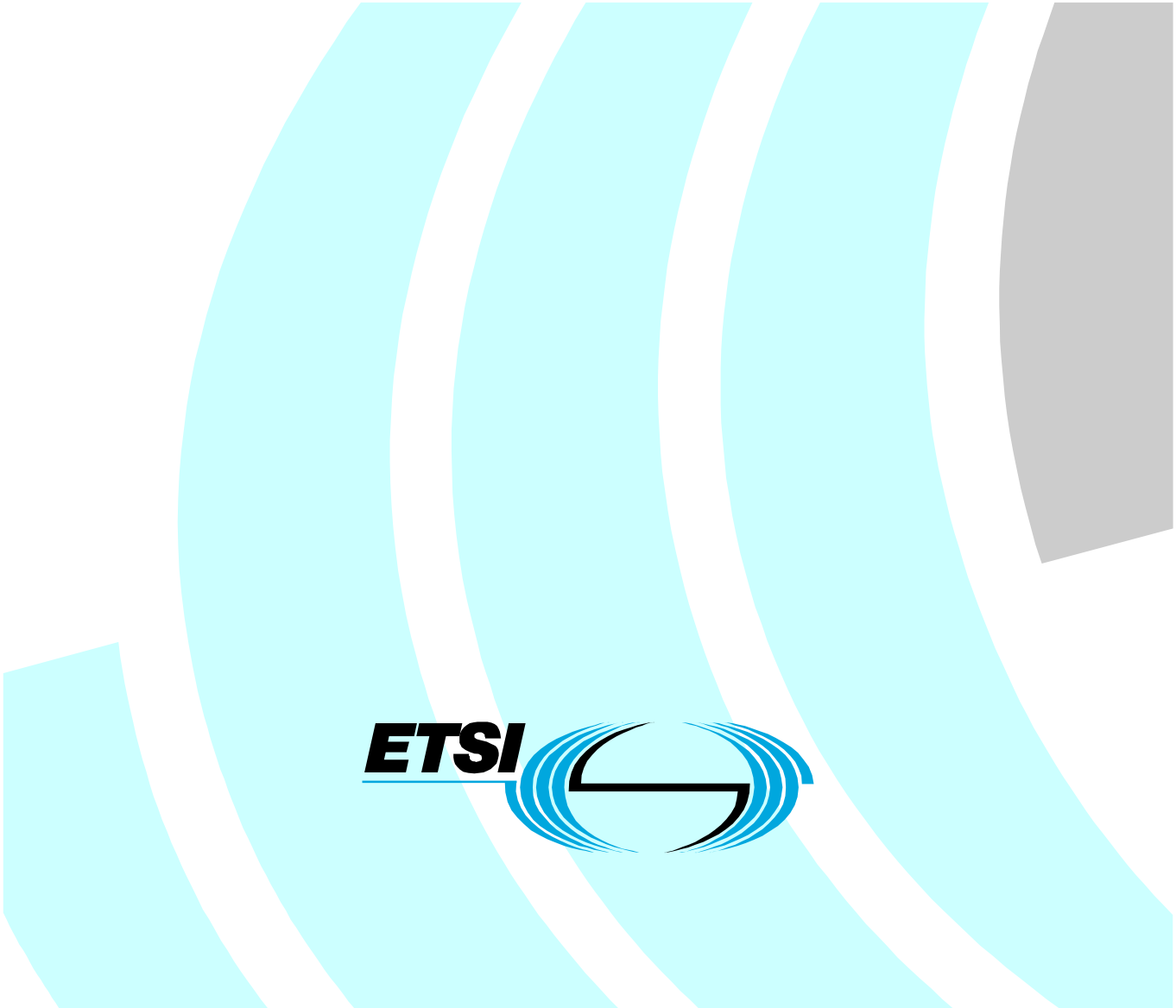
ETSI TR 102 153 V1.1.1 (2003-02)

Technical Report

Electronic Signatures and Infrastructures (ESI); Pre-study on certificate profiles



Reference
DTR/ESI-000015

Keywords
authentication, 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).

All published ETSI deliverables shall include information which directs the reader to the above source of information.

Foreword

This Technical Report (TR) has been produced by ETSI Technical Committee Electronic Signatures and Infrastructures (ESI).

ETSI TC ESI has remarked that existing certificate profiles, among them TS 101 862 [6], are considered too open, allowing too many choices, which lead to incompatible implementations. It has then agreed to launch a pre-study to assess the preconditions for an action to further profile the certificate formats.

The purpose of this study is to cover, but not be limited to, qualified certificates.

The main finding of this study is that more rigid profiles are deemed necessary to actually achieve interoperability and, therefore, "to ensure the free movement within the internal market and to build trust in electronic signature" (see Directive 1999/93/EC recital (5) [1]).

Therefore the next step should be to issue a Technical Standard specify the full format of a Qualified Certificate both from an issuer point of view and from a verifier point of view. Formats for "citizen" certificates (Electronic Identity Certificates (EIC)) could also be indicated.

1 Scope

The study was intended to include:

- Investigation on the major sources of incompatibility.
- Review of existing certificate configurations in the public domain, i.e. for open user communities.
- Review of proposed profiles.
- Conclusion whether a normative task is feasible and meaningful.

Since the conclusion reached is that a normative task is required, the study also covers the rest of what the ToR required:

- Proposed strategy for harmonization with existing standards in the area, notably with the IETF and ETSI QC-profiles.
- Proposal for the way of publishing, e.g. annex to existing standard or stand-alone document.
- ToR of the task to be carried out, including estimated effort and time.

The following two certificate types have been covered:

1) certificates to be used in a qualified signature;
2) authentication certificates.

It is to be noted that the purpose of the study was mainly to investigate if there actually are risks of major incompatibilities among existing profiles. In other words, the survey was not intended to take into exam all existing profiles, which would have been too broad an effort for the limited resources available. The goal was instead to collect, if applicable, sufficient evidence of such risks. When it has been achieved, no additional certificate profiles have been taken into exam.

For this reason a few certificate profiles have been left out; for example: the Italian Electronic Identity Document (EID) certificate profile and the corresponding experimental French one. This simply means that the purpose had been achieved before their turn to be taken in exam had arrived.

2 References

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

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

[2] IETF RFC 3279: "Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", W. Polk, R. Housley, L. Bassham. April 2002.

[3] IETF RFC 3280: "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile". R.Housley, W. Ford, W. Polk, D. Solo. April 2002.

[4] IETF RFC 3039: "Internet X.509 Public Key Infrastructure - Qualified Certificates Profile". S. Santesson, W. Polk, P. Barzin, M. Nystrom. January 2001.

[5] ISO/IEC 9594-8: "Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks" - Fourth Edition 2001-08-01.

[6] ETSI TS 101 862: "Qualified certificate profile".

[7] IETF RFC 2459: "Internet X.509 Public Key Infrastructure Certificate and CRL Profile".

3 Definitions and abbreviations

3.1 Definitions

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

authentication certificate: Public Key Certificate (PKC) intended to be used in an electronic signature which serves as a method of authentication, as specified in Directive [1], article 2.1.

Certification Authority: authority trusted by one or more users to create and assign public key certificates

Public Key Certificate (PKC): data structure containing the public key of an end-entity and some other information, which is digitally signed with the private key of the CA which issued it

Qualified Certificate: Public Key Certificate (PKC) that conforms to Directive [1], annex I and that is issued by a Certification Authority that conforms to the requirements of Annex II of the same Directive.

3.2 Abbreviations

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

CA	Certification Authority
CRL	Certificate Revocation List
CSP	Certificate Service Provider
EESSI	European Electronic Signature Standardization Initiative
EIC	Electronic Identity Certificates
EID	Electronic Identity Document
IETF	Internet Engineering Task Force
ISO	International Organization for Standardization
PKC	Public Key Certificate
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure X.509 based
QC	Qualified Certificate
ToR	Terms of Reference

4 Implications from the requirements of the Directive

Directive [1] whereas (5) provides a clear hint to interoperability: "***The interoperability of electronic-signature products should be promoted***; *in accordance with Article 14 of the Treaty, the internal market comprises an area without internal frontiers in which the free movement of goods is ensured;* ***essential requirements specific to electronic-signature products must be met in order to ensure free movement within the internal market and to build trust in electronic signatures,***…".

Directive [1] whereas (7) stresses the need to promote international communications: "*The internal market ensures the free movement of persons, as a result of which* ***citizens and residents of the European Union increasingly need to deal with authorities in Member States other than the one in which they reside; the availability of electronic communication could be of great service in this respect***".

Similarly whereas (10) states: "*The internal market enables certification-service providers to develop their cross-border activities with a view to increasing their competitiveness, and thus to* ***offer consumers and businesses new opportunities to exchange information and trade electronically in a secure way, regardless of frontiers.***

From the above quotations a strong need stems for interoperability that has as a first pillar the certificate profile. Other main pillars are: signature formats, certificate status information format, Certificate Service Provider (CSP) status information format, time stamping format.

From the Directive [1], article 5 both subsections, both qualified certificates and non qualified certificates appear to be subject to interoperability issues and therefore both deserve an interoperability focussed study. Actually it is impossible to profile every non qualified certificate type. Furthermore such an effort would be somewhat questionable.

To focus on a feasible and useful purpose, thus endeavouring in an effort both effective and efficient, this study addressed only two meaningful certificate types:

1) certificate to be used in qualified signatures;

2) authentication certificates (for both purposes: "peer entity authentication" and "data origin authentication").

5 Documents scrutinized

The following profiles and documents have been analysed by the task components.

Document name	Organization	Country
A-Trust - Certificate and CRL Specification	A-Trust Gesellschaft für Sicherheitssysteme im elektronischen Zahlungsverkehr GmbH.	Austria
FINEID S4-1 - Implementation profile 1 of the FINEID - S1 specification.	Population Register Centre	Finland
FINEID S4-2 - Implementation profile 2 (for organizational usage) of the FINEID S1 specification.	Population Register Centre	Finland
Common ISIS-MTT specification for PKI applications from T7 & teletrust - Part 1 - Certificate and crl profiles - Version 1.0.1, November 15th 2001	TeleTrusT and T7	Germany
Identification Cards - Electronic ID Certificate	SIS - Standardiseringen i Sverige	Sweden
SmartTrust Certificate Formats	SmartTrust	Sweden
Circolare AIPA/CR/24	Autorità per l'Informatica nella Pubblica Amministrazione	Italy

6 Analysis outcomes

6.1 Profile comparison

The following table gives a synoptic view of the main characteristics (i.e.: extensions and fields) of the examined profiles. Given the limited study purpose the profile examination has not been done in depth: the task members' goal was to ascertain if the existent certificates assure a satisfactory interoperability or, instead, if new profiles are to be agreed upon. So, when it became apparent a new certificate set is to be devised, it was no more necessary to extend the documents examination.

	ISIS-MTT	A-Trust	Svensk Standard	SmartTrust	FINEID	Europe SmartCard	Italian pre-Directive profile (see note 1)
Basic certificate fields							
CertificateSerialnumber	max. 20 octets ($< 2^{159}$)	max. 16 bytes	max. 8 bytes (64 bits)	max. 16 bytes	max. 8 bytes	max. 8 bytes	As per RFC 2459 [7] (Max 20 octets)
Signature AlgorithmIdentifier	sha1WithRSA Encryption is preferred RIPEMD-160 with RSA support recommended	Sha1WithRSA Encryption	md5WithRSA Encryption sha1WithRSA Encryption	sha1WithRSAEncryption	sha1WithRSAEncryption	sha1WithRSAEncryption	sha1WithRSAEncryption OR RIPEMD-160 with RSA
Issuer	MUST: countryName, organizationName SHOULD contain: organizationalUnit Name	countryName, organizationName, commonName, organizationalUnit Name	countryName, organizationName, commonName	countryName, organizationName, commonName	countryName, organizationName, commonName	countryName, organizationName, commonName	DN as per RFC 2459 [7]
Subject	MUST: commonName, countryName	countryName, title, surname, givenName, commonName, serialNumber	countryName, surname, givenName, serialNumber	countryName, surname, givenName, commonName, serialNumber	countryName, surname, givenName, commonName, serialNumber	countryName, surname, givenName, serialNumber	DN up to CN (see note 2)
Standard certificate extensions							
AuthorityKeyIdentifier	MUST: authorityCertIssuer, authorityCertSerialNumber SHOULD contain: keyIdentifier	keyIdentifier non-critical	keyIdentifier	keyIdentifier non-critical	keyIdentifier non-critical	keyIdentifier	At least KeyIdentifier Non-critical
SubjectKeyIdentifier	The keyIdentifier is composed of the 160-bit SHA-1 hash of the value of the BIT STRING subjectPublicKey (excluding the tag, length, and number of unused bits)	The keyIdentifier is composed of a four bit type field with the value 0100 followed by the least significant 60 bits of the SHA-1 hash of the value of the BIT STRING subjectPublicKey non-critical	The keyIdentifier is composed of a four bit type field with the value 0100 followed by the least significant 60 bits of the SHA-1 hash of the value of the BIT STRING subjectPublicKey	The keyIdentifier is composed of a four bit type field with the value 0100 followed by the least significant 60 bits of the SHA-1 hash of the value of the BIT STRING subjectPublicKey non-critical	The keyIdentifier is composed of a four bit type field with the value 0100 followed by the least significant 60 bits of the SHA-1 hash of the value of the BIT STRING subjectPublicKey non-critical	The keyIdentifier is composed of a four bit type field with the value 0100 followed by the least significant 60 bits of the SHA-1 hash of the value of the BIT STRING subjectPublicKey	At least keyIdentifier As per RFC 2459 [7] (both coding formats are accepted) Non-critical

	ISIS-MTT	A-Trust	Svensk Standard	SmartTrust	FINEID	Europe SmartCard	Italian pre-Directive profile (see note 1)
KeyUsage (signature key certificate)	NonRepudiation	Non Repudiation signature: nonRepudiation, Authentication: digitalSignature Encryption certificate: DigitalSignature, keyEncipherment, dataEncipherment Critical	Alternatively: nonRepudiation OR digitalSignature, depending on the purpose. Additionally keyEncipherment, dataEncipherment may be used: it is not specified how the bits might be combined Critical	nonRepudiation critical	nonRepudiation Alternatively: DigitalSignature, keyEncipherment, dataEncipherment Critical	At least two certificates are required: 1) nonRepudiation 2) authentication + encipherment Three key pairs (nonRepudiation, authentication, encipherment) are accepted Critical	nonRepudiation Critical
SubjectAltName	Optional	optional non-critical		optional non-critical			
BasicConstraints (end user certificate)	SHOULD NOT appear in end entity certificates. non-critical, critical	cA is set to false non-critical		cA is set to false non-critical			MUST NOT appear in end entity certificates
CertificatePolicies	non-critical	mandatory: policyIdentifier optional: policyQualifiers non-critical	mandatory: policyIdentifier optional: policyQualifiers	mandatory: policyIdentifier optional: policyQualifiers non-critical	mandatory: policyIdentifier optional: policyQualifiers non-critical	both mandatory policyIdentifier policyQualifiers non-critical	Mandatory: policyIdentifier+ CPS URL Non-critical
CRLDistributionPoints	non-critical	distributionPoint non-critical		distributionPoint non-critical	distributionPoint non-critical	distributionPoint non-critical	Mandatory: CRL access URL Non-critical
ExtKeyUsage	critical or non-critical	signature key certificate: emailProtection non-critical (see note 4)	SHALL NOT be used				SHOULD NOT appear in end entity certificates
SubjectDirectoryAttributes	SHOULD NOT	optional non-critical	SHALL NOT be used		forbidden		
Private extensions							
QcStatements	Optional non-critical	Optional critical		optional	optional	qcCompliance mandatory non-critical	N.A. (see note 3)
AuthorityInfoAccess	if OCSP service is offered, its URL MUST be contained in this extension	non-critical		non-critical			N.A. (see note 3)

	ISIS-MTT	A-Trust	Svensk Standard	SmartTrust	FINEID	Europe SmartCard	Italian pre-Directive profile (see note 1)
Cardnumber			optional	optional			N.A. (see note 3)
BiometricData	Optional			optional			N.A. (see note 3)

NOTE 1: Italian provisions currently in force do not specify each and every certificate component, stating that non specified components must abide by RFC 2459 (now subsided by RFC 3280 [3]). Similarly, an authentication certificate profile is being worked out by Assocertificatori (the association among currently accredited CAs), whose main difference from the nonRepudiation certificate is that the only keyUsage it provides for is digitalSignature and that extKeyUsage may be "TLS WWW Client Autentication" (Object ID 1.3.6.1.5.5.7.3.2). Other values may be accepted, provided they do not collide with requirements as per 1.3.6.1.5.5.7.3.2. NON Critical

NOTE 2: It is required that a subject's unique code is included in the certificate. This is achieved by inserting in commonName the Fiscal Code, assigned by the Minister of Finance, which is biunique to the subject.

NOTE 3: These extensions are not present in the Italian requirements, since they have been set before RFC 3039 [4] and TS 101 862 [6].

NOTE 4: Extended keyusage emailProtection is going to be removed from the A-Trust signature key certificate.

6.2 Profiles inconsistencies

A few inconsistencies stem out of the previous table.

Their severity has been classified as follows:

Severity 1. The inconsistency gives way to outright incompatibility since what is permitted or mandatory for one or more profile is unacceptable for other ones.

Severity 2. The inconsistency requires the signature verification application to accept and handle a very wide range of possible options, thus becoming clumsily awkward.

Severity 3. The inconsistency is a minor one, easily handled without much effort on the signature verification application.

6.2.1 Inconsistencies list

#	Inconsistency	Severity	Comment
1	CertificateSerialNumer field length	S3	The acceptable field length spans between 8 bytes and 20 bytes. It can be easily handled by suitable application programs, but a uniform length it would be preferable.
2	Allowed Signature Algorithms	S1	All provide for SHA1 with RSA encryption, but two of them accept also RIPEMD-160 and one accepts MD5. RIPEMD-160 has a very limited utilization (RFC 3279 [2] does not even mention it). As early as in 1995 MD5 was found no more reliable for future applications, so RFC 3279 [2] states: "The use of MD5 for new applications is discouraged. It is still reasonable to use MD5 to verify existing signatures." It is therefore proposed to discourage use of RIPEMD-160, for interoperability sake, and to outright avoid MD5, for security reasons.
3	Issuer	S2	Many, but not all, profiles require the commonName field, which falls within the attributes RFC 3039 [4] states about: "Additional attributes MAY be present but they SHOULD NOT be necessary to identify the issuing organization". Either RFC 3039 [4] is modified in order to include commonName among the main attributes, or there is a risk of incompatibility.
4	Subject	S1	In this case there is a wide range of choices: commonName yes/no, serialNumber yes/no, etc. This looks like a sure recipe for non interoperability.
5	KeyIdentifier (both Subject and Authority)	S2	While 5 profiles adopt one of the two possible methods of calculating the identifier, one outright adopts the other one, and the 7th, solomonically, has no preference. It is highly preferable to have a single method.
6	Basic Constraints	S3	There is no apparent reason to specify basicConstraints with cA false, since it is the default value. Skipping it, is easier to handle and more compact.

#	Inconsistency	Severity	Comment
7	KeyUsage	S1	In three profiles only the nonRepudiation certificate is covered. In the remaining profiles different directions seem coexist: 1) two certificates: authentication (digitalSignature only) encryption, where two configurations are possible: a) only keyEncryption and dataEncryption b) keyEncryption and dataEncryption plus digitalSignature 2) one certificate, both for authentication and encryption It is, in any case, worth noting that, should the authentication be intended as SSL/TLS client authentication, the extendedKeyUsage "TLS WWW client authentication" should be used. RFC 3280 [3] specifies, about it: "Key usage bits that may be consistent [with TLS WWW client authentication]: digitalSignature and/or keyAgreement". In other words: no encryption. On the other hand, as the dual usage (i.e.: encryption and digitalSignature) certificate should in any case abide by the common practice not to backup the digitalSignature key, there could be a problem, since it is also the *d*ecryption key. Conclusion: additional investigation is to be performed to verify if possible incompatibilities lurk around. Should incompatibilities depend on improper combined use of nonRepudiation and digitalSignature, it would be a very serious problem, hence the Severity level 1assigned to this topic.
8	SubjectDirectoryAttributes	S1	In two certificate profiles it is forbidden and another one recommends against. RFC 3039 [4] explicitly refers to subjectDirectoryAttribute to store information such as title; dateOfBirth; placeOfBirth; gender; countryOfCitizenship; and countryOfResidence. This information most likely will be necessary to better specify the certificate user's information. Also in this case additional investigation is to be performed.
9	Private extensions	S3	These extensions are still in their infancy, so no definite assessment is reasonable to be done. Additional investigation is therefore recommended.

6.2.2 Comments on the findings

Major concerns arise from the previous table:

1) non full interoperability among certificates;

2) questionable choices, mostly in the authentication certificate profile.

Both concerns may lead to major problems in exchanging signed electronic documents across frontiers and in mutually recognizing Member States electronic identification documents.

It is therefore highly recommended that a thorough investigation is implemented across European Member States to overcome the previous problems.

7 Proposed strategy and implementation phases

It has already been pointed out that an actual interoperability is indispensable to achieve the Directive purposes, as specified in clause 4.

It is a common belief of those who took part in the study that a task force is to be charged of working out certificate profiles that meet the following requirements:

1) achieve acceptance and consensus throughout Europe;

2) leave open only options that do not give way to interoperability issues with a higher than level 3 Severity;

3) meet the recognized specifications, namely ISO/IEC 9594-8 (2001) [5], RFC 3039 [4], RFC 3279 [2], RFC 3280 [3], TS 101 862 [6] or their follow on;

4) achieve consensus on formats compliant with generally deemed "best practice" specifications.

These requirements imply the following implementation specifications:

a) Since profiles are to be developed so that all Member States will de facto implement them in their regulations, team members must have suitable political clout and standing as well as diplomatic skill and undisputed technical knowledge. If necessary, EESSI SG may be involved as well by providing its support.

b) At first sight, interoperability issues appear not to stem out of RFC 3280 [3], RFC 3039 [4], TS 101 862 [6] themselves; rather, from misunderstanding of their provisions or from having certificates been issued before them. A more thorough investigation is therefore required to ascertain, jointly with the national bodies responsible for each certificate profile, the rationale of their choices alongside the mentioned specifications.

   Should the outcomes demonstrate the latter are to be amended, such amendments must achieve consensus among at least the majority of the involved bodies, prior to be proposed to the IETF PKIX as well.

   However, completely new profiles, complying with the requirements agreed upon with the bodies, will have to be defined and will need achieve TC ESI consensus before being submitted to the involved bodies for their approval.

   It will also be necessary to work out with each and all involved bodies a harmonized phase-in/phase-out plan of current and new/revised profiles.

   All Member States relevant bodies will be made aware of such each other's profiles and relevant phasing in and out plan.

   The outcome of the above effort will be a new ETSI Technical Specification.

Annex A:
Participation to the task

Although it is the ETSI habit not to mention the components of a task that drafted one document, given this task peculiarity of voluntary participation and, moreover, in order to give a better understanding of the profiles assessment relevance, name, country and organization of those who enlisted as volunteers are hereafter specified.

Surname	Name	Country	Organization
BIELY	Helmut	Austria	BDC-EDV Consulting
CACCIA	Andrea	Italy	Innovery
ENDERSZ	György	Sweden	Telia
ESPOSITO	Alfredo	Italy	Infocamere
HILL	Jane	UK	Chambers of Benet Hytner Q.C.
MANCA	Giovanni	Italy	Autorità per l'Informatica nella Pubblica Amministrazione
NILSSON	Hans	Sweden	Hans Nilsson Consulting
RUGGIERI	Franco	Italy	FIR DIG Consultants
SAARIPUU	Tuire	Finland	Population Register Centre
SIMONATO	Carolina	Italy	Infocamere
TOVO	Gianluca	Italy	Saritel

History

Document history		
V1.1.1	February 2003	Publication