ETSI TS 119 422 V1.0.1 (2015-07)

Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp profiles

Reference
RTS/ESI-0019422-TS

Keywords
electronic signature, security, time-stamping,
trust services

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 4
Foreword 4
Modal verbs terminology 4
Introduction 4
1 Scope 5
2 References 5
2.1 Normative references 5
2.2 Informative references 5
3 Definitions and abbreviations 6
3.1 Definitions 6
3.2 Abbreviations 6
4 Requirements for a time-stamping client 6
4.1 Profile for the format of the request 6
4.1.1 Core requirement 6
4.1.2 Parameters to be supported 6
4.1.3 Hash algorithms to be used 6
4.2 Profile for the format of the response 7
4.2.1 Core requirement 7
4.2.2 Parameters to be supported 7
4.2.3 Algorithms to be supported 7
4.2.4 Key lengths to be supported 7
5 Requirements for a time-stamping server 7
5.1 Profile for the format of the request 7
5.1.1 Core requirement 7
5.1.2 Parameters to be supported 7
5.1.3 Algorithms to be supported 7
5.2 Profile for the format of the response 7
5.2.1 Core requirement 7
5.2.2 Parameters to be supported 8
5.2.3 Algorithms to be used 8
6 TSU certificate profile 8
6.1 General requirements 8
6.2 Subject name requirements 8
6.3 Key lengths requirements 8
6.4 Key usage requirements 8
6.5 Algorithm requirements 9
7 Profiles for the transport protocols to be supported 9
8 Object identifiers of the cryptographic algorithms 9
9 Additional requirements for Regulation (EU) No 910/2014 9
9.1 Regulation statement 9
Annex A (normative): Structure for the policy field 10
Annex B (normative): ASN.1 declarations 11
History 12

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).

The present document was previously published as ETSI TS 101 861 [i.2].

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Introduction

The present document is aiming to meet the general requirements of the international community to provide trust and confidence in electronic transactions including, amongst others, applicable requirements from Regulation (EU) No 910/2014 [i.3].

Time-stamping is critical for digital signatures in order to know whether the digital signature was affixed during the validity period of the certificate. One method of assuring the signing time is to affix a time-stamp bound to the signature as defined in IETF RFC 3161 [1].

IETF RFC 3161 [1] defines a time-stamp protocol and a time-stamp token format. The present document limits the number of options by placing some additional constraints.