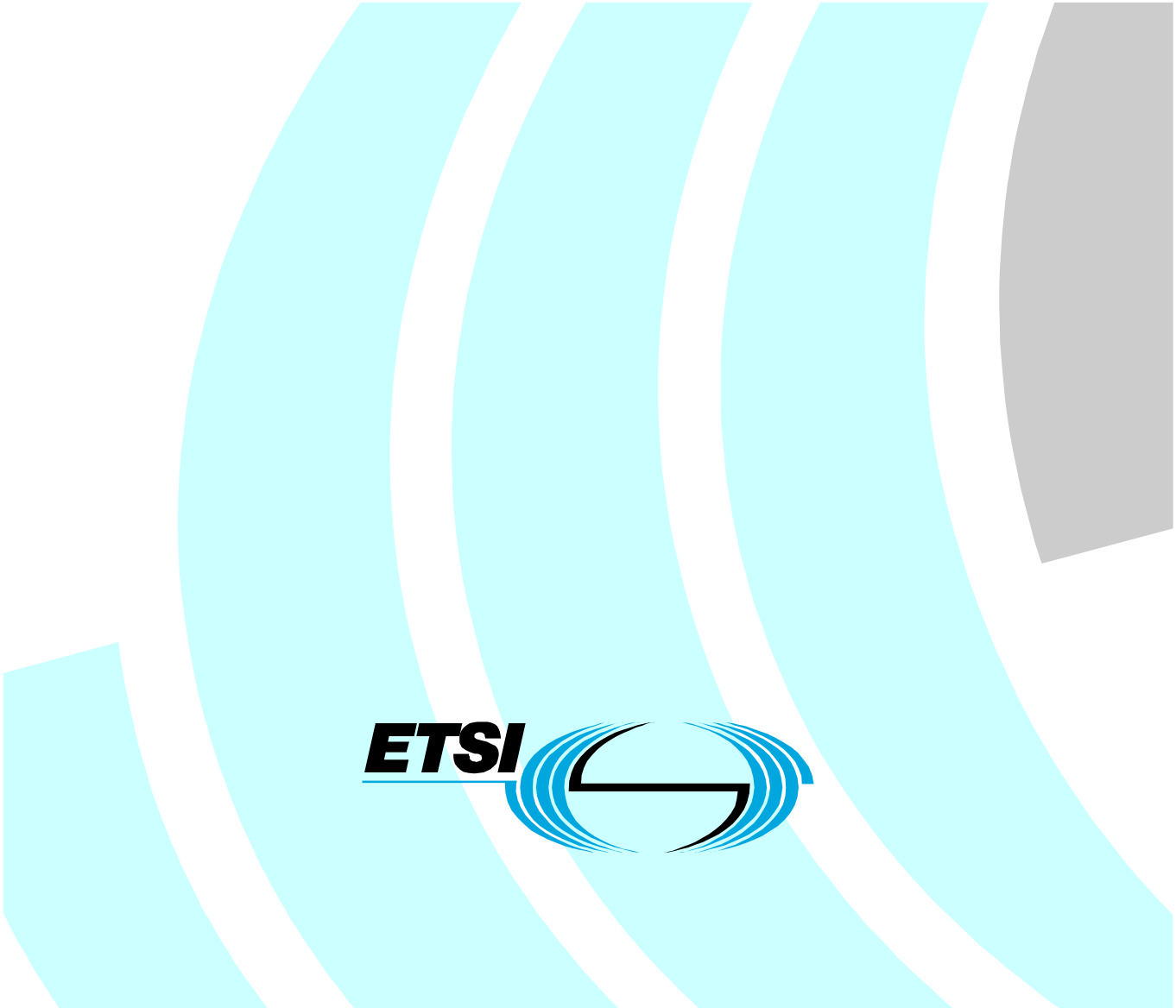
ETSI TS 101 456 V1.4.3 (2007-05)

Technical Specification

Electronic Signatures and Infrastructures (ESI);
Policy requirements for certification authorities issuing qualified certificates



Reference
RTS/ESI-000058

Keywords
e-commerce, electronic signature, security

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

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://webapp.etsi.org/IPR/home.asp).

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).

Introduction

Electronic commerce is emerging as a way of doing business and communicating across public and private networks. An important requirement of electronic commerce is the ability to identify the originator of electronic information in the same way that documents are signed using a hand-written signature. This is commonly achieved by using electronic signatures which are supported by a certification-service-provider issuing certificates, commonly called a certification authority.

For users of electronic signatures to have confidence in the authenticity of the electronic signatures they need to have confidence that the CA has properly established procedures and protective measures in order to minimize the operational and financial threats and risks associated with public key crypto systems.

The Directive 1999/93/EC of the European Parliament and of the Council on a Community framework for electronic signatures [1] (hereinafter referred to as "the Directive") identifies a special form of electronic signature which is based on a "qualified certificate". Annex I of this Directive specifies requirements for qualified certificates. Annex II of the Directive specifies requirements on certification-service-providers issuing qualified certificates (i.e. certification authorities issuing **qualified** certificates). The present document specifies baseline policy requirements on the operation and management practices of certification authorities issuing qualified certificates in accordance with the Directive. The use of a secure-signature-creation device, as required through annex III of the Directive, is an optional element of the policy requirements specified in the present document.

The present document applies also to certification authorities that include attributes in qualified certificates. Policy requirements for Attribute Authorities, i.e. for authorities that issue Attribute Certificates, are specified in TS 102 158 [14].

1 Scope

The present document specifies policy requirements relating to Certification Authorities (CAs) issuing qualified certificates (termed certification-service-providers issuing qualified certificates in the Directive [1]). It defines policy requirements on the operation and management practices of certification authorities issuing qualified certificates such that subscribers, subjects certified by the CA and relying parties may have confidence in the applicability of the certificate in support of electronic signatures.

The policy requirements are defined in terms of:

a) the specification of two closely related qualified certificate policies for qualified certificates issued to the public, one requiring the use of a secure-signature-creation device;

b) a framework for the definition of other qualified certificate policies enhancing the above policies or for qualified certificates issued to non-public user groups.

The policy requirements relating to the CA include requirements on the provision of services for registration, certificate generation, certificate dissemination, revocation management, revocation status and, if required, signature-creation device provision. Other certification-service-provider functions such as time-stamping, attribute certificates and confidentiality support are outside the scope of the present document. In addition, the present document does not address requirements for certification authority certificates, including certificate hierarchies and cross-certification. The policy requirements are limited to requirements for the certification of keys used for electronic signatures.

These policy requirements are specifically aimed at qualified certificates issued to the public, and used in support of qualified electronic signatures (i.e. electronic signatures that are legally equivalent to hand-written signatures in line with article 5.1 of the European Directive on a community framework for electronic signatures [1]). It specifically addresses the requirements for CAs issuing qualified certificates in accordance with annexes I and II of this Directive [1]. Requirements for the use of secure-signature-creation devices as specified in annex III, which is also a requirement for electronic signatures in line with article 5.1, is an optional element of the policy requirements specified in the present document.

Certificates issued under these policy requirements may be used to authenticate a person who acts on his own behalf or on behalf of the natural person, legal person or entity he represents.

These policy requirements are based around the use of public key cryptography to support electronic signatures.

The present document may be used by competent independent bodies as the basis for confirming that a CA meets the requirements for issuing qualified certificates.

It is recommended that subscribers and relying parties consult the certification practice statement of the issuing CA to obtain further details of precisely how a given certificate policy is implemented by the particular CA.

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

NOTE: See CEN Workshop Agreement 14172 "EESSI Conformity Assessment Guidance".