



**Electronic Signatures and Infrastructures (ESI);
Certificate Profiles;
Part 2: Certificate profile for certificates issued
to natural persons**

Reference

RTS/ESI-0019412-2-TS

Keywords

electronic signature, IP, profile, 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/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	4
Foreword.....	4
Modal verbs terminology.....	4
Introduction	4
1 Scope	5
2 References	5
2.1 Normative references	5
2.2 Informative references.....	6
3 Definitions and abbreviations.....	6
3.1 Definitions.....	6
3.2 Abbreviations	6
4 Void.....	7
5 General certificate profile requirements.....	7
5.1 Generic requirements	7
5.2 Basic certificate fields	7
5.2.1 Version.....	7
5.2.2 Void	7
5.2.3 Signature.....	7
5.2.4 Issuer.....	7
5.2.4.1 Legal person issuers	7
5.2.4.2 Natural person issuers	8
5.2.5 Void	8
5.2.6 Subject	8
5.2.7 Subject public key info	8
5.3 Void.....	9
5.4 Standard certificate extensions	9
5.4.1 Authority key identifier	9
5.4.2 Void	9
5.4.3 Key usage.....	9
5.4.4 Void	10
5.4.5 Certificate policies	10
5.4.6 Policy mappings.....	10
5.4.7 Subject alternative name	10
5.4.8 Issuer alternative name	10
5.4.9 Subject directory attributes	10
5.4.10 Void	10
5.4.11 Name constraints	10
5.4.12 Policy constraints.....	10
5.4.13 Extended key usage	10
5.4.14 CRL distribution points	10
5.4.15 Inhibit any-policy.....	10
5.4.16 Void	11
5.5 IETF RFC 5280 internet certificate extensions	11
5.5.1 Authority Information Access.....	11
5.5.2 Void	11
5.6 Void.....	11
5.6.1 Void	11
5.6.2 Void	11
6 EU qualified certificate requirements.....	11
6.1 EU QCStatements.....	11
6.2 Certificate policies.....	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 is part 2 of the multipart deliverable covering the Certificates Profiles. Full details of the entire series can be found in part 1 [i.4].

The present document was previously published as ETSI TS 102 280.

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

ITU and ISO issued standards for certification of public keys in ITU X.509 | ISO/IEC 9594-8 [i.3] which are used for the security of communications and data for a wide range of electronic applications.

Regulation (EU) No 910/2014 [i.5] of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC defines requirements on specific types of certificates named "qualified certificates". Implementation of Directive 1999/93/EC [i.1] and deployment of certificate infrastructures throughout Europe as well as in countries outside of Europe, have resulted in a variety of certificate implementations for use in public and closed environments, where some are declared as qualified certificates while others are not.

Applications need support from standardized identity certificates profiles, in particular when applications are used for electronic signatures, authentication and secure electronic exchange in open environments and international trust scenarios, but also when certificates are used in local application contexts.

This multi-part document aims to maximize the interoperability of systems issuing and using certificates both in the European context under the Regulation (EU) No 910/2014 [i.5] and in the wider international environment.