ICS 35.240.30 SLOVENSKÁ TECHNICKÁ NORMA September 2023

STN	**Elektronické podpisy a infraštruktúry (ESI) Požiadavky politiky a bezpečnostné požiadavky pre poskytovateľov dôveryhodných služieb vydávajúcich časové pečiatky**	**STN EN 319 421 V1.2.1** 87 9421

Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps

Táto norma obsahuje anglickú verziu európskej normy.
This standard includes the English version of the European Standard.

Táto norma bola oznámená vo Vestníku ÚNMS SR č. 08/23

Obsahuje: EN 319 421 V1.2.1:2023

137255

Úrad pre normalizáciu, metrológiu a skúšobníctvo Slovenskej republiky, 2023
Slovenská technická norma a technická normalizačná informácia je chránená zákonom č. 60/2018 Z. z. o technickej normalizácii v znení neskorších predpisov.

ETSI EN 319 421 V1.2.1 (2023-05)

Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps

Reference
REN/ESI-0019421v1.2.1

Keywords
e-commerce, 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 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Important notice

The present document can be downloaded from:
https://www.etsi.org/standards-search

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the prevailing version of an ETSI deliverable is the one made publicly available in PDF format at www.etsi.org/deliver.

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
https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

If you find a security vulnerability in the present document, please report it through our
Coordinated Vulnerability Disclosure Program:
https://www.etsi.org/standards/coordinated-vulnerability-disclosure

Notice of disclaimer & limitation of liability

The information provided in the present deliverable is directed solely to professionals who have the appropriate degree of experience to understand and interpret its content in accordance with generally accepted engineering or other professional standard and applicable regulations.
No recommendation as to products and services or vendors is made or should be implied.
In no event shall ETSI be held liable for loss of profits or any other incidental or consequential damages.

Any software contained in this deliverable is provided "AS IS" with no warranties, express or implied, including but not limited to, the warranties of merchantability, fitness for a particular purpose and non-infringement of intellectual property rights and ETSI shall not be held liable in any event for any damages whatsoever (including, without limitation, damages for loss of profits, business interruption, loss of information, or any other pecuniary loss) arising out of or related to the use of or inability to use the software.

Copyright Notification

No part may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm except as authorized by written permission of ETSI.
The content of the PDF version shall not be modified without the written authorization of ETSI.
The copyright and the foregoing restriction extend to reproduction in all media.

© ETSI 2023.
All rights reserved.

Contents

Intellectual Property Rights 5
Foreword 5
Modal verbs terminology 5
Introduction 6
1 Scope 7
2 References 7
2.1 Normative references 7
2.2 Informative references 8
3 Definitions of terms, symbols, abbreviations and notation 9
3.1 Terms 9
3.2 Symbols 9
3.3 Abbreviations 10
3.4 Notation 10
4 General concepts 11
4.1 General policy requirements concepts 11
4.2 Time-stamping services 11
4.3 Time-Stamping Authority (TSA) 11
4.4 Subscriber 11
4.5 Time-stamp policy and TSA practice statement 12
5 Introduction to time-stamp policies and general requirements 12
5.1 General requirements 12
5.2 Policy name and identification 12
5.3 User community and applicability 13
5.3.1 Best practices time-stamp policy 13
6 Policies and practices 13
6.1 Risk assessment 13
6.2 Trust Service Practice Statement 13
6.3 Terms and conditions 13
6.4 Information security policy 13
6.5 TSA obligations 14
6.5.1 General 14
6.5.2 TSA obligations towards subscribers 14
6.6 Information for relying parties 14
7 TSA management and operation 14
7.1 Introduction 14
7.2 Internal organization 14
7.3 Personnel security 15
7.4 Asset management 15
7.5 Access control 15
7.6 Cryptographic controls 15
7.6.1 General 15
7.6.2 TSU key generation 15
7.6.3 TSU private key protection 16
7.6.4 TSU public key certificate 16
7.6.5 Rekeying TSU's key 17
7.6.6 Life cycle management of signing cryptographic hardware 17
7.6.7 End of TSU key life cycle 17
7.7 Time-stamping 18
7.7.1 Time-stamp issuance 18
7.7.2 Clock synchronization with UTC 18
7.8 Physical and environmental security 19
7.9 Operation security 19

7.10 Network security 20
7.11 Incident management 20
7.12 Collection of evidence 20
7.13 Business continuity management 20
7.14 TSA termination and termination plans 21
7.15 Compliance 21

8 Additional requirements for qualified electronic time-stamps as per Regulation (EU) No 910/2014 21
8.1 TSU public key certificate 21
8.2 TSA issuing non-qualified and qualified electronic time-stamps as per Regulation (EU) No 910/2014 21

Annex A (informative): Potential liability in the provision of time-stamping services 22

Annex B (informative): Model TSA disclosure statement 23

B.1 Introduction 23

B.2 TSA disclosure statement structure 23

Annex C (informative): Coordinated Universal Time (UTC) 25

Annex D (informative): Long term verification of time-stamps 26

Annex E (informative): Regulation (EU) No 910/2014 and qualified electronic time-stamp policy cross-reference 27

Annex F (informative): Possible implementation architectures - time-stamping service 28

F.1 Managed time-stamping service 28

F.2 Selective alternative quality 28

Annex G (informative): Major changes from ETSI TS 102 023 30

Annex H (informative): Conformity Assessment Check list 31

Annex I (informative): Change History 32

History 33

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are 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 (https://ipr.etsi.org/).

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, 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.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

Foreword

This European Standard (EN) has been produced by ETSI Technical Committee Electronic Signatures and Infrastructures (ESI).

The present document is derived from the requirements specified in ETSI TS 102 023 [i.8].

National transposition dates	
Date of adoption of this EN:	1 May 2023
Date of latest announcement of this EN (doa):	31 August 2023
Date of latest publication of new National Standard or endorsement of this EN (dop/e):	29 February 2024
Date of withdrawal of any conflicting National Standard (dow):	29 February 2024

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.4].

The Regulation includes requirements for Trust Service Providers (TSP) providing services to the public, including TSPs issuing time-stamps. Additionally, more specific requirements are identified in the Regulation for a specific class of TSP called a Qualified TSP, with further specific requirements for those Qualified TSPs which issue qualified time-stamps. The present document is aimed to meet the requirements of the Regulation for both Qualified and non-Qualified TSPs issuing Qualified and non-Qualified electronic time-stamps respectively.

In order to verify an electronic signature, it can be necessary to prove that the signature from the signer was applied when the signer's certificate was valid. This is necessary in two circumstances:

1) during the validity period of the signer's certificate, should the signer's certificate be revoked before the end of its validity, e.g. because the signer's private key has been compromised;

2) after the end of the validity period of the signer's certificate, since CAs are not mandated to process revocation status information beyond the end of the validity period of the certificates they have issued.

One method consists to use a time-stamp which allows proving that a datum existed before a particular time. This technique allows proving that the signature was generated before the date contained in the time-stamp. Policy requirements to cover that case are the primary aim of the present document.

However, these policy requirements allow addressing other needs.

Time-stamping is gaining an increasing interest by the business sector and is becoming an important component of digital signatures, this is commonly based upon the Time-Stamp protocol from the IETF RFC 3161 [i.2] which is profiled in ETSI EN 319 422 [5]. Agreed minimum security and quality requirements are necessary in order to ensure trustworthy validation of long-term digital signatures.

1 Scope

The present document specifies policy and security requirements relating to the operation and management practices of TSPs issuing time-stamps.

These policy requirements are applicable to TSPs issuing time-stamps. Such time-stamps can be used in support of digital signatures or for any application requiring to prove that a datum existed before a particular time.

The present document can be used by independent bodies as the basis for confirming that a TSP can be trusted for issuing time-stamps.

The present document does not specify protocols used to access the TSUs.

NOTE 1: A time-stamping protocol is defined in IETF RFC 3161 [i.2] including optional update in IETF RFC 5816 [i.3] and profiled in ETSI EN 319 422 [5].

The present document does not specify how the requirements identified can be assessed by an independent party, including requirements for information to be made available to such independent assessors, or requirements on such assessors.

NOTE 2: See ETSI EN 319 403-1 [i.9] for guidance on assessment of TSP's processes and services.

NOTE 3: The present document references ETSI EN 319 401 [4] for general policy requirements common to all classes of TSP's services.

2 References

2.1 Normative 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 https://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.

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

[1] Recommendation ITU-R TF.460-6 (2002): "Standard-frequency and time-signal emissions".

[2] ISO/IEC 19790:2012: "Information technology -- Security techniques -- Security requirements for cryptographic modules".

[3] ISO/IEC 15408 (parts 1 to 3): "Information security, cybersecurity and privacy protection -- Evaluation criteria for IT security ".

[4] ETSI EN 319 401: "Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers".

[5] ETSI EN 319 422: "Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles".

[6] FIPS PUB 140-2 (2002): "Security Requirements for Cryptographic Modules".

[7] FIPS PUB 140-3 (2019): "Security Requirements for Cryptographic Modules".

2.2 Informative 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.

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

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 EN 319 122-1: "Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 1: Building blocks and CAdES baseline signatures".

[i.2] IETF RFC 3161 (2001): "Internet X.509 Public Key Infrastructure: Time-Stamp Protocol (TSP)".

[i.3] IETF RFC 5816: "ESSCertIDV2 update to RFC 3161".

[i.4] Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

[i.5] Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts.

[i.6] BIPM Circular T.

NOTE: Available from the BIPM website https://www.bipm.org/.

[i.7] ETSI TS 119 312: "Electronic Signatures and Infrastructures (ESI); Cryptographic Suites".

[i.8] ETSI TS 102 023: "Electronic Signatures and Infrastructures (ESI); Policy requirements for time-stamping authorities".

[i.9] ETSI EN 319 403-1: "Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment; Part 1: Requirements for conformity assessment bodies assessing Trust Service Providers".

[i.10] ETSI EN 319 411-1: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements".

[i.11] ETSI EN 319 411-2: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates".

[i.12] EN 419231: "Protection profile for trustworthy systems supporting time stamping", (produced by CEN).

[i.13] TS 419221-2: "Protection profiles for TSP Cryptographic modules - Part 2: Cryptographic module for CSP signing operations with backup", (produced by CEN).

[i.14] TS 419221-3: "Protection profiles for TSP Cryptographic modules - Part 3: Cryptographic module for CSP key generation services", (produced by CEN).

[i.15] TS 419221-4: "Protection profiles for TSP Cryptographic modules - Part 4: Cryptographic module for CSP signing operations without backup", (produced by CEN).

[i.16] EN 419221-5: "Protection profiles for TSP Cryptographic modules - Part 5: Cryptographic module for trust services", (produced by CEN).

[i.17] ETSI TS 119 612: "Electronic Signatures and Infrastructures (ESI); Trusted Lists".

koniec náhľadu – text ďalej pokračuje v platenej verzii STN