

# ETSI TS 119 312 V1.1.1 (2014-11)



TECHNICAL SPECIFICATION

## **Electronic Signatures and Infrastructures (ESI); Cryptographic Suites**

---

**Reference**

DTS/ESI-0019312

---

**Keywords**e-commerce, electronic signature, security,  
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>

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:

[http://portal.etsi.org/chaicor/ETSI\\_support.asp](http://portal.etsi.org/chaicor/ETSI_support.asp)

---

**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 2014.

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 Maintenance of the document .....	9
5 Hash functions.....	10
5.1 General .....	10
5.2 Recommended hash functions .....	10
5.2.1 SHA-224 .....	10
5.2.2 SHA-256.....	10
5.2.3 SHA-384.....	11
5.2.4 SHA-512.....	11
5.2.5 SHA-512/256.....	11
5.3 Other hash functions.....	11
5.3.1 SHA-1 is no more recommended.....	11
5.3.2 WHIRLPOOL is no more recommended.....	11
5.3.3 SHA-3.....	12
6 Signature schemes .....	12
6.1 Signature algorithms.....	12
6.1.1 General.....	12
6.1.2 Recommended signature algorithms .....	12
6.1.2.1 RSA.....	12
6.1.2.2 DSA.....	13
6.1.2.3 Elliptic curve analogue of DSA based on a group $E(F_p)$ .....	13
6.1.2.4 Elliptic curve analogue of DSA based on a group $E(F_2^m)$ .....	14
6.1.2.5 EC-GDSA based on a group $E(F_p)$ .....	14
6.1.2.6 EC-GDSA based on a group $E(F_2^m)$ .....	14
6.1.2.7 Other EC-DSA variants for future applications .....	15
6.2 Key generation algorithms .....	15
6.2.1 General.....	15
6.2.2 Recommended key generation algorithms .....	15
6.2.2.1 Key and parameter generation algorithm rsagen1 .....	15
6.2.2.2 Key and parameter generation algorithm dsagen1 .....	16
6.2.2.3 Key and parameter generation algorithm ecgen1 for ecdsa-Fp.....	16
6.2.2.4 Key and parameter generation algorithm ecgen2 for ecdsa-F2m.....	17
6.2.2.5 Key and parameter generation algorithm ecgen1 for ecgdsa-Fp.....	17
6.2.2.6 Key and parameter generation algorithm ecgen2 for ecgdsa-F2m.....	17
7 Signature suites .....	17
7.1 General .....	17
7.2 Padding methods .....	18
7.3 Recommended signature suites .....	19
8 Random number generation methods.....	19
8.1 General .....	19

8.2	Recommended random number generation methods .....	20
8.2.1	General.....	20
8.2.2	Random generator requirements trueran.....	20
8.2.3	Random generator requirements pseuran.....	21
9	Recommended hash functions and key sizes versus time .....	22
9.1	Basis for the recommendations .....	23
9.2	Recommended hash functions versus time.....	23
9.3	Recommended key sizes versus time .....	23
10	Time period resistance of hash functions and keys .....	26
10.1	General notes.....	26
10.2	Time period resistance for hash functions.....	26
10.3	Time period resistance for signer's key .....	26
10.4	Time period resistance for trust anchors.....	26
10.5	Time period resistance for other keys.....	27
11	Practical ways to identify hash functions and signature algorithms.....	27
11.1	General .....	27
11.2	Hash functions and signature algorithms objects identified using OIDs.....	27
11.2.1	Hash functions .....	27
11.2.2	Signature algorithms .....	27
11.2.3	Signature suites .....	28
11.3	Hash functions and signature algorithms identified objects using URNs.....	28
11.3.1	Hash functions .....	28
11.3.2	Signature algorithms .....	28
11.3.3	Signature suites .....	29
11.4	Recommended hash functions and signature algorithms objects that do not yet have an OID or a description .....	29
<b>Annex A (normative): Algorithms for various data structures.....</b>		<b>30</b>
A.1	CAAdES and PAdES .....	30
A.2	XAdES .....	31
A.3	Signer's certificates.....	31
A.4	CRLs.....	32
A.5	OCSP responses .....	32
A.6	CA certificates.....	32
A.7	Self-signed certificates for CA issuing CA certificates.....	33
A.8	TSTs based on RFC 3161.....	33
A.9	TSU certificates.....	33
A.10	Self-signed certificates for CAs issuing TSU certificates .....	34
<b>Annex B (informative): Recommended key sizes (historical).....</b>		<b>35</b>
<b>Annex C (informative): Signature maintenance .....</b>		<b>36</b>
History .....		37