-160 digest algorithm is defined in ISO/IEC 10118-3 [6].

Information about RIPEMD-160 can also be found in the following publications (see bibliography in annex A):

- "RIPEMD-160, a strengthened version of RIPEMD";
- "Handbook of Applied Cryptography";
- "The RIPEMD-160 cryptographic hash function";
- "The cryptographic hash function RIPEMD-160".

At the time of publication of the present document, this information was available at the following address:

http://www.esat.kuleuven.ac.be/~bosselae/ripemd160.html#Outline

The algorithm identifier for RIPEMD-160 is:

```
{iso(1) identified-organization(3) teletrust(36) algorithm(3) hashAlgorithm(2) ripemd160(1)}
```

7.2 Signature algorithm

The RSA signature algorithm is defined in RFC 2437 [5]. RFC 2437 [5] specifies the use of the RSA signature algorithm with the SHA-1 and MD5 message digest algorithms.

When the hash function to be used is SHA-1, then the OID should be:

```
sha1WithRSAEncryption OBJECT IDENTIFIER ::= { iso(1) member-body(2) US(840) rsadsi(113549)
pkcs(1) pkcs-1(1) 5}
```

Annex A (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.
- RFC 2459: "Internet X.509 Public Key Infrastructure Certificate and CRL Profile".
- 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	August 2001	Publication