



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

Reference

RTS/ESI-0019421-TS

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

Important notice

The present document can be downloaded from:

<http://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 only prevailing document is the print of the Portable Document Format (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://portal.etsi.org/tb/status/status.asp>

If you find errors in the present document, please send your comment to one of the following services:

<https://portal.etsi.org/People/CommitteeSupportStaff.aspx>

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.

© European Telecommunications Standards Institute 2015.

All rights reserved.

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

Contents

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

7.12	Collection of evidence	17
7.13	Business continuity management	17
7.14	TSA termination and termination plans.....	17
7.15	Compliance.....	18
8	Additional requirements for Regulation (EU) No 910/2014.....	18
8.1	TSU public key certificate.....	18
Annex A (informative):	Potential liability in the provision of time-stamping services	19
Annex B (informative):	Model TSA disclosure statement	20
B.1	Introduction	20
B.2	TSA disclosure statement structure	20
Annex C (informative):	Coordinated Universal Time (UTC).....	22
Annex D (informative):	Long term verification of time-stamps.....	23
Annex E (informative):	Regulation (EU) No 910/2014 and qualified electronic time-stamp policy cross-reference	24
Annex F (informative):	Possible implementation architectures - time-stamping service.....	25
F.1	Managed time-stamping service.....	25
F.2	Selective alternative quality	25
Annex G (informative):	Major changes from ETSI TS 102 023.....	27
Annex H (informative):	Conformity Assessment Check list	28
History		29