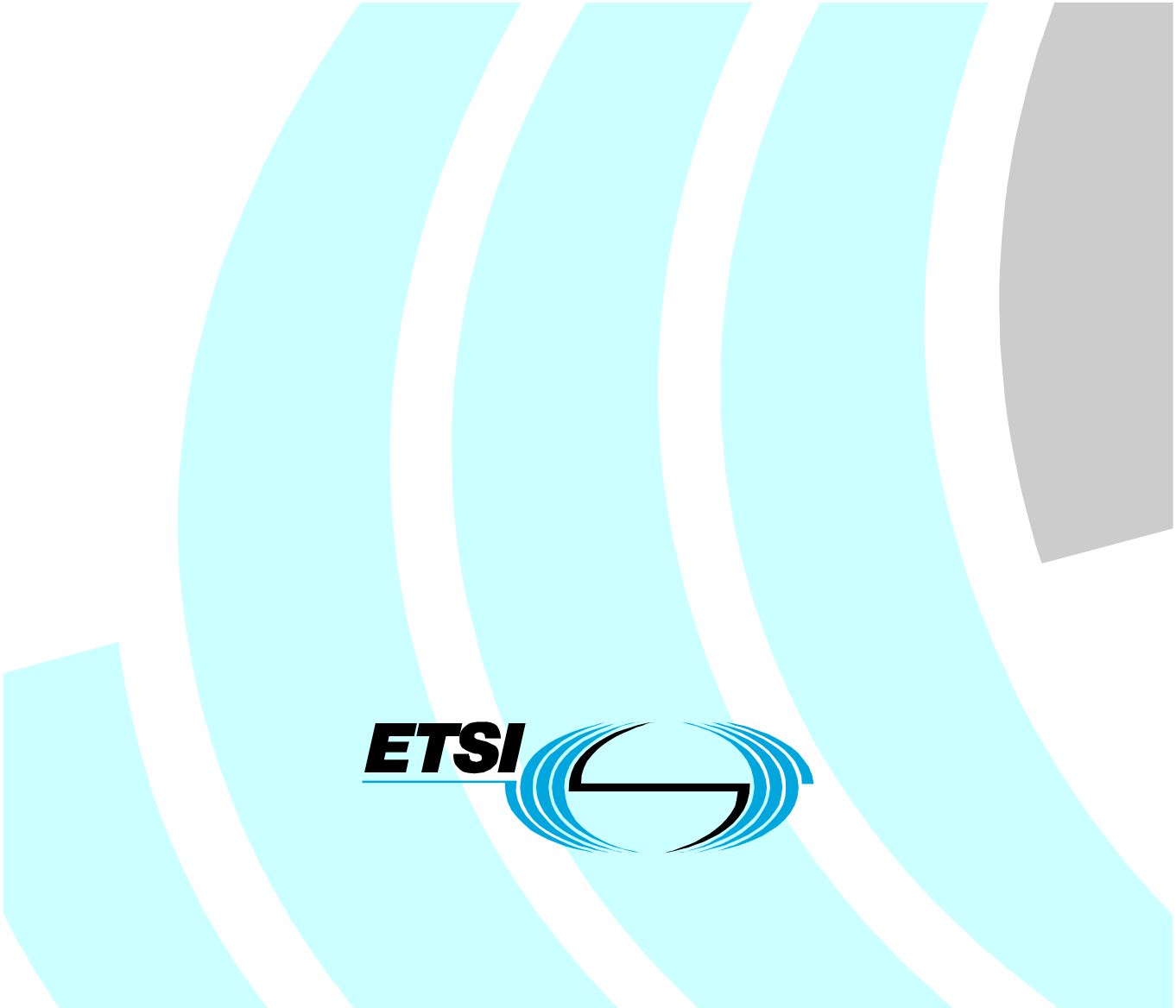
ETSI TR 102 040 V1.2.1 (2004-02)

Technical Report

International Harmonization of Policy Requirements for CAs issuing Certificates



Reference
RTR/ESI-000009

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

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 Electronic Signatures and Infrastructures (ESI).

1 Scope

The present document presents the results of ongoing work to harmonize existing ETSI Technical Specification (TS) 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] IETF RFC 2527: "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework".

NOTE: Obsoletes RFC 3647 [9].

[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 CD 21188-1: "Banking - Public Key Infrastructure Practices and Policy Framework".

[9] IETF RFC 3647: "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework".

NOTE: Obsoletes RFC 2527 [3].

[10] CEN Workshop Agreement 14172-2: "EESSI Conformity Assessment Guidance - Part 2: Certification Authority services and processes".

[11] ITU-T Recommendation X.509 (2000) | ISO/IEC 9594-8 (2001): "Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks".

[12] CEN Workshop Agreement 14167-1: "Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements".

[13] ISO 15782-1: "Certificate management for financial services -- Part 1: Public key certificates".

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

NOTE: See X.509 | 9594-8 [11].

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

NOTE: See X.509 | 9594-8 [11].

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

NOTE: See X.509 | 9594-8 [11].

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

NOTE: See RFC 3647 [9].

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
eSTG	eSecurity Task Group
FPKI	Federal Public Key Infrastructure
IETF	Internet Engineering Task Force
ISO	International Organization for Standardization
PAG	PKI Assessment Guidelines

NOTE: Document published by the ABA [6]).

PKI	Public Key Infrastructure
QCP	Qualified Certificate Policy

NOTE: Policy defined in TS 101 456.

4 Objective

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

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 systems accredited under the internationally recognized standards may also be able 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] (referred to in this document as the ETSI QCP) 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.

The ETSI QCP was developed around the concepts specified in RFC 2527 [3], and a mapping to the provisions required in RFC 2527 [3] is specified in an annex to TS 101 456 [1]. Most of the international certificate policy and accreditation schemes considered in this technical report are based around RFC 2527 [3]. Thus TS 101 456 [1] provides a useful basis for work on international harmonization.

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 QCP.

RFC 2527 [3] has been revised by the IETF as RFC 3647 [9]. Whilst the technical changes in RFC 3647 [9] are described as minimal, the recommended structure of PKI policy and practice statements have significantly changed with some sections, such as obligations, being spread across several different parts of the document.

RFC 3647 [9] is only recently released and this has yet to have a significant effect on the general direction. It is suggested that future work on the ETSI QCP take into account changes in RFC 3647 [9], possibly adding an additional annex providing cross references to the new RFC. However, RFC 2527 [3] is likely to remain important basis for cross comparison between the QCP and systems for some time to come.

5.3 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 ETSI should continue to keep ongoing contact with ABA's work on this area.

5.4 US Federal PKI

The United States federal government has established PKI infrastructure to support inter-departmental and inter-governmental security called the Federal PKI (FPKI). This is based around a Bridge CA which supports mapping between approved PKI domains. The approval is based around a "Federal Bridge CA Certificate Policy" against which other PKI domain Certificate Policies may be mapped.

The US FPKI executive and members of the ETSI ESI committee have worked together to develop a policy mapping document. This FPKI / ETSI QCP mapping document analyses elements of the two policies based upon the RFC 2527 [3] framework. This document has yet to be finalized but has gone through several iterations. A number of areas were initially identified as missing in the ETSI QCP, however many of these gaps are addressed by other ETSI and CEN specification. Particularly, there were a number of requirements relating to auditing and accreditation which covered by CEN Workshop Agreement 14167-1 [12].

As a result of this analysis a mapping from the FPKI requirements on to the ETSI QCP (with associated ETSI and CEN specifications) has been agreed. This agreement enables European CAs operating in line with the QCP (and associated specifications to be considered for bridging into the American Federal PKI. An opposite mapping between the ETSI QCP on to the FPKI, which may be used as the basis of recognition of CAs operating in the US being recognized in Europe.

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 TS 101 456 [1] and TS 102 042 [2] form a significant part.

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. A detailed analysis has been carried out between the different accreditation and certificate policy frameworks that have been developed around the ASIA-Pacific rim (including Australia, Canada, USA, Hong Kong and Singapore) as well as the ETSI Qualified Certificate Policy (QCP) based around an RFC 2527 [3] based model. The specific policies and accreditation schemes considered are listed below:

Table 1: Policy and accreditation Schemes compared by APEC

Australia	Gatekeeper (federal government)	Grade 2
Canada	Government of Canada PKI	Medium assurance
European Union	ETSI QCP - TS 101 456 [1]	Qualified certificate
Hong Kong, China	Electronic Transactions Ordinance	Certificate issued by an accredited CA
Singapore	Electronic Transactions Act	Certificate issued by an accredited CA
United States	Federal Bridge Certification Authority	Medium assurance

The work carried out under APEC provides a useful step towards identifying a direct relationship between the ETSI QCP and other accreditation systems / policy requirements. However, the APEC model lacks the details necessary to be the basis of direct cross recognition. Direct analysis may still be necessary between the ETSI QCP specific requirements for national schemes in deciding if cross recognition is possible.

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 [7], 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 [7] annex B include much common text and a similar basic content structure.

Whilst ANSI X9.79 [7] 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 [7] has been adopted as the basis of the AICPA/CICA (American and Canadian institutes for accountants) WebTrust 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 [7]. 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 progressed with the publication of a first Committee Draft (ISO CD 21188-1 [8]) in October 2002. This document was reviewed by ETSI and number of detailed comments were submitted to facilitate alignment. These comments were reviewed by a lengthy editing process with the production of a 2nd CD which is due to be published early in 2004. The ETSI comments were mostly, but not all, accepted with the four major comments addressed as described in Annex A. The resulting 2nd CD is much more clear in its concepts and terminology. In general, the document is taking the direction of being directed to an approach targeted at the financial sector, rather than being a general framework which could be adapted for use in other sectors. This document has a less broad applicability than the ANSI document (X9.79 [7]) which was used as the starting point for ISO 21188-1 [8].

CD 21188-1 [8] has still some way to go before it becomes an agreed International Standard, with a second CD ballot potentially completed in mid 2004 and potentially final publication in 2005.

It is thought likely that PKI systems could conform to both the future ISO standard and the ETSI QCP, although the ISO standard and ETSI QCP would not be directly equivalent. They are aimed at differing, albeit broadly overlapping, application requirements. CD 21188-1 [8] is aimed at a broader set of security services and security levels, but in a few cases uses a model of operation based on assumptions specific to the financial sector. However, ETSI has been successful in avoiding unnecessary divergence.

6 Recommendations

Members of ETSI technical committee on Electronic Signatures and Infrastructures have been active in working with other international activities relating the certificate policy requirements in other parts of the world, and have been successful in influencing these activities to maximize the harmonization with the ETSI QCP.

All these systems are broadly similar to the ETSI QCP. All the schemes identified in TS 101 456 [1] are based around the same concepts and principles defined in RFC 2527 [3] and in many cases the policy requirements are directly equivalent. Also, through the involvement of ETSI members it has been possible to reduce unnecessary differences. However, there are still differences in the details of the schemes considered. Each scheme has differing aims and fits in with different administrative environments thus inevitably there are differences.

In many cases, the lack of specific requirements in TS 101 456 [1] regarding auditing of conformance was considered to be an issue when comparing the ETSI QCP with other schemes. This was generally resolved by adding the CEN Workshop Agreement 14172-2 [10], or a comparable national "voluntary accreditation" scheme, to the cross comparison. Similarly, other EESSI specifications need brought in when relating the ETSI QCP to other policy requirement specifications.

When considering cross recognition between schemes either for cross certification or for acceptance under some regulatory or accreditation scheme, it will still be necessary to do detailed analysis of each element of the respective policy requirement specifications. This is the approach taken in the mapping between the American FPKI and the ETSI QCP and the two parties are close to final agreement for cross recognition.

Work has started in APEC with similar comparisons with schemes operating in the Asia Pacific region. This is a far bigger job as it involves several different forms of policy requirement specification. A model and comparison matrix is being produced by APEC but there is significant work to be done to achieve the detailed equivalence mapping produced for the Federal PKI.

It is suggested that effort on harmonization of certificate policies continues this detailed analysis to assist future cross recognition.

Annex A:
Disposition of Major ETSI comments on ISO CD 21188-1

A number of comments were submitted by ETSI on the 1st Draft ISO CD 21188-1 [8] – Banking - Public Key Infrastructure Practices and Policy Framework. This included four major comments which was addressed as follows:

1) Nationally approved algorithms should be allowed as an alternative to the TC68 standard algorithms. Specific algorithms are not required by ISO CD 21188-1 [8]. Bibliography will be cleaned up of non referenced documents by editor.

2) Text in Annex B should be worded as requirements (i.e. using "shall") but with a lead in statement (as in clause 7.3.1 etc) stating that these are controls are "to be considered for this control objective".
Annex B is now normative and "shalls" are retained. Generally the control objectives are mandatory (shall), and in many cases the controls to be used to meet the objectives are also mandatory.

3) Requirements on the financial and organizational standing of the CA should be added (as in clause 7.5 of TS 101 456 [1]).
Rejected - Capital adequacy is not an issue for standardization.

4) The use of concepts / terms needs to be made consistent throughout document.
Resolved - Accepted both internally and with alignment to ISO 15782 [13].

History

Document history		
V1.1.1	March 2002	Publication
V1.2.1	February 2004	Publication