

## **Electronic Signatures and Infrastructures (ESI); International Harmonization of Policy Requirements for CAs issuing Certificates**

---



---

Reference

RTR/ESI-000027

---

Keywords

e-commerce, electronic signature, public key,  
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**

Individual copies of the present document can be downloaded from:

<http://www.etsi.org>

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the 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 except as authorized by written permission.  
The copyright and the foregoing restriction extend to reproduction in all media.

© European Telecommunications Standards Institute 2005.  
All rights reserved.

**DECT**<sup>TM</sup>, **PLUGTESTS**<sup>TM</sup> and **UMTS**<sup>TM</sup> are Trade Marks of ETSI registered for the benefit of its Members.  
**TIPHON**<sup>TM</sup> and the **TIPHON logo** are Trade Marks currently being registered by ETSI for the benefit of its Members.  
**3GPP**<sup>TM</sup> is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners.

---

# Contents

Intellectual Property Rights .....	4
Foreword.....	4
1 Scope .....	5
2 References .....	5
3 Definitions and abbreviations.....	6
3.1 Definitions .....	6
3.2 Abbreviations .....	6
4 Objective .....	7
5 Relevant activities .....	7
5.1 Introduction .....	7
5.2 IETF PKIX policy and practices framework .....	7
5.3 ABA PKI assessment guidelines .....	7
5.4 US Federal PKI .....	8
5.5 APEC TEL eSTG .....	8
5.6 ANSI X9.79 - PKI policy and practices framework.....	9
5.7 ISO TC68 - PKI policy and practices framework .....	9
5.8 OECD.....	9
6 Recommendations .....	9
<b>Annex A: Letter from US on Mapping to US Federal PKI.....</b>	<b>11</b>
History .....	13

---

## 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 [6] 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: Obsoleted by RFC 3647 [4].
- [4] IETF RFC 3647: "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework".
- NOTE: Obsoletes RFC 2527 [3].
- [5] ISO/IEC 14516: "Information technology - Security techniques - Guidelines for the use and management of Trusted Third Party services".
- [6] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.
- [7] American Bar Association: "PKI Assessment Guidelines (PAG)".
- [8] ANSI X9.79: "Financial Services Public Key Infrastructure (PKI) Policy and Practices Framework".
- [9] ISO/DIS 21188: "Public key infrastructure for financial services - Practices and policy framework".
- [10] CEN CWA 14172-1: "EESSI Conformity Assessment Guidance Part 1 - General".
- [11] CEN CWA 14172-2: "EESSI Conformity Assessment Guidance - Part 2: Certification Authority services and processes".
- [12] ITU-T Recommendation X.509 (2000) | ISO/IEC 9594-8 (2001): "Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks".
- [13] CEN CWA 14167-1: "Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements".
- [14] 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-forgable by encipherment with the private key of the certification authority which issued it

NOTE: See ITU-T Recommendation X.509 | ISO/IEC 9594-8 [12].

**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 ITU-T Recommendation X.509 | ISO/IEC 9594-8 [12].

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

NOTE: See ITU-T Recommendation X.509 | ISO/IEC 9594-8 [12].

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

NOTE: See RFC 3647 [4].

### 3.2 Abbreviations

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

ABA	American Bar Association
AICPA	American Institute of Certified Public Accountants
ANSI	American National Standards Institute
APEC	Asia-Pacific Economic Community
CA	Certification Authority
CEN	Comité Européen de Normalisation
CICA	Canadian Institute of Chartered Accountants
EESSI	European Electronic Signature Standardization Initiative
eSTG	eSecurity Task Group
FPKI	Federal Public Key Infrastructure
IETF	Internet Engineering Task Force
ISC	Information Security Committee
ISO	International Organization for Standardization
ISSS	Information Society Standardisation System
PAG	PKI Assessment Guidelines

NOTE: Document published by the American Bar Association [7].

PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure X.509 based
QCP	Qualified Certificate Policy

NOTE: Policy defined in TS 101 456 [1].

WPISP	Working Party on Information Security and Privacy
-------	---

---

## 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 1999/93/EC [6].

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 1999/93/EC [6]) 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 the present 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 (PKIX) working group published in March 1999 a Certificate Policies and Certification Practices Framework - RFC 2527 [3]. This provides a structure for the specification of certificate policies and certification practice statements.

RFC 2527 [3] has been revised by the IETF as RFC 3647 [4]. Whilst the technical changes in RFC 3647 [4] 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 [4] was released in November 2003. This is now starting to be used instead of RFC 2527 [3] including adoption of the basis of ongoing work in the Federal PKI and APEC. The new release of the ETSI Qualified Certificate Policy TS 101 456 [1] also uses this as its main reference instead of RFC 2527 [3]. However, RFC 2527 [3] is still remains important basis for many existing PKI infrastructures.

The ETSI QCP was developed around the concepts specified in RFC 2527 [3] and RFC 3647 [4], and a mapping to the provisions required in both documents are 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] or RFC 3647 [4]. Thus TS 101 456 [1] provides a useful basis for work on international harmonization.

### 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) [7]. 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 only a small amount of guidance regarding European legislation with a small amount of information on the Electronic Signature Directive 1999/93/EC [6]. The PAG was published in 2003.

## 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 been finalized and on July 7 2004 the US General Services Administration - Office of Government-wide Policy made it official that the ETSI QCP (see annex A):

"is fundamentally comparable to the USPKI Federal Bridge Certification Authority (FBCA) Certificate Policy at the medium assurance level.

.....

The result is that Qualified certificates issued by Certification Authorities (CAs) established in European Member States, and which are compliant with the associated EESSI standards published by ETSI and Comité Européen de Normalisation (CEN), could be assured of their compatibility with the US Federal PKI should they wish to pursue cross recognition".

This comparability was achieved taking also in account other specifications issued by ETSI ESI and by the CEN Information Society Standardisation System (CEN/ISSS) WS/E-SIGN workshop, in particular CEN CWA 14167-1 [13], CEN CWA 14172-1 [10] and CEN CWA 14172-2 [11].

It is suggested that future work is performed on 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 has produced "Guidelines for Schemes to Issue Certificates Capable of Being Used in Cross Jurisdiction eCommerce". These guidelines are based around a detailed analysis of a number of certificate policies and "accreditation" schemes 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).

**Table 1: Policy and accreditation Schemes compared by APEC**

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

From this analysis, APEC identified common approaches and identified a model for accreditation of "certification service providers" including guidance on the policy requirements based around the RFC 3647 [4] framework. The current APEC model, now near to be finalized, includes nearly all of the numerous amendments ETSI has proposed. Although this is a great step towards cross recognition between the ETSI QCP specific requirements for national schemes and the APEC TEL eSTG Model, direct analysis may still be necessary.



## 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 [8], 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 [8] annex B include much common text and a similar basic content structure.

Whilst ANSI X9.79 [8] 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. ANSI X9.79 [8] 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 [9] based on ANSI X9.79 [8]. 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 1999/93/EC [6] and TS 101 456 [1].

Work progressed with the publication of a first Committee Draft (ISO CD 21188-1) in October 2002. The ISO document [9] 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 was eventually agreed for progression to DIS towards the end of 2004. The document is likely to progress to an ISO standard towards the end of 2005.

In general, the ISO document [9] 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. The ISO document [9] has a less broad applicability than the ANSI document (ANSI X9.79 [8]) which was used as the starting point for ISO CD 21188-1 [9]. 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. ISO CD 21188-1 [9] will be 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.

## 5.8 OECD

The OECD Working Party on Information Security and Privacy (WPISP) is looking at issues of authentication around cross border electronic transactions. As part of this work ETSI provided a note on the need for harmonized approval criteria for Trust Service Providers, as yet it is not clear whether there will be any activity in that area.

---

# 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 its replacement RFC 3647 [4]) 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.

Since publication of RFC 3647 [4] a number of organizations, whose previous documents were based on RFC 2527 [3], have decided, or have expressed their intention, to adopt RFC 3647 [4]. Since this later RFC is structured somehow differently from RFC 2527 [3], is it acknowledged that mapping the current QCP to any RFC 3647 [4] based document would be rather complex. Furthermore, RFC 3647 [4] introduces additional security requirements that should be addressed in QCP. It is therefore suggested that future work is performed on the ETSI QCP to better mirror RFC 3647 [4].

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 CWA 14172-2 [11], 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 to achieve the result referred to in clause 5.4.

APEC are now nearing completion with its "Guidelines for Schemes to Issue Certificates Capable of Being Used in Cross Jurisdiction eCommerce". This provides a unified set of requirements for PKI assessment schemes around the Pacific rim to which TS 101 456 [1] may be related. Whether this will have a direct impact on the market is yet to be seen.

It is suggested that effort on harmonization of certificate policies continues this detailed analysis to assist future cross recognition particularly with the completion of the inverse of the current mapping between TS 101 456 [1] and the US Federal PKI.

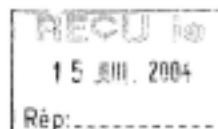
## Annex A: Letter from US on Mapping to US Federal PKI



GSA Office of Governmentwide Policy

JUL -7 2004

Mr. Karl Heinz Rosenbrock  
ETSI Director General  
650 Route des Lucioles  
F-06921 Sophia Antipolis Cedex  
FRANCE



Dear Mr. Rosenbrock:

I am pleased to inform you that a meeting in London between representatives from the European Telecommunications Standards Institute (ETSI) Electronic Signatures and Infrastructures Technical Committee (TC ESI), working as part of the European Electronic Signature Standard Initiative (EESSI), and the United States Federal Public Key Infrastructure Committee (USFPKI) has resulted in the agreement on the part of the U.S. Federal Government that the European Telecommunications Standards Institute (ETSI) Technical Specification (TS) 101 456, *Policy requirements for certification authorities issuing qualified certificates (Qualified Certificate Policy)*, is fundamentally comparable to the USFPKI Federal Bridge Certification Authority (FBCA) Certificate Policy at the medium assurance level. The resulting comparison matrix is enclosed for your information.

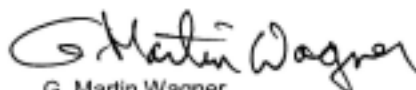
This agreement represents the culmination of a two-year collaboration between ETSI and USFPKI to harmonize their Public Key Infrastructure (PKI) policy requirements. The result is that Qualified Certificates issued by Certification Authorities (CAs) established in European Union Member States, and which are compliant with the associated EESSI standards published by ETSI and Comite Europeen de Normalisation (CEN), could be assured of their compatibility with the U.S. Federal PKI should they wish to pursue cross recognition. By the same token, the fact that a European CA may be issuing certificates which are *not* compliant with the Qualified Certificate Policy would not preclude the pursuit of cross recognition; however it would require more effort on both sides.

U.S. General Services Administration  
1890 F Street, NW  
Washington, DC 20405-0002  
www.gsa.gov

- 2 -

The successful conclusion of this project is an important first step in building trust and recognition across national boundaries for electronic authentication solutions. We in the United States look forward to future opportunities to build on the successes already achieved. If you would like to further discuss the contents of this letter or if you have any additional questions or concerns, please do not hesitate to contact me. Staff inquiries may be directed to Ms. Judith Spencer, Chair, Federal PKI Steering Committee, on (202) 208-6576.

Sincerely,



G. Martin Wagner  
Associate Administrator

Enclosure

cc: Dr. György Endersz  
Chairman of ETSI TC ESI  
TeliaSonera Sverige AB  
S-123 86 Farsta  
SWEDEN

---

## History

<b>Document history</b>		
V1.1.1	March 2002	Publication
V1.2.1	February 2004	Publication
V1.3.1	March 2005	Publication