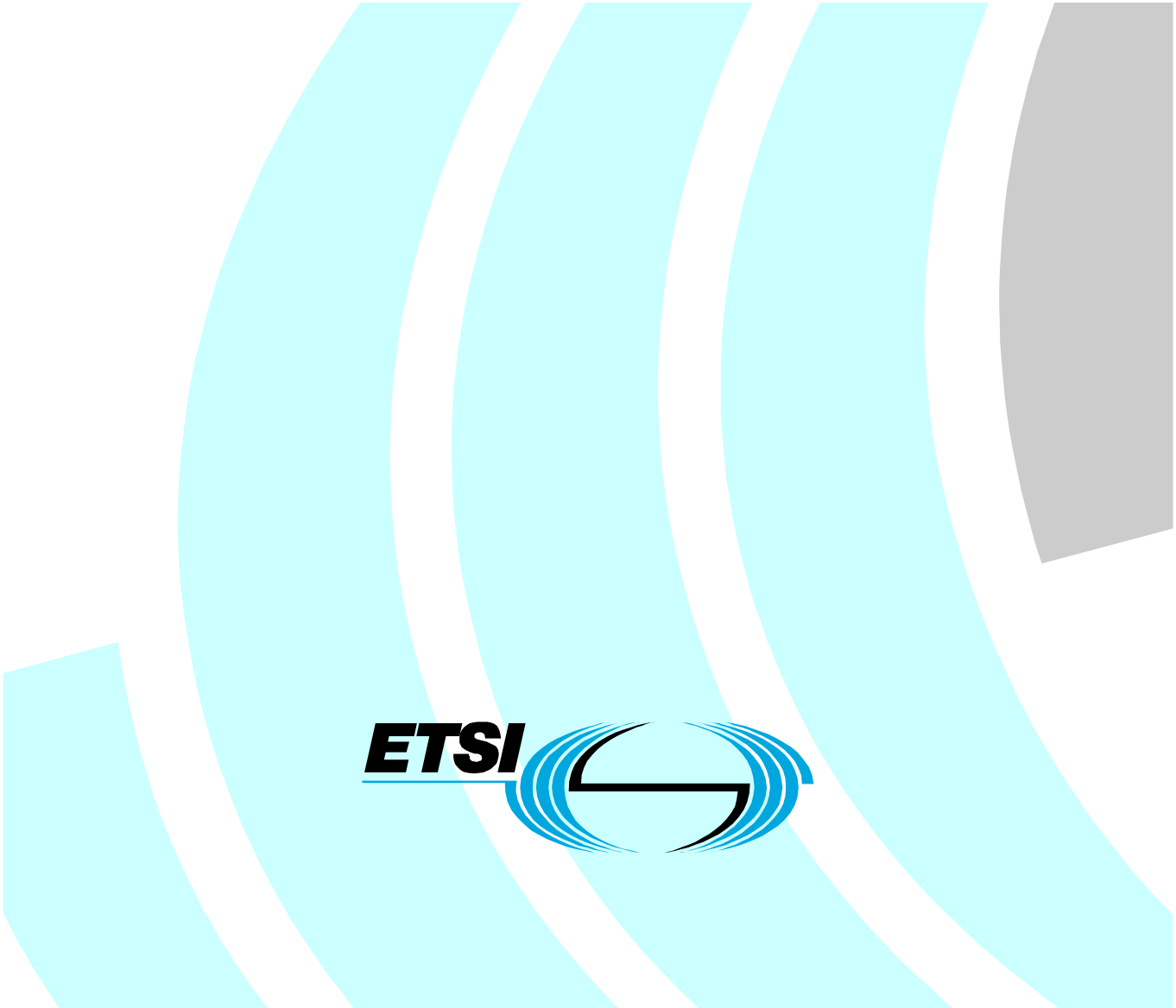
ETSI TR 102 040 V1.1.1 (2002-03)

Technical Report

International Harmonization of Policy Requirements for CAs issuing Certificates



Reference
DTR/SEC-004015

Keywords
e-commerce, electronic signature, public key,
trust services, 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 4
Foreword 4
1 Scope 5
2 References 5
3 Definitions and abbreviations 5
3.1 Definitions 5
3.2 Abbreviations 6
4 Objective 6
5 Relevant activities 6
5.1 Introduction 6
5.2 IETF PKIX policy and practices framework 6
5.3 ISO SC27 TTP guidelines 7
5.4 ABA PKI assessment guidelines 7
5.5 APEC TEL eSTG 7
5.6 ANSI X9.79 - PKI policy and practices framework 7
5.7 ISO TC68 - PKI policy and practices framework 8
6 Recommendations 8
History 9

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 Report (TR) has been produced by ETSI Technical Committee Security (SEC).

1 Scope

The present document presents the results of ongoing work to harmonize existing ETSI technical specification on policy requirements for certification authorities (TS 101 456 [1] and TS 102 042 [2]) with other internationally recognized standards and related activities.

The aim of the present document is to identify the way forward to meet the requirements of European Electronic Signature Directive 1999/93/EC [5] whilst operating within an internationally harmonized certificate policy framework to facilitate cross recognition between PKI policy environments.

2 References

For the purposes of this Technical Report (TR) the following references apply:

[1] ETSI TS 101 456: "Policy requirements for certification authorities issuing qualified certificates".

[2] ETSI TS 102 042: "Policy requirements for certification authorities issuing public key certificates".

[3] RFC 2527: "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework".

[4] ISO/IEC 14516: "Information technology - Security techniques - Guidelines on the use and management of Trusted Third Party services".

[5] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.

[6] American Bar Association: "PKI Assessment Guidelines (PAG)".

[7] ANSI X9.79: "Public Key Infrastructure (PKI) Practices and Policy Framework".

[8] ISO/TC68/SC2 N1140 - New Work Item Proposal - Public Key Infrastructure for Financial Services - Practices and Policy Framework.

NOTE: This work item has been agreed and the resulting standard has been designated the identifier ISO 21188.

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

certificate: public key of a user, together with some other information, rendered un-forgeable by encipherment with the private key of the certification authority which issued it

certificate policy: named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements

certification authority: authority trusted by one or more users to create and assign certificates

certification practice statement: statement of the practices which a certification authority employs in issuing certificates

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

ABA	American Bar Association
ANSI	American National Standards Institute
APEC	Asia-Pacific Economic Community
CA	Certification Authority
EESSI	European Electronic Signature Standardization Initiative
IETF	Internet Engineering Task Force
ISO	International Organization for Standardization
PAG	PKI Assessment Guidelines (document published by the ABA [6])
PKI	Public Key Infrastructure

4 Objective

The major objective of the present document on international certificate policy harmonization is that other internationally recognized policies are harmonized with CA policy requirements which meet the requirements of European electronic signature Directive [5] and other equivalents which are not constrained by the European legal framework.

Thus, the main aim of harmonization is:

- To ensure that European CAs, both operating within the framework of European Directive and more generally, have at least equal recognition in the wider international marketplace;
- To ensure that certification schemes accredited under the internationally recognized standards are recognized to meet the security and management requirements of the European approval (termed accreditation in European electronic signature Directive [5]) schemes/frameworks.

In order to achieve these objectives it is also important that there is a simple relationship between the structure and requirements of ETSI documents and other internationally recognized standards.

5 Relevant activities

5.1 Introduction

There are a wide range of activities relating to certificate policies and practices which have some international relevance. This clause does not aim to provide a comprehensive list of relevant activities; rather it identifies those which are most closely related to TS 101 456 [1] and TS 102 042 [2] and hence have aspects that are already aligned with these ETSI specifications.

5.2 IETF PKIX policy and practices framework

The Internet Engineering Task Force (IETF) Public Key Infrastructure X.509 [3] (PKIX) working group has published a Certificate Policies and Certification Practices Framework - RFC 2527 [3]. This provides a structure for the specification of certificate policies and certification practice statements. This framework was considered when developing TS 101 456 [1], and a mapping to RFC 2527 [3] is included in the ETSI TS. However, it was found necessary to diverge significantly from this structure to ensure that that all aspects of policy, including security management and organization, are effectively covered.

RFC 2527 [3] only provides a structure for the specification of certificate policies and certification practices. It does not include specific requirements such as covered by the ETSI TS.

RFC 2527 [3] is currently being revised by the IETF. The resulting revised structure needs to be taken into account in any future work on harmonization of policies and practices.

5.3 ISO SC27 TTP guidelines

ISO JTC1 SC 27, concerned with International Standards for security techniques, produced an international standard ISO/IEC 14516 [4]. This provides general guidance on the management of trusted third parties, and was useful background material to the development of TS 101 456 [1]. However, it does not include the specific policy requirements necessary for assessment of a certification authority.

5.4 ABA PKI assessment guidelines

The American Bar Association (ABA) Information Security Committee (ISC) has produced guidelines for the assessment of a public key infrastructure called the PKI Assessment Guidelines (PAG) [6]. The PAG provides general guidance particularly from the legal perspective. However, as a general guide the PAG does not identify specific requirements as necessary for a certificate policy.

The PAG includes little guidance relating to European legislation, in particular the European electronic signature Directive [5]. It could provide a more useful international guide if the European legislative perspective could be incorporated into the PAG, possibly as an annex.

In addition, the ABA ISC has begun work on a new publication "Model Terms for Certification Services Agreements". This ABA activity has relevance to the TS 101 456 [1] and TS 102 042 [2] clauses on requirements for dissemination of terms and conditions and the ABA should be encouraged to take into account the work of ETSI in this area.

5.5 APEC TEL eSTG

The eSecurity Task Group (eSTG) is a task group of the Business Facilitation Steering Group of the APEC Telecommunications and Information Working Group (APEC TEL) - APEC is the Asia-Pacific Economic Community. eSTG does not have a formal charter but has two basic functions:

- the security of information infrastructure and networks;
- interoperability of electronic authentication schemes within the APEC region and with other non APEC entities.

APEC does not develop agreements guidelines or even recommendations. Rather it brings information to the attention of member economies. To this end, eSTG has shown interest in the general work on electronic signature standardization in Europe (called EESSI) of which the ETSI policy requirements specifications [1] and [2] form a significant part. An inward-mission has been planned for March 2002 and it is hoped that subsequently a reciprocal visit could be hosted by EESSI. Sharing information and views on harmonizing certificate policies will be a significant aspect of this liaison.

APEC does not intend to develop a generic certificate policy or certification practice statement. Its approach has been to look at what its member economies are doing and identifying potential impediments to interoperability. Developing even a model certificate policy or certification practice statement would be difficult in the APEC context. The Asia PKI Forum and the PKI Forum are the vehicles for those types of activities rather than APEC.

5.6 ANSI X9.79 - PKI policy and practices framework

ANSI developed a framework for PKI policies and practices aimed at the financial services around the time of the development of TS 101 456 [1]. An annex to this ANSI document (ANSI X9.79, annex B) includes specific requirements for PKI policies and practices, which have similar objectives to TS 101 456 [1]. An early draft of this annex was used as the starting point of the policy requirements of TS 101 456 [1], and was fed on into TS 102 042 [2]. Unlike TS 101 456 [1], the ANSI document does not mandate particular requirements to be adopted by a CA. The CA is left to select those policy requirements which are relevant to the objectives of its own policy. TS 101 456 [1] and ANSI X9.79 annex B include much common text and a similar basic content structure.

Whilst ANSI X9.79 is aimed at the specific requirements of the financial community it has been adopted in the wider marketplace as the basis for assessing a PKI. It is a recommended reference of PKI Forum (an international group of PKI suppliers and users). In addition, ANSI X9.79 has been adopted as the basis of the AICPA/CICA (American and Canadian institutes for accountants) Web Trust Program for certification authorities. WebTrust is being promoted in both American and Europe as the basis of assessing the adequacy and effectiveness of controls employed by certification authorities.

5.7 ISO TC68 - PKI policy and practices framework

ANSI proposed a new work item to ISO TC68 (standards for the financial services sector) for a Public Key Infrastructure for Financial Services - Practices and Policy Framework [8] based on ANSI X9.79. TC68 members agreed to this work item in the latter part of 2001 but with a number of European members requesting that the work takes into account the European electronic signatures Directive [5] and TS 101 456 [1].

Work started on drafting the present document (to be WD 21188) at a meeting in December 2001. This merged requirements from ANSI X9.79 with those in TS 101 456 [1]. These requirements are defined in terms of a framework, providing options from which the appropriate requirements may be selected for the PKI services being provided by a CA. At the time of writing the present document the resulting text of the working draft had not been distributed.

6 Recommendations

In order to most effectively achieve the objectives of harmonization described in clause 4, with the limited resources available to ETSI, it is recommended that future activities on harmonization be targeted at activities that are closest to TS 101 456 [1] (and hence also TS 102 042 [2]) and are most likely to have a significant impact on the international marketplace.

The current direction being taken by ISO TC68 in the Framework for PKI Policies and Practices [8] is already closely aligned with that of ETSI. The TC68 working draft is expected to have much in common with TS 101 456 [1] and TC68 members have agreed to take the requirements of the European electronic signatures Directive [5] into account. Whilst it is aimed at the financial services sector it is very likely that the present document, like X9.79, will have an impact on other sectors. The financial sector will inevitably have a major influence on a PKI used for electronic commerce, as financial services are commonly a key player in any commercial transaction.

The TC68 Framework for PKI Policies and Practices will be a flexible framework from which specific requirements may be derived to meet particular policy objectives. Thus, by selecting the appropriate options within the TC68 framework it should be possible to derive a "qualified" certificate policy meeting the requirements of the European electronic signatures Directive [5], i.e. a policy equivalent to that defined in TS 101 456 [1].

Thus, it is suggested this TC68 work item be the prime target for any future activity of ETSI regarding international harmonization of PKI policies and practices. It should be the aim of any ETSI participation in this work item to ensure that the policy requirements of the European electronic signatures Directive [5], such as defined in TS101 456 [1], are included in the TC68 PKI framework standard.

In the longer term, once a standard has been ratified by TC68, an equivalent specification to TS 101 456 [1] can be defined for a "Qualified" Certificate Policy, meeting the requirements of the European electronic signature Directive [5], conforming to the international standard.

So that the TC68 activity does not diverge from other relevant PKI policy related standards this group should be encouraged to:

- take into account development of any future revisions to the Certificate Policy and Certification Practice Framework to replace RFC 2527 [3];
- feed their work into ISO JTC1 SC27 to become in the long term a standard which can be recognized by all sectors.

In addition, maintenance of ongoing links with the American Bar Associations Information Security Committee's work relating to PKI would facilitate harmonization of the implementation of legal aspects of PKI practices.

History

Document history		
V1.1.1	March 2002	Publication