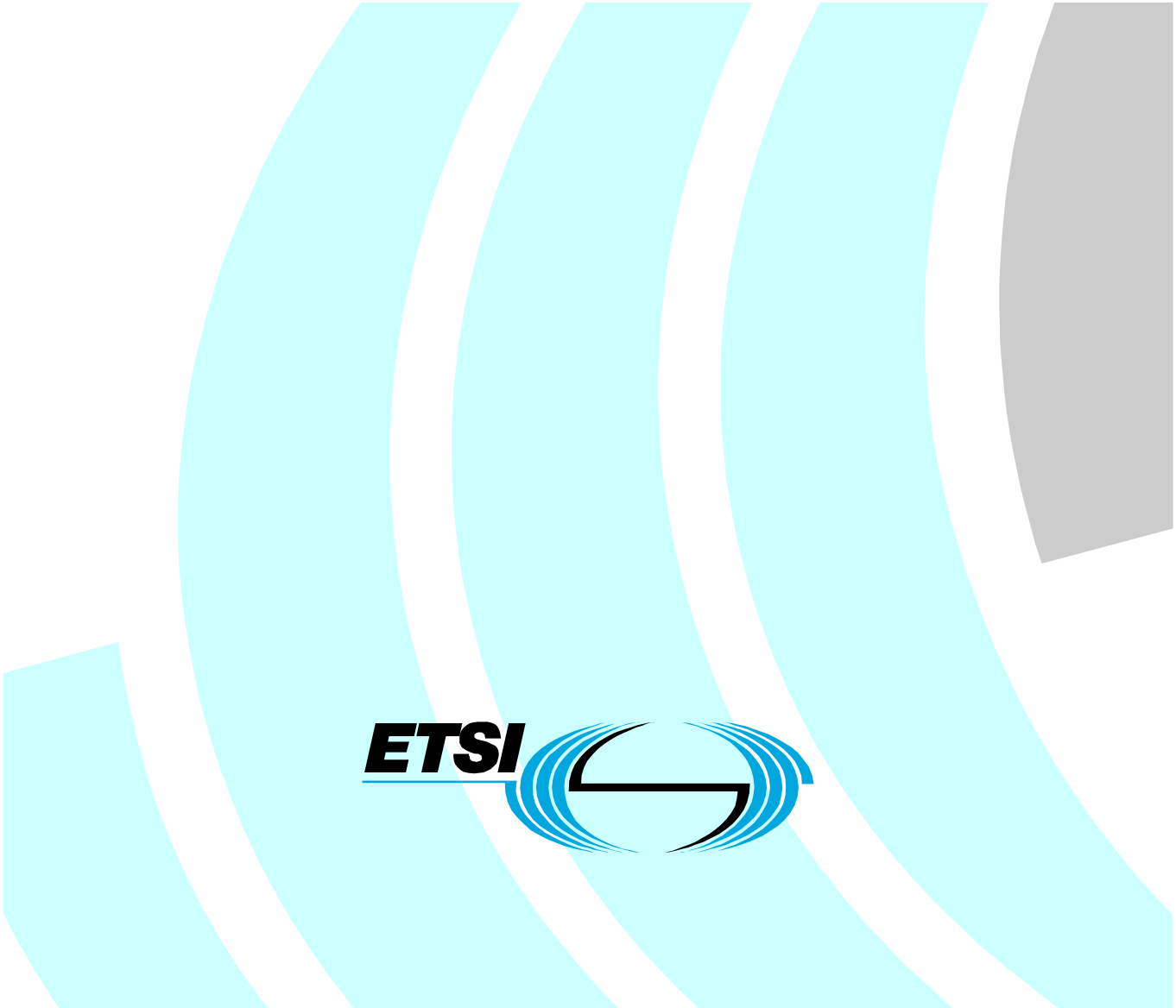
ETSI TR 102 044 V1.1.1 (2002-12)

Technical Report

Electronic Signatures and Infrastructures (ESI); Requirements for role and attribute certificates



Reference
DTR/ESI-000005

Keywords
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).

The objective of the present document is to identify a set of requirements that will provide a basis on which a subsequent standard can build policy requirements for attributes certified by Attribute Authorities or Certification Authorities either in a subject's PKCs (Public Key Certificates) or in ACs (Attribute Certificates).

By attribute it is intended a person's qualification that entitles him/her to exert specific functions, e.g. CEO from company AAA, doctor in medicine from country BBB, barrister from country CCC, sales director from company DDD, etc. or obtain some privileges, e.g. member from Golf Club EEE, etc.

A survey has been made on potential usages of attributes and the outcome has been that very little attribute usage currently exists, so very little (if any) experience can be draw from the real world. Therefore the present document is based both on the few information received and the best assumptions that could be done on that topic.

When no distinction is wished to be made between an Attribute Authority and a Certification Authority, the generic term Attribute Certification Authority (ACA) is being used.

The findings of the present document are intended mainly for the support of electronic signatures, but nothing prevents them from being used for other reasons, e.g. for authorization.

1 Scope

The present document identifies a set of requirements that will provide a basis for a subsequent standard, which will then build policy requirements for attributes certified by Attribute Authorities or Certification Authorities complying with [4] and related standards.

In some electronic signature applications, roles and attributes can be exerted only if a claimer's right to use them is certified by one competent authority which is trusted by the signed document users.

The scope of the present document is to investigate on the attribute certification related topics in order to cover the general use of certified attributes in the context of electronic signatures. Attributes that can be used in such a context can also be used for other reasons, e.g. for authorization.

2 References

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

[1] ETSI TS 101 733: "Electronic Signatures and Infrastructures (ESI); Electronic Signature Formats".

[2] ETSI TR 102 041: "Signature Policies Report".

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

[4] ISO/IEC 9594-8 (2001): "Information technology; Open Systems Interconnection; The Directory: Public-key and attribute certificate frameworks".

[5] 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.

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

[7] ITU-T Recommendation X.520: "Information technology; Open Systems Interconnection; The Directory: Selected attribute types".

[8] IETF RFC 3281: "An Internet Attribute Certificate Profile for Authorization", S. Farrell. R. Housley, April 2002.

[9] EN 45013: "General criteria for certification bodies operating certification of personnel".

[10] ISO/IEC FDIS 17024 (2002): "Conformity assessment; General requirements for bodies operating certification of persons" draft.

[11] EAC/G4: "Guidelines on the Application of EN 45013", issued in September 1995 by the European Accreditation of Certification.

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

[13] ISO/IEC 9594-6: "Information technology; Open Systems Interconnection; The Directory: Selected attribute types".

3 Definitions and abbreviations

3.1 Definitions

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

attribute: information bounded to an entity that specifies a characteristic of an entity, such as a group membership or a role, or other information associated with that entity

Attribute Authority (AA): authority trusted by one or more users to create and sign attribute certificates

NOTE: It is important to note that the AA is responsible for the attribute certificates during their whole lifetime, not just when registering them.

Attribute Certificate (AC): data structure containing a set of attributes for an end-entity and some other information, which is digitally signed with the private key of the AA which issued it

Attribute Certificate Policy (ACP): named set of rules that indicates the applicability of an attribute certificate to a particular community and/or class of application with common security requirements or which indicates basic rules for registering, delivering and revoking attributes contained in certificates

Attribute Certification Authority (ACA): authority trusted to include attributes in either PKCs or ACs

Attribute Certificate validity period: the time period during which the attributes included in an attribute certificate are deemed to be valid

Attribute certification period: the time period during which ACs including a given attribute will effectively be provided by the AA

Attribute Certification Practice Statement (ACPS): statement of the practices that an Attribute Certification Authority employs in issuing certificates. authoritative

Attribute Issuing Authority (AIA): the authoritative source of an attribute

certificate: either Attribute Certificate or a Public Key Certificate

NOTE: Where there is no distinction made the context should be assumed that the term could apply to both an Attribute Certificate or a Public Key Certificate.

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

group membership: state of being a member of a group, e.g. a club, a company, an organization, an organization branch or a project

Privilege Management Infrastructure (PMI): the infrastructure able to support the management of privileges in support of a comprehensive authorization service and in relationship with a Public Key Infrastructure

Public Key Certificate (PRC): 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 (QC): Public Key Certificate that conforms to annex I from the Directive 1999/93/EC and that is issued by a Certification Authority that conforms to the requirements from annex II from the same Directive

NOTE: See [3].

role: function, position or status that somebody has in an organization, in society or in a relationship

3.2 Abbreviations

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

AA	Attribute Authority
AC	Attribute Certificate
ACA	Attribute Certification Authority
ACP	Attribute Certificate Policy
ACPS	Attribute Certification Practice Statement
AIA	Attribute Issuing Authority
ASN.1	Abstract Syntax No. 1
CA	Certification Authority
EESSI	European Electronic Signature Standardization Initiative
OID	Object IDentifier
PKC	Public Key Certificate
PKI	Public Key Infrastructure
PMI	Privilege Management Infrastructure
QC	Qualified Certificate

4 Implications from the requirements of the Directive

Directive [3] article 2(3) states that: "'*signatory' means a person who … acts either on his own behalf or on behalf of the natural or legal person or entity he represents*", introduces the need to define under which role do subjects sign.

Directive [3], annex I specifies that: "*Qualified certificates must contain (…) …*
(d) provision for a specific attribute of the signatory to be included if relevant, depending on the purpose for which the certificate is intended"

The previously quoted annex I (d) of the Directive [3] clearly lays down the possibility to include "*attributes*" in a QC (Qualified Certificate). This provides sufficient legal support to adopt QCs to specify Attributes, where deemed useful and applicable. This can be achieved by inserting them in the "title" field within the subjectDirectoryAttribute extension defined in ISO/IEC 9594-8 [4], as per IETF RFC 3039 [6].

It is to be noted that, although article 6(3), (4) and annex I (i), (j) of the Directive [3] also explicitly provide for the possibility to specify "limitation to the value of a transaction" and "limitations of use" in a QC, such data, that might be thought of as signer's "attributes", have their natural location respectively in the field "*QcEuLimitValue*", defined in TS 101 862 [12], and in the extensions *keyUsage*, *extendedKeyUsage*, defined in ISO/IEC 9594-8 [4].

On the other hand, as per the QC requirements stated in Directive [3] annex I, a QC must hold the signature verification data (letter e), so an Attribute Certificate cannot be a QC, since it bears no public key.

The following Directive [3] provisions are worth noting.

1) As per article 6(1), liabilities apply on issuing QC CSP, namely "as regards the accuracy at the time of issuance of all information contained in the qualified certificate …", which includes "provision for a specific attribute of the signatory to be included if relevant, depending on the purpose for which the certificate is intended", as per annex I, letter (d)

2) Annex II, letter (l), 3rd bullet requires that a QC may be publicly available only upon subject's consent. This requirement must be taken in account also when issuing attributes-specifying QCs.

Directive annex II (d) also puts a clear onus on the QC issuing certification service providers that specify subjects' Attributes: "verify, by appropriate means in accordance with national law, the identity and, if applicable, **any specific attributes** of the person to which a qualified certificate is issued".

From the previous Directive excerpts it is clear that specific requirements are to be met by any authority that certifies any kind of attribute.

If this authority is the same CA that issues PKCs certifying attributes, e.g. through the subjectDirectoryAttribute extension, then the Certificate Policy shall be enriched with additional requirements related to attribute Certification.

If it is an Attribute Authority issuing Attribute Certificates, then AAs shall specify in every AC the applicable Attribute Certificate Policy.

5 European surveys

A survey has been performed in order to ascertain, at least in Europe:

1) if the current requirements of personnel certification, by accredited certification bodies, matches the forecast usage of attribute certificates;

2) currently implemented attribute certificate usage.

5.1 Personnel certification

In addition to perusing EAC/G4, the following certification organizations accredited by national bodies have been contacted, by phone and by e-mail:

France

- AFNOR
- BRGM (BUREAU RECHERCHE GEOLOGIQUES MINIERES (see note)

Germany

- TGA-GMBH (see note)
- TUV Akademie Rheinland - Koeln

Italy

- CEPAS (see note) Documentation available on the Internet - www.cepas.it

The Netherlands

- Det Norske Veritas
- Kema Quality
- KIWA NV

NOTE: Marks those that provided Task2 with support or documentation.

As more in detail explained in clause 7.2.1, it has been learned that the basic difference between bodies addressed by EN 45013 [9] and Attribute Certification Authorities resides in that an ACA ("authority trusted to *include attributes in either PKCs or ACs*") takes no commitment on the subject's actual competency "in performing specific services", which is instead "the raison d'être" of personnel certification bodies acting in compliance with EN 45013 [9].

It has been taken into consideration that very little usage of attribute certification is still in force, relevant to the capacity of persons to exhibit In order to ascertain the attribute certification correspondence with the "real world".

5.2 Currently implemented attribute certificate usage

A survey within the PERMIS European project has been performed.

The following three organizations participating to the PERMIS project have been contacted:

1) Municipality of Bologna.

2) Safelayer Secure Communications S.A. - Camerfirma (Partners in the Municipality of Barcelona implementation).

3) Prof. David Chadwick of the University of Salford, partner in the Municipality of Salford implementation).

The outcome of such survey is that only the Barcelona project makes use of practices to certify attributes. In fact:

1) the Municipality of Bologna currently does not make use of ACs;

2) the Municipality of Salford implementation covers only an AC based application, and expects that Attribute Certification Authorities implement the practices they deem suitable for their environment.

It is interesting to make a few remarks on the Practices Camerfirma makes use of, to issue attribute specifying PKCs to legal entities representatives.

In addition to the subject's Identification documents, public or private documents are required, asserting the juridical person of the legal represented entity. Additionally, where necessary, documents specifying in a formal manner the specific powers implied by this Company position. An example of powers to be specified is also provided for in the practices.

This "real world" example endorses the present document provisions not to require an ACA to directly assess the subject's capability to exert the specific services related to the certified attribute. Rather, it shall ascertain that the documents that corroborate the attribute assertion are valid.

The Italian Assocertificatori association has been contacted as well. Please find in annex B an extract of the document it issued on issuing PKCs specifying attributes. The present document, currently in force for the Assocertificatori members, was drafted and approved by a specifically appointed Work Group composed of experts from Assocertificatori members, external consultants and a relevant governmental body. It has been added as an annex of the present document because it implements its basic principles, of which it provides a valuable field test.

6 Various kinds of attributes

An attribute may specify group memberships, roles, or other authorization information. This clause lists examples of attributes and their uses.

6.1 Group memberships

Group membership apply to hierarchical groups or functional groups.

Hierarchical groups involve several persons belonging to the same organization branch of an enterprise or a company. It specifies the position of the individual within an enterprise or a company.

Functional groups involve several persons having the same function or working on the same project.

6.2 Roles

A role is a way of expressing an organizational or functional responsibility. The responsibility is often mirroring a user's job title. It may be fulfilled by just one person (e.g. head of department) or by several persons.

A role also designates an individual's status in a particular society. It corresponds to a socially expected behaviour pattern.

Within an organization or a company, roles usually specify a job function. In some cases the job can only be filled by a single individual. Example: CEO of the company, Financial Director.

Subjects can be assigned different roles depending on the organization type they belong to: Companies, Public Administrations, Educational organization, Public Offices, religious bodies, professional associations, etc. Subjects can be assigned several roles at the same time.

One subject can be assigned more than one role, either within a single organization (e.g. "CEO" + "CFO ad interim"), or from different organizations.

A role may be defined independently of any individual. Most processes involve tasks performed by individuals, not because of who they are, but because of the role they have. Once roles have been defined, then they can be assigned to one or more individuals.

Roles in an enterprise are relatively stable and may be a first approximation of the invariant of the enterprise. They are frequently defined at the enterprise level. Their administration is often performed by a User Administrator or Role Manager.

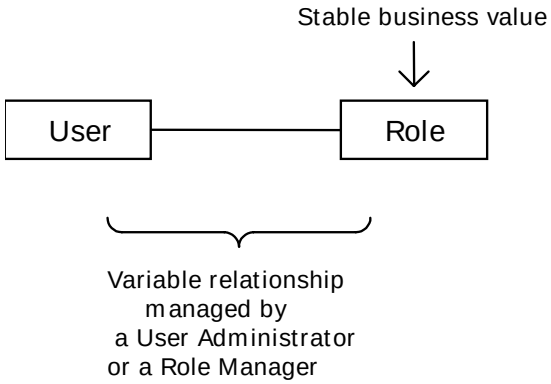


Figure 1: Roles: a stable concept in an organization

As figure 1 illustrates, the ease of management relies on the stability of the role concept, since if it is changed, the change will need to be simultaneously managed at all points in the system where that role is used.

The attraction is that applications need only know about roles, instead of caring for identities to know whether a given signature is appropriate and only use the identity for auditing purposes. The management of change is therefore greatly simplified, since applications can only be aware of the roles and thus ignore the names of the individuals when making sure that a signed document is valid for the application.

Some examples will illustrate:

- When people leave or join the company, the User Administrator removes or adds the person names from the role. There is no need for applications to do anything.
- When a person changes job within the organization, the user administrator simply changes the role(s) associated with that user. There is no need for applications to do anything.
- When a new application is supported, the application administrator needs only decide which roles are permitted. There is no need for a user administrator to do anything further.

In some cases it should be noted that the revoking authority may be different from the role certifying one. An example of this kind, listed in the table from annex A, is the Italian Notary, who is appointed by the President of the Republic, is assigned to a seat by the Minister of Justice, but can be revoked only by a Court. Such very peculiar cases are recalled in order to remind that beyond what is detailed in the present document, additional requirements may occur, depending on specific legal or local requirements.

A role may denote the function, the position or the status that somebody has in an organization, in society or in a relationship. In order to illustrate this, a few examples are provided below:

- function in society: mayor, bishop, judge;
- function in a company: CEO, financial Director;
- function in an organization: Managing director, secretary, treasurer;
- status in society: Doctor honoris causa, Academic Palms, first aid certified, senior citizen;
- position in society: Republic President, Doctor es sciences from Harvard University;
- status in an organization: Company fellow.

These different roles may be delivered by various kinds of authorities:

- a company;
- an organization (Payment protection scheme, Health protection scheme);
- an association (Club, Trade Union, Trade association, Charity);
- a school, a University;
- a Government body (e.g. Justice Department, Ministry);
- a religious body.

6.3 Other authorization information

In this category, two authorization information are being considered:

- proxies; and
- capabilities.

6.3.1 Proxies

A subject may sign on behalf of another individual, either under the name of that individual or under an attribute from that individual.

The person delegating its signature may like to restrict the use of its attributes, so that the signature can only be applied under some signature policies or/and for some commitment types. This means that each attribute may potentially be individually restricted. It should be noticed that the targeting information currently defined in [8] is tailored to be used for access control purposes only.

A subject may temporarily act on behalf of another person. This can technically be achieved in two ways:

- an AA issues to a delegate an AC which includes all or part of the delegating person's attributes;
- the delegating person directly delegates to the delegate all or part of his/her functions by issuing him/her, an attribute certificate signed by himself/herself that includes all or some of his own attributes;

The delegating person may limit the delegated powers by using a few possible different ways, that depend on whether the delegate is issued a certificate directly by the delegating person or by a third party AA.

If the delegate is issued an AC by an AA which is not the delegating person itself, he/she might be issued an attribute subset encompassing only a restricted delegating person's attribute set.

If the delegate is directly empowered by the delegating person, two possible ways can be envisaged:

1) wisely crafting the delegating person's attribute set granularity (when an ACA initially certifies his/her attributes) so that he/she can carefully select which ones are to be delegated, depending on the delegate;
2) making use of a "restriction" extension which could specify in which context(s) the attributes may be used.

6.3.2 Capabilities

Capabilities are well known when used in an access control context. In a capability-based system, access to protected objects such as files is granted if the would-be accessor possesses a capability for the object. The capability can be implemented by using a token that gives the bearer or holder the right to access a system resource. Possession of the token is accepted by a system as proof that the holder has been authorized to access the resource named or indicated by the token.

In the context of an electronic signature, a capability would be interpreted as the right to use a commitment type under a policy.

This implies that every time a new signature policy/commitment type is created, signers need to be given a new capability. This can be easily used when there are a few signature policy/commitment types and numerous signers, but is of limited use when there are many signature policy/commitment types.

7 Claimed and certified attributes

7.1 Claimed attributes

An attribute may be claimed instead of being certified. When it is claimed, the claimant will be responsible for the assertion and in case the assertion is proven to be false, it will have to support the consequences. When the role is a company role, and if the verifier finds out later on that the signer did not had the authority to sign under that role, it will first be a legal issue between the verifier and the company the individual belongs to, and then a legal issue between the company and the individual.

Some applications may accept attributes that are claimed by the end-users, whereas some other applications may only accept attributes that are certified. Therefore certified attributes are not always necessary.

7.2 Certified Attributes

When an attribute is certified, it is certified by an ACA based information provided by an AIA. The same organization may be in charge of both the ACA function and the AIA function; in such a case attributes are said to be directly-certified. When different organizations are involved, the ACA takes the information provided by the AIA; in such a case attributes are said to be verified. The Directive requires liabilities on the CA if it lacks accuracy on the data included in the Qualified Certificate, including, therefore, attributes. This principle is extended to ACAs.

7.2.1 The Attribute Issuing Authority

In EN 45013 [9], clause 2.5 mentions:

"Document issued under the rules of a certification system, indicating that adequate confidence is provided that the named person is *competent in performing specific services*."

The AIA is an authority that ascertains "that the named person is competent in performing specific services", as per EN 45013 [9]. The AIA skills must be adequate to assess the person's competence, while the ACA skills is based on ICT knowledge, more specifically on PKI and PMI. There is a clear separation between the competence of the AIA and the competence of the ACA, while in some cases a single organization can support both functions. However in such a case a clean separation has to be maintained between the personal in charge of each function.

The ACA makes use of documents or information provided by the AIA.

The above conclusion has been drawn from three sources:

1) EAC/G4 [11];

2) Draft ISO/IEC FDIS 17024 [10]; and

3) Quality Assurance Handbook of a French accredited personnel certification body.

EAC/G4 [11**]**

In EAC/G4 [11], clause 2.5 EAC Guidance, item 3 states that a "Certificate of competence" is intended to "give confidence to all concerned that the person named in it is competent to undertake specified tasks or has some other specified competence. Reference should be made to documents in which the statement of this competence is given. They could be standards, other normative documents or statements issued by appropriate bodies indicating specific competence to which the certificate attests." Item 5 in the same clause states: "[t]he basis of assessment should be stated e.g. written examination, practical test, involvement in the field over a period etc or any combination of such.", which is a requirement on the AIA.

Draft ISO/IEC FDIS 17024 [10**]: 2002(E)**

Draft ISO/IEC FDIS 17024 [10] states in its Introduction: "one of the characteristic functions of the personnel certification body is *to conduct an examination*", assertion which is corroborated by its clause 3.9 - examination: "mechanism *that is part of the evaluation*, which measures a candidate's competence by one or more means such as written, oral, practical and observational".

Additionally, as far as separation of person certification function is concerned, draft ISO/IEC FDIS 17024 [10]: 2002(E) clause 4.2.4, item b) states:

"The certification body shall:

……

b) have policies and procedures that distinguish between the certification of persons and any other activities,"

Quality Assurance Handbook

This handbook details the criteria taken in account to assess a person's qualification. This spans from the person's initial education through his/her practical experience and complementary education to stages the person has done within and under the certification body supervision. Finally, the candidate has to undergo a practical test to demonstrate his/her actual skill.

The basic difference between bodies addressed by EN 45013 [9] and an Attribute Certification Authority is the following: The ACA is the "authority trusted to *include attributes in either PKCs or ACs*". This does not imply that an ACA takes any commitment on the subject's actual competency "in performing specific services". Clause 6.2.2 of the present document, while envisaging that an ACA shall "specify in its Attribute Certification Practice Statement the details of the official information and practices upon which the attributes have been issued", clearly makes no such requirement on the ACA to directly assess that the subject "is *competent* in performing specific services".

In other words: it is to be clear that an ACA is only trusted "to include attributes in either PKCs or ACs", which means that it shall only ascertain (by ways it shall publish in its Attribute Certification Practice Statement) that the individual is actually entitled to get a certain attribute. It is useful to highlight that no direct involvement of the ACA is required to assess the actual skill and competence of the certified person by means of exams, tests, stages, etc.: this is a requirement on what the present document defines as an Attribute Issuing Authority: "authoritative source of an attribute".

If the same organization is both an ACA and an AIA, the last paragraph of clause 11.1.1 makes clear that the organization division that acts as an ACA must be independent from its division acting as the AIA.

7.2.2 Directly certified attributes

Attributes are directly certified when the authority issuing the certificate (i.e. the ACA) is also the authoritative source of an attribute (i.e. the AIA).

This is the case, for example for judges which are testified by the official bodies (i.e. the Lord Chancelor Department for judges). This may also be the case for roles defined by an organization or a company where only some managers provide the roles. It may be, for example, the Human Resources Department or an individual in the organization's or company's hierarchy.

When the attribute certification authority is "the" authoritative source of an attribute officially and fully entitled to bestow the to-be-certified attribute, no doubt reasonably exists on the attribute itself.

7.2.3 Verified attributes

Attributes are verified when the authority issuing the certificate (i.e. the ACA) is not the authoritative source of an attribute (i.e. the AIA).

Before being granted, attributes shall be verified in a way that the ACA has no reasonable doubt on their truth. It shall be verified that, at the time of registration for that attribute, the individual was entitled to get that attribute.

Since the Attribute Certification Authority is liable for the accuracy of the attributes, it is up to the attribute Certification Authority to choose how to ascertain the attribute accuracy for which it will be liable.

The Attribute Certification Authority shall specify in its Attribute Certification Practice Statement the details of the official information and practices upon which the attributes are verified.

In any case, the Attribute Certification Authority shall keep a copy of the official information upon which the attribute has been verified. This information may have been presented to the ACA or collected by the ACA.

8 Attribute meaning and representation

8.1 Attribute meaning

As a basis to decide whether an attribute can be used in an application, a clear description of the meaning of an attribute is needed. That description shall be given in readily-understandable terms, and if appropriate the law that defines the attribute shall be indicated. There must be a way to find the description.

8.2 Attribute representation

Once an attribute is defined, it is important for a verifier to be able to recognize it. An attribute can be:

- either only directly user understandable; or
- only machine processable; or
- both machine processable and user understandable.

An attribute that is only user understandable is not able to be processed and directly compared with conditions stated by the signature policy. Therefore it has to be interpreted by a human being to find out if the role is adequate or not. If an attribute is directly user understandable, then a **character string** may be appropriate.

An attribute that is machine processable can be processed and directly compared with conditions stated by the signature policy. This allows to automate to a greater extend the verification of electronic signatures. If an attribute is only machine processable, an **OID** or a DN (e.g. "cn=System Admin,o=ETSI) may be appropriate.

When a character string is being used, that string is language dependent and may only be easily understandable in one country. While this is certainly useful, this does not allow an easy recognition by humans among all the EU countries. In many cases, attributes in one country have an equivalence in another country. For example, a CEO is a well understood position within a company and may have some equivalence in each of the EU countries. Some documents need to be signed by a CEO and therefore an easy recognition of this position would be beneficial. A machine processable CEO position would allow an automatic verification of contracts or documents that need to be signed by a CEO.

It would be adequate to conduct a study about the equivalence of some "useful" attributes, that have an equivalence among all the European countries.

Thereafter, it would be appropriate to use a simple way to represent each such useful attribute. While a character string would not be the most appropriate means to convey the information, an OID, which is a sequence of integers, would do the job much better.

8.2.1 Group membership

The group attribute carries information about group memberships.

8.2.2 Role

The role attribute is the only attribute specified in ISO/IEC 9594-8 [4]; it carries information about roles. It is composed of two components: a role Authority and a role name.

The role Authority is optional: when the AIA is not the AA, it allows to identify the AIA for that role.

The role name contains the definition of the role. Many syntaxes are possible for it. For example, it can be either a character string, an OID or a URI.

9 Other Attribute characteristics

9.1 Attribute life span

Three major **attribute validity** classes have been identified:

1) life lasting: the attribute is linked to the individual for his/her entire life; nevertheless the individual, under exceptional conditions, can be stripped of his/her attribute; examples can be: honorific position, professional position, like lawyer or physician, and clerical status;

2) long lasting: the attribute usually lasts longer than the individual's PKC validity period; where necessary this attribute can be revoked, e.g. CEO, Minister;

3) short lasting: the attribute life is shorter than the PKC's validity period; examples can be: member of a commission lasting a few weeks; this type of attribute may or may not be revoked: see clause 8.4.

9.2 Attribute certification period

1) The Attribute life span is a main criterion to be used in order to know whether an attribute should be placed in a PKC or an AC. Once the decision to place it in an AC is taken, then the ACA has to decide how long it will accept to certify this attribute. This time period is called the **Attribute certification period**. The AA may charge its services for that time period.

9.3 Attribute certificate validity period

Even if the life span of an attribute is large, it is not necessary to certify that attribute by issuing an attribute certificate for its whole life-span period. The attribute certificate validity period should not be confused with the attribute certification period. The **attribute certificate validity period** is the period during which some attributes included in a certificate are deemed to be valid. The attribute certificate validity period is always smaller than or at most equal to the attribute certification period.

9.4 Attribute revocation and Attribute Certificate revocation

In many cases, in order to avoid a revocation status check, which implies to query some server, attributes will be granted by an AA for a period of time that is short enough so that revocation is not considered to be meaningful. This can be hours, a day, a week or more. It should be noted that validity periods longer than one day might not be applicable in some cases.

In that case, the mechanism used to convey the attribute will even signal that there is no revocation status information managed by the authority that has granted the attribute.

When revocation is supported, this can be provided by an on-line server (like OCSP) or via an off-line mechanism (like Attribute Certificate Revocation Lists). Users are required to test the revocation status of ACs, according to the signature policy, unless the AC contains information saying that no revocation status is available for that AC.

It is possible to distinguish between:

- attributes that are usually revoked only in exceptional cases (e.g. like life-lasting attributes);
- attributes that can be revoked at any time;
- attributes the revocation of which is not handled, for example for honorific attributes, like Doctor honoris causa or Professor emeritus.

Attributes can be managed in two ways:

- by assigning an attribute validity period equal to their attribute life span, while managing revocation status information;
- by assigning an attribute validity period much shorter than its life span (e.g. by periodically renewing the attribute) without the need to manage the revocation status information. This kind of attribute is called "ephemeral".

When looking at a single attribute certificate, it may be impossible to tell when the attribute was initially both registered and verified and until when the attribute will be certified: this is because the beginning of the attribute certificate validity period does not necessarily match with the time of the initial registration and because the end of the attribute certificate validity period does not necessarily match with the end of the attribute certification time.

9.5 Attribute privacy

Users may not necessarily want to always disclose all of their attributes. For that reason these attributes should not be included in PKCs but only included in ACs which are then only attached to the documents that need to take advantage of them.

9.6 Ways to acquire attributes

There are threeways to acquire attributes:

- by default, when they are included in a PKC;
- upon request, when they are included in an AC;
- by getting them from ACs stored in a repository.

In the first case, individuals do not ask themselves for their attributes, but have them by default assigned to them in PKCs. In the second case, individuals specifically ask for being granted some attributes. In the last case, pre-produced ACs are stored in a repository and can be accessed either by the subjects only or both by the subject and the relying parties.

9.7 Delegable attributes

Some attributes may only be directly assigned to an individual (and be non-transferable), while some others may be designated as delegable. It is not because an attribute is delegable that anyone that has the attribute type may be allowed to delegate it. Some individuals may be designated to have the right to delegate that attribute.

In the usual proxy case, while an individual is going on vacations and for the time of his vacations, he allows someone else to impersonate him. When talking about attributes, this means to allow the use of some (but not necessarily all) of his attributes.

This is one typical case where the delegating person delegates someone else to exert only a subset of its attributes.

It is advisable that such delegation occurs only for a limited time and to as few people as possible, preferably only one. It is also advisable to only allow delegation one level down and prevent to sub-delegate any further. The trust will mostly diminish/lessen if the chain of delegation gets too long.

Another dimension to consider is the application of some restrictions to the attributes. Normally attributes may be accepted in any context, i.e. for signing any kind of document. In the case of delegation, the delegating person may wish to apply restrictions so that the attributes can only be used in some restricted context, i.e. some kinds of documents. This feature is usually known as a **restriction**. In that case, the restriction may include the signature policies and/or the commitment types for which the attribute can be used.

It shall always be possible to know who has performed the delegation. When roles are involved to be able to sign, then for accountability reasons, the name of the delegating person shall either be directly or indirectly traceable.

10 Placement of attributes in certificates

There are two ways to certify attributes.

- using Public Key Certificates,
- using Attribute Certificates.

In any case a subject needs at least one PKC. Therefore a subject may end up owning:

a) one or more PKCs, possibly issued under different certificate policies and with different validity periods each one with zero or more attributes;

b) none, one or more Attribute Certificates issued by one or more AAs; each AC points to one and only one PKC and may include one or several attributes.

X.509 [4] defines a certificate validity as "the time interval during which the CA warrants that it will maintain information about the status of the certificate".

Therefore, a CA which is also an ACA could, theoretically, rightfully issue a PKC that includes attributes having a life span shorter than the PKC validity: provided that the CA revokes the PKC at attribute expiration, no security breach would arise, but PKCs would need to be revoked and re-issued quite frequently.

On the other hand IETF RFC 3280 [5] indicates: "When a certificate is issued, it is expected to be in use for its entire validity period. However, various circumstances may cause a certificate to become invalid prior to the expiration of the validity period. Such circumstances include change of name, change of association between subject and CA (e.g. an employee terminates employment with an organization)". However, the exact circumstances under which a certificate may be revoked are left open.

The CA is not mandated to continuously monitor the validity of the attributes that it grants, but shall revoke a certificate, if informed that an attribute in it is no longer valid.

Since certificates might be revoked as soon as one of the attributes is no more valid, it is recommended that attributes are included in a PKC only if their life span is no shorter than the PKC validity. This recommendation derives from two major reasons:

1) the certificate is "expected to be in use for its entire validity period". If the PKC were issued bearing an attribute which is known to expire before the belonging PKC, this one would not be "expected" to have such duration;

2) if a PKC were issued under these deprecated conditions, CRLs would soon bloat with impact both on issuing CA and on users.

It is also to be outlined that the basic difference between PKC and AC is that a PKC needs be issued by a CA (which might be a QC issuing CSP), while ACs can be issued by AAs that are not CAs.

10.1 Using Public Key Certificates

There is need to minimize the information to be kept on identity certificates. Public-key certificates can natively support some attributes. There are two means to do so:

- using the *Common Name* attribute type (see [7]), and/or
- using the *Title* attribute type (see [7]).

The *Common Name* attribute type specifies an identifier of an object. A Common Name is a name by which the object is commonly known in some limited scope (such as an organization) and conforms to the naming conventions of the country or culture with which it is associated.

An attribute value for common name is a character string. For example, a typical name of a person in an English-speaking country comprises a personal title (e.g. Mr., Ms., Rd, Professor, Sir, Lord), a first name, middle name(s), last name, generation qualifier (if any, e.g. Jr.) and decorations and awards (if any, e.g. QC).

EXAMPLE 1: CN = "Mr. Robin Lachlan McLeod BSc(Hons) CEng MIEE"; (This example is copied from the ISO 9594-6 [13]).

When the Common Name comprises a personal title, decorations or awards, it shall be realized that these attributes become part of the name and thus cannot be individually tested. So they will not be usable under a signature policy. Therefore if these attributes are going to be usable, they shall be placed in the subjectDirectoryAttributes extension.

The *Title* attribute type specifies the designated position or function of the object within an organization. An attribute value for Title is a string.

EXAMPLE 2: T = "Manager, Distributed Applications". This example is copied from the ISO/IEC 9594-6 [13].

Since a role is a function, a position or a status that somebody has in an organization, in society or in a relationship, the notion of *title*, as defined in X.509, maps to the notion of role rather than the notion of title (e.g. Mr., Ms., Rd, Professor, Sir, Lord). In order to avoid a misinterpretation, the use of the Title attribute type in the "subject" field is deprecated.

Public-key certificates may contain a subjectDirectoryAttributes extension that contains attributes associated with the subject of the public-key certificate.

IETF RFC 3039 [6] provides for the possibility to insert into the subjectDirectoryAttribute the following attributes:

title;
dateOfBirth;
placeOfBirth;
gender;
countryOfCitizenship; and
countryOfResidence.

Where "The title attribute type SHALL, when present, be used to store a designated position or function of the subject within the organization specified by present organizational attributes in the subject field." The association between the title, the subject and the organization is not described."

IETF RFC 3039 [6] has focused on the attributes that were useful to directly support QCs and thus the above list of attributes should not be taken as limitative. To summarize, three places allow to include attributes:

- in the *Common Name* attribute type; the use of this attribute is deprecated. If used, then it becomes part of the name;
- in the *Title* attribute type in the "subject"; the use of this attribute is deprecated, because its official definition is closer to the definition of a role;
- in the PKC *subjectDirectoryAttribute* extension; the use of this attribute is recommended.

If the CA is also the ACA, it may issue a PKC that includes the attribute to be certified, or it may revoke the existing PKC and re-issue a new PKC including the attribute to be certified.

Directive [3] stipulates that compliant CAs are liable, as a minimum, for all the information that is present in a qualified certificate at the time of registration - article 6(1). This includes also the attributes. Thus, unless more strict national rules of law are provided at least for use within the public sector (article 3(7)), CAs are not bound to any verification subsequent to issuance time.

10.2 Using Attribute Certificates

The authority for assignment of some attributes may be different from the authority issuing a public-key certificate and different attributes may be assigned by different Attribute Authorities (AA), hence a different authority is needed to grant these attributes.

An Attribute Certificate is a data structure issued by an Attribute Authority which contains a set of attributes for an end-entity and some other information allowing to link that data structure to a PKC. The whole structure is digitally signed with a private key of the Attribute Authority which has issued it.

Currently there exist specifications ([4] and [8]) describing data structures to support the concept of an Attribute Certificate. It should be noticed that these data structures do not include a provision for the definition of an Attribute Certificate Policy, similar to a Certificate Policy. This concept is needed and an extension should be defined to support it.

In the more general case, attributes will have lifetimes that do not match the validity period for a public-key certificate. Attributes should not be placed in PKCs (see clause 9) when attributes have a lifetime shorter than the binding of the identity and the public key. In this case attributes should be separate from the PKC and should be issued in Attribute Certificates.

Privacy reasons may also lead to separate attributes so to enable the subject to selectively apply only the ones strictly required by specific Signature Policies. This could be implemented by issuing a set of ACs, each one referenced by an attribute subset name.

As per IETF RFC 3281 [8], the attribute policy authority is an organization that allocates attribute values, whereas the AC issuer is one of the servers managed by that organization. A distinction between the AC issuer and the attribute policy authority has to be made. This is useful for situations where a single attribute policy authority (e.g. an organization) allocates attribute values, but where multiple AC issuers (i.e. servers) are deployed for performance or other reasons.

11 Attribute Certificates management

11.1 Attribute verification by the ACA

The only liability provided on the CA in Directive [3] article 6(2), that may be applicable also for attribute verification, is "for failure to register revocation of the certificate unless the certification-service-provider proves that he has not acted negligently." Therefore a PKC issuing CA is not required to necessarily verify attributes, as well as any other information kept in a PKC, after its issuance time, provided that it promptly revokes it upon request. Thus, lacking any additional commitment by the CA, the attribute may be **only be verified at the time of registration**. In this case, should any value inside a PKC be subject to a change, it is the responsibility of the bearer (or of the third party under whose assertion/request the PKC has been issued) to inform the CA and to ask for the revocation of the certificate.

NOTE: This is an additional reason for which attributes included in a PKC should have a life-time longer or equal to the validity period of the certificate. If, in a PKC, a CA only includes attributes that have a life-time longer or equal to the validity period of the certificate, then these attributes can always be trusted until revoked upon request.

For ACs, presently there exists no rule, so it is possible to define policies that make a difference between:

- attributes that are only verified by the ACA at the time they are registered,
- attributes that are subsequently checked by the ACA for their continued accuracy.

When attributes are **subsequently checked for their continued accuracy**, a confirmation must be done at some regular time interval (i.e. by making a periodic verification), otherwise the attribute will no longer be associated with the individual. **Subsequent verifications** are not necessarily **directly** done by the AA, but, can be **delegated**. At the time of registration, the individuals or the authority able to ask for the confirmation or for the revocation of the attribute should be nominated.

11.2 Link with a PKC

Attribute Certificates contain attributes and are unambiguously linked to the subject's PKC by referencing it via the *baseCertificateID* as defined in [4]. The "*baseCertificateID*" indicates the Issuer name (and optionally its *UniqueIdentifier*) and the serial number of the certificate owner's PKC.

When a subscriber applies for an attribute, he/she shall present one of its PKCs. The AA shall make sure that the PKC that is presented has actually been issued to the subscriber, otherwise another person would be granted an attribute he/she is not the rightful owner of. This shall not be accomplished by authenticating the individual, e.g. taking advantage of an authentication exchange using the existing PKC, but rather by making sure that the certificate was indeed delivered to the right person.

There are basically two ways to achieve this goal:

- the identifier (i.e. the subject name and/or the subjectAltName) contained in the PKC contains information which directly maps to information contained in an identity card that is presented to the AA; otherwise
- the CA must provide to the subscriber an attestation which allows to relate the already issued PKC to the registration information that was presented by the person when requesting the PKC.

The former case may be illustrated by the following example: the Italian rules of law require QCs to specify in the subject name the person's Fiscal Code which is derived from the person's name and from his date and place of birth. Thus, if one exhibits to the AA: a valid identity document, the PKC, the plastic card where his Fiscal Code is embossed, and the document proving he's entitled to the attributes he's requiring the certification of, there is no reasonable doubt about who's the attribute rightful owner.

The later case places a requirement on the CA: when a subscriber may want to obtain an AC linked to its PKC, then the CA must be able, upon request from the subscriber, to deliver an attestation to the subscriber that allows to confirm that the certificate belongs to the right individual. This attestation may be provided at the time of the initial registration to the CA, or at any time later on.

Should a PKC reach the end of its validity period or should it be revoked, all related ACs will become unusable. When the PKC to which an AC is linked is close to the end of its validity period, such that the AC validity period spans beyond the PKC end of validity time, the presentation of another PKC is necessary, but it is not always necessary to provide again the attestation from the CA: if the CA has renewed the PKC, this means that it has verified the registration information again. If the subject field of the new certificate is identical to the previous certificate, then the AA may check the equality of the subject fields from the two PKCs from the same CA. To this end, it is recommended to only place long term and stable information in the DN subject name. Temporary information like e-mail and postal addresses should be placed in the subjectAltName extension.

It should be noticed that IETF RFC 3039 [6] mentions that the subject field SHALL contain an appropriate subset of the following attributes:

countryName;
commonName;
surname;
givenName;
pseudonym;
serialNumber;
organizationName;
organizationalUnitName;
stateOrProvinceName
localityName and
postalAddress.

If an AC is going to be linked to a QC, then for a QC issued to an individual person (i.e. not identified as working for a company), because a change of the postal address may be frequent, the incorporation of the following attributes in the subject field should be considered with great care:

stateOrProvinceName
localityName and
postalAddress.

In such a case, the following subset of attributes is recommended:

countryName;
commonName;
surname;
givenName;
pseudonym;
serialNumber.

If an AC is going to be linked to a QC, then for a QC issued to a person identified as working for a company, because a change of the organization unit name may be frequent, the incorporation of the following attribute in the subject field should be considered with great care:

organizationalUnitName.

If the CA is not also the ACA, an AA will issue an AC that points directly or indirectly to an already issued PKC. The Holder field from an AA indicates the link with the PKC.

The Holder field is a SEQUENCE allowing three different (optional) syntaxes: baseCertificateID, entityName and objectDigestInfo. IETF RFC 3281 [8] RECOMMENDS that only one of the options be used in any given AC. It seems, at a first glance, that either baseCertificateID or entityName could be used.

```
          Holder ::= SEQUENCE {
                baseCertificateID   [0] IssuerSerial OPTIONAL,
                          -- the issuer and serial number of
                          -- the holder's Public Key Certificate
                entityName          [1] GeneralNames OPTIONAL,
                          -- the name of the claimant or role
                objectDigestInfo    [2] ObjectDigestInfo OPTIONAL
                          -- used to directly authenticate the holder,
                          -- for example, an executable }

GeneralNames ::= SEQUENCE SIZE (1..MAX) OF GeneralName

GeneralName ::= CHOICE {
     otherName                       [0]     OtherName,
     rfc822Name                      [1]     IA5String,
     dNSName                         [2]     IA5String,
     x400Address                     [3]     ORAddress,
     directoryName                   [4]     Name,
     ediPartyName                    [5]     EDIPartyName,
     uniformResourceIdentifier       [6]     IA5String,
     iPAddress                       [7]     OCTET STRING,
     registeredID                    [8]     OBJECT IDENTIFIER }
```

When the baseCertificateID option is being used, then the life time of the Attribute Certificate is constrained by the life-time of the PKC: it cannot last longer than the validity period of the PKC. This has severe implications: close to the end of the validity period of the certificate, the next certificate from the same CA with the same subject DN must be made available to the AA so that the new certificate serial number can be used. In order to allow the renewal of Attribute Certificates without the need for the subscriber to present a new attestation for the renewed certificate, the AA should take notice of the subject DN contained in either the subject field or the subjectAltName extension (another way is to take a copy of the full certificate).

If the PKC is not renewed, then a certificate from another CA has to be made available to the AA and it must be proven that it belongs to the right individual.

IETF RFC 3281 [8] specifies: "If the holder field uses the entityName option and the underlying authentication is based on a PKC, the entityName MUST be the same as the PKC subject field or one of the values of the PKC subjectAltName field extension (if present)". It is to be noted that IETF RFC 3281 [8] is relevant to authorization. Therefore parts of it may not apply to non-repudiation signatures or data origin authentication. In fact, in such case this definition has two problems:

- the name of the CA is ignored;
- the match must not be done with any of the values of the subjectAltName extension but only with the directoryName that contains a DN, because this DN is then guaranteed to be unique for the CA (see IETF RFC 3280 [5], clause 4.2.1.7).

If the entityName option is going to be used, since the structure of that field does NOT explicitly contain the name of the CA, then the structure of the entity name is not defined with enough precision to unambiguously point to a certificate issued by a given CA. For that reason this option cannot be used in an open environment involving more than one CA. It would be necessary to enlarge the meaning of that field, so that it can include not one element but two:

- a DN to be compared with either the subject field from the certificate to which the AC is linked, or with a DN contained in the directoryName from the subjectAltName extension; and
- a DN to be compared with the issuer field from the certificate to which the AC is linked.

11.3 Attribute Certificate revocation management

When the AC validity is so short that the duration of the revocation process, leading to a status change, is such that the new status (i.e. "revoked") would be issued when the certificate has already expired, there is no need/usefulness to maintain an attribute certificate revocation status information.

When the intrinsic transaction value is so negligible that applications or verifiers are not interested in verifying the attribute validity, checking the revocation status information may be skipped.

When the attribute type itself is believed to be very unlikely to be revoked, then the user might choose under his/her sole responsibility to skip checking the revocation status information.

Revocation is handled very differently from the case of a PKC. The revocation will not necessarily be requested on one particular Attribute Certificate, but on all active Attribute Certificates that contain a particular attribute. This means that the AA must keep track of all currently valid Attribute Certificates so that he can then know which ones need to be revoked, if any.

This also raises an issue: if a subscriber asks for a particular attribute subset name that contains an attribute that has been revoked, the subscriber should be informed of the reason why the attribute will not be present in the AC.

The AA shall indicate in its Policies the conditions to revoke the attributes.

11.4 Attribute Certificate acquisition

Once attributes are registered, they need to be made available to subscribers in the form of an Attribute Certificate.

In some cases, an individual would like to exercise a subset of its attributes. This relates to the principle of "*least privileges*", where only the privileges useful for an operation are presented. So that are requirements to provide upon request a subset of the attributes.

When the ACA is able to register more than one attribute, the end-user may wish to obtain a subset of its attributes in one AC. In that case, the subsets may be defined by the end-user or by the ACA.

- when defined by the end-user, ways to see all the attributes and to group them by assigning attribute set names should be made available to the end-user.

NOTE: An "attribute set name" is a way to name a set of attributes, that may include attributes like group-memberships, roles, clearances, etc. This notion has been covered in the past under the "role name" concept which has very often be confused with the notion of a "role attribute".

- when defined by the ACA, the end-user must have ways to see all the attribute set names and the attributes that correspond to these sets.

Another reason for getting attributes separately is the fact that different authorities may be involved, each one managing a different set of attributes.

Once attributes have been registered by the AA, there are several ways for the subscriber to obtain an AC. This differs from the case of a PKC where, after registration, one and only one PKC is available for a long validity period. ACs may be obtained:

1) by asking the "default" AC, where the attributes that are contained in it are defined by the AA;

2) by specifying an attribute set name, where the attributes that are contained in it are defined by the AA;

3) by specifying an attribute set name, where both the attribute set name and the attributes that are contained in it, are defined by the subscriber;

4) by specifying an attribute set name, where both the attribute set name and the attributes that are contained in it, have been defined by a delegating individual.

The AA shall indicate in an "AC Practice Statement" how AC can be acquired.

It should be noticed that currently there exists no standard protocol to acquire an Attribute Certificate. LDAP could be used, but no LDAP schema to allow retrieval of Attribute Certificate has been written up to now. Until such a protocol is defined and implemented, it is unlikely that ACs will commonly be used. Recently (March 2002) two proposals have been made to the PKIX WG:

- Attribute Certificate Request Message Format <draft-ietf-pkix-acrmf-01.txt>
- Attribute Certificate Management Messages over CMS <draft-ietf-pkix-acmc-01.txt>

11.5 Attribute delegation management

An attribute may be delegated during some period of time to another individual. When performing the delegation, the subscriber shall indicate that period of time and nominate the delegate by specify an unambiguous link to the certificate of that person.

In addition the subscriber may wish to restrict the use of the attribute so that it can only be used with some signature policies or/and commitment types.

Finally, the person receiving the delegation shall be informed of the way to acquire the single or multiple attributes certificates.

When delegation is supported, the AA shall indicate in an "AC Practice Statement" how AC can be delegated and acquired. Additional protocols or additional parameters to protocols may be necessary to support these features.

12 Recommendations

12.1 Requirements for Attribute Certificate Policies

Whereas a PKC is always issued under a fixed set of Certificate Policies, every AC can be issued under a different Attribute Certificate Policy. So the same AA can support multiple policies but shall make sure that every grouping of attributes is done under a single coherent set of Attribute Certificate Policies.

12.1.1 Requirements for ACAs

The Attribute Certification Authority is liable for the accuracy of the attributes when they are initially registered. If it is a Qualified Certificate issuer it is legally required binding. It is up to the Attribute Certification Authority to choose how to ascertain the attribute accuracy for which it will be liable. In any case, the Attribute Certification Authority must keep a copy of the official information the ACA collected in this process.

For a CA, that will include the attribute in an PKC, the duration during which the attribute is no longer verified is indicated in the PKC (it is the PKC validity period).

The Attribute Certification Authority shall specify in the Attribute Certification Practise Statement the details of the official information and practices upon which the attributes have been issued.

If the same authority acts both as an ACA and as an AIA, its ACA function must have deep skill in ICT and more specifically in PKI and/or PMI operation and management. Moreover, the ACA function should be supported on by a department separate from the AIA function, in order to achieve the necessary separation of duties.

The ACA should not engage itself in activities which could compromise its impartiality.

For any attribute, whether it is handled by a PKC or an AA, the ACA shall specify:

a) the description of the attribute in readily-understandable terms, and where appropriate the law that defines the attribute (e.g. CEO has been established in article xx of law nnn of 19yy);

b) how the attribute will be represented (e.g. a character string and/or an OID);

c) whether the attribute is certified by the authoritative source (i.e. the Attribute Issuing Authority) or is only verified. In the latter case, which documents the subject must exhibit to prove his/her right to have the attribute certified, the procedures used for the verification and the ACA's commitment to result;

d) whether the attribute can be publicly available or is restricted (and the extent of the restriction). Consistently with the Directive [3] annex II letter l) provisions quoted in clause 6, it is of primary importance that a CA makes sure whether or not the subscriber agrees to publish the certificate with these attributes included;

e) how the attribute will be provided, i.e. in a PKC or in an AC.

12.1.2 Requirements for AAs

Any kind of attribute (life lasting, long lasting, short lasting) may be included in an AC.

An AA is liable for the accuracy of the attributes when they are initially registered. The AA shall indicate whether it handles revocation or not. If handled, it may simply continue to certify the attribute, i.e. accept to re-issue an AC that contains that attribute, unless a specific revocation for that attribute is received.

The AA may also choose to subsequently check attributes for their continued accuracy. In such a case, during the whole attribute certification period, a confirmation will be performed subsequently and, if applicable, at some regular time interval (i.e. by making periodic verifications), otherwise the attribute will no longer be certifiable. Subsequent verifications are not necessarily directly done by the AA, but, can be delegated. At the time of registration, the individuals or the authorities able to ask for the confirmation or for the revocation of the attribute should be nominated.

The AA shall indicate for every AC that is issued which of these three following alternatives it follows:

a) attribute checking at initial registration only, with no revocation support,

b) attribute checking at initial registration only, with revocation support,

c) subsequent attribute checking, with revocation support and, where applicable, a time period for the check.

For any attribute, when it is handled by an AA, the AA shall specify in the ACPS, when applicable:

1) the attribute certification period;

2) the possible validity periods of ACs containing this attribute. The attribute certificate validity period can be equal or shorter than the attribute certification period, while managing revocation status information, or may be much shorter than its attribute certification period, e.g. by periodically renewing the attribute certificate without the need to manage the revocation status information;

3) the support or the non support of attribute revocation. When revocation is supported, the revocation conditions and the rules for revocation;

4) whether this attribute can be obtained with other attributes in an attribute subset. When this is the case, how attribute subsets may be obtained. For example, it may be defined by the end-user or by the ACA. In the former case, ways to see all the attributes and to group them by assigning attribute set names should be made available to the end-user. In the later case, the end-user must have ways to see all the attribute set names and the attributes that correspond to these sets;

5) whether the attribute can be delegated. When this is the case, the name of the delegating person shall be traceable and the means to trace it shall be indicated (e.g. in an audit trail or in the certificate). It shall be indicated if some restrictions, like applicable signature policies, apply to the delegation.

An Attribute Authority should inform its subscribers and relying parties about the need to use applications that check both the AC to be used and the associated PKC are valid (i.e. they are neither expired nor revoked).

12.2 Definition of cross-European roles

It would be adequate to conduct a study about the equivalence of some "useful" attributes, that have an equivalence among all the European countries.

When a character string is being used, that string is language dependent and may only be easily understandable in one country. While this is certainly useful, this does not allow an easy recognition by humans among all the EU countries. In many cases, attributes in one country have an equivalence in another country. For example, a CEO is a well understood position within a company and may have some equivalence in each of the EU countries. Some documents need to be signed by a CEO and therefore an easy recognition of this position would be beneficial.

12.3 Attribute Certificate Profile for Electronic Signatures

IETF RFC 3281 [8] specifies an Internet Attribute Certificate Profile for Authorization. This means that this RFC is targeted to be used in the context of an access control service and not in the context of non repudiation nor data origin authentication services. In the previous clauses several enhancements to this certificate profile have been identified and the goal of this clause is to summarize the findings.

1) There is a need to define an "Attribute Certificate Policies Extension". Attributes inserted in a certificate are verified at the time of the initial registration of the attribute for a given end-entity. Unless a specific revocation request is received and granted by the ACA, attributes will continue to be certified. However, ACAs may choose to regularly verify some attributes so that relying parties may be more confident about their association with the end-entity. This information may be made available directly in a certificate through a policy qualifier.

   When a relying party receives a certificate, it may be useful to avoid to forward the certificate itself and to pass only a reference of the certificate together with a location where the certificate is stored. In some cases the ACA may provide the information on whether it is a private publication or not. If that information is present in the certificate then it can be extracted and forwarded to another relying party. This information could be made available directly in a certificate through policy qualifiers or specific extensions.

2) An unambiguous link between an AC and a PKC can, more or less, be done today by specify the CA name and the serial number of a certificate (i.e. using the baseCertificateID option). It should be noted that the CA name can be ambiguous. Anyway, the use of the serial number does not allow the life time of the Attribute Certificate to last longer than the validity period of the PKC. It would be advantageous to consider stable links with an entity that would be independent from a certificate but linked to a certificate content. There exists various alternatives to keep the life time of the Attribute Certificate independent from the validity period of the PKC, as long as the PKC is renewed:

   - using a subject DN (either placed in the subject field or in the subjectAltName) associated with an ambiguous CA name, i.e. the name of the CA together with all the names of the CAs from the hierarchy. This could be provided by profiling the **`entityName`** field so that he could include two fields;

   - using the Permanent Identifier recently defined in a PKIX draft.

3) The Role syntax has been correctly defined in X.509 and is the single attribute defined there. Additional attributes have been defined in IETF RFC 3281 [8], but unfortunately their structure is not copied from the RoleSyntax structure. The RoleSyntax is constructed in the following way:

```
RoleSyntax ::= SEQUENCE {
                roleAuthority   [0] GeneralNames OPTIONAL,
                roleName        [1] GeneralName
```

The first element which is optional allows to define the issuing authority for the role. This allows to make a difference between the issuing authority for the role and the Attribute Authority which may only have verified the attribute value delivered by the role Issuing Authority. Furthermore the restriction made by IETF RFC 3281 [8], to only allow a URI to be included as a role appears to be too restrictive.

1) In the case of a delegation of signature, there is a need to define a "restrictions extension" allowing to restrict the use of the attributes to specific signature policies and/or specific commitment types.

2) In the case of a delegation of signature, there is a need to define a "delegating person extension" allowing to identify the delegating person for audit purposes. This field would include either a reference to a certificate from the delegating person or both the subject and the issuer DNs.

These various arguments indicate that there would be a need to draft a new document called: "Attribute Certificate Profile for Electronic Signatures".

12.4 Attribute Certificate Acquisition Protocol

There are two kinds of protocols to consider whether the Attribute Certificates are produced upon request or directly by the Attribute Authority.

When Attribute Certificates are produced upon request, then they are returned to the requestor and a reference to these Attribute Certificates can be used to fetch them later on from some repository, e.g. using LDAP with an appropriate schema.

When Attribute Certificates are produced directly by an Attribute Authority and placed in a repository, then they can be fetched from that repository using LDAP and an appropriate schema. Such a schema has recently be proposed to the PKIX WG: LDAP Schema and Syntaxes for PMIs <draft-ietf-pkix-ldap-pmi-schema-00.txt>.

It should be noticed again that placing Attribute Certificates in a repository may lead to privacy issues unless an access control service is being enforced.

12.5 Criteria for using PKCs or ACs

Non-public attributes should only be included in ACs.

For the reasons set forth in clause 8, life/long lasting attributes are preferably to be included in PKCs while short lasting attributes should be included in ACs:

- If the attribute does not expire before the related PKC, the attribute may be included in the PKC.
- If the attribute expires before the related PKC, the attribute should not be included in the PKC, but placed in an AC.

An ACA is bound to verify attributes inserted in a PKC only at the time the PKC is issued, it is not required to take any commitment on subsequent verifications. When it is desirable to check for the continued accuracy of an attribute, then it shall be handled by an ACA under an appropriate policy.

Supporting ACs, means that AAs need to be set up in addition to CAs. Managing AAs, generally speaking, is for sure about as complex to manage as CAs. So it is advisable to implement it only when necessary and, if possible, the least complex possible.

Annex A:
Attribute syntax in ASN.1

Attribute syntax

Although the Attribute syntax is defined in IETF RFC 3280 [5], its definition is repeated here for convenience.

```
Attribute ::= SEQUENCE {
      type      AttributeType,
      values    SET OF AttributeValue
        -- at least one value is required
}

AttributeType ::= OBJECT IDENTIFIER

AttributeValue ::= ANY DEFINED BY AttributeType
```

Group attribute syntax

Although the group attribute syntax is defined in IETF RFC 3281 [8], its definition is repeated here for convenience.

```
The group attribute carries information about group memberships.
      name      id-aca-group
      OID       { id-aca 4 }
      syntax    IetfAttrSyntax
      values:   one Attribute value only;
                multiple values within the IetfAttrSyntax
```

Where the IetfAttrSyntax is defined as follows.

```
IetfAttrSyntax ::= SEQUENCE {
     policyAuthority     [0] GeneralNames    OPTIONAL,
     values         SEQUENCE OF CHOICE {
                    octets    OCTET STRING,
                    oid       OBJECT IDENTIFIER,
                    string    UTF8String
    }
}
```

The IetfAttrSyntax type allows a separation between the AC issuer and the attribute policy authority.

NOTE 1: Using the terminology of the present document, the attribute policy authority is the AIA.

This is useful for situations where a single policy authority (e.g. an organization) allocates attribute values, but where multiple AC issuers are deployed for performance or other reasons. From this text, copied from IETF RFC 3281 [8], the attribute policy authority is an organization that allocates attribute values, whereas the AC issuer is one of the servers managed by that organization.

The syntaxes allowed for values are restricted to OCTET STRING, OBJECT IDENTIFIER, and UTF8String, which significantly reduces the complexity associated with matching more general syntaxes. All multi-valued attributes using this syntax are restricted so that each value MUST use the same choice of value syntax. For example, AC issuers must not use one value with an OID and a second value with a string.

It should be noticed that this restriction does not allow an attribute to include both a character string (UTF8String) and an OID.

Member attribute syntax

Although a member attribute is defined in ITU-T Recommendation X.520 [7], clause 5.10.2, its definition is repeated here for convenience.

The *Member* attribute type specifies a group of names associated with the object.
An attribute value for Member is a distinguished name.

```
member ATTRIBUTE ::= {
   SUBTYPE OF     distinguishedName
   ID             id-at-member }
```

with:

```
id-at-member ::= OBJECT IDENTIFIER {id-at 31}
id-at ID           ::= attributeType
```

while X.501 specifies the OID for attributeType:

```
ID                 ::= OBJECT IDENTIFIER
ds ID              ::= {joint-iso-itu-t ds (5)}
attributeType ID   ::= ds {4}
```

Role attribute syntax

Although the role attribute syntax is defined in X.509 [7] its definition is repeated here for convenience.

The roleAuthority field MAY be used to specify the issuing authority for the role.

```
name      id-at-role
OID       { id-at 72 }
syntax    RoleSyntax
values:   Multiple allowed
```

The syntax used for this attribute is:

```
RoleSyntax ::= SEQUENCE {
         roleAuthority   [0] GeneralNames OPTIONAL,
         roleName        [1] GeneralName
 }
```

The roleAuthority field MAY be used to specify the issuing authority for the role.

NOTE 2: Using the terminology of the present document, the issuing authority indicates the name of the AIA.

IETF RFC 3281 [8] indicates: The roleName field MUST be present, and roleName MUST use the uniformResourceIdentifier CHOICE of the GeneralName. However, that limitation is not present in X.509 and it is doubtful why it should be followed.

Role Occupant attribute syntax

Although the Role Occupant attribute syntax is defined in X.520 [7] its definition is repeated here for convenience

The Role Occupant attribute type specifies the name of an object which fulfills an organizational role.
An attribute value for Role Occupant is a distinguished name.

```
roleOccupant ATTRIBUTE ::= {
SUBTYPE OF  distinguishedName
ID  id-at-roleOccupant }
```

with:

```
id-at-roleOccupant ::= OBJECT IDENTIFIER {id-at 33}
id-at ID           ::= attributeType
```

while X.501 specifies the OID for attributeType:

```
ID                 ::= OBJECT IDENTIFIER
ds ID              ::= {joint-iso-itu-t ds (5)}
attributeType ID   ::= ds {4}
```

Annex B:
Guidelines for the certification of roles in subscription certificates

This annex contains an excerpt from a document produced by the "Funzioni, qualifiche e poteri "(Functions, qualifications, and powers) Assocertificatori Work Group 4. Assocertificatori is a free Association of Certification Authorities officially accredited in Italy.

For a better understanding, an excerpt of the Circular AIPA/CR/24, dictating the technical regulation, has also been added in annex C.

The parts of the original document that are of no interest for the present document, such as references to the Italian Regulation, have been removed. The text that was removed is replaced by the term "OMISSION".

Assocertificatori has granted permission to ETSI to publish the present document as an informative annex to the present document.

This text is provided by ETSI as information only.

Foreword

The Assocertificatori document proposes to use the Description attribute as defined in ITU-T Recommendation X.520 [7], clause 5.5.1. Description is "text which describes the associated object". It is a character string encoded as a DirectoryString.

Since the current proposal only includes one role component, a single role can be included in a public key certificate.

While it is possible to say how to construct Description attribute, its inside components cannot be extracted. However, Substrings Match allows to look for a match inside a DirectoryString.

Looking for a given role can be done, using either "final" [2] or "any" [1] in the SubstringAssertion (see clause 6.1.3 from ITU-T Recommendation X.520 [7]).

This means that it is not possible to extract the role, but if an application is expecting a given role, it is possible to know whether that role is included in the Description.

While the "Description" attribute is currently supported in the Distinguished Name, this attribute that includes the role specification might move in the subjectDirectoryAttributes extension, as explained in Assocertificatori document clause 4.1.5.

ASSOCERTIFICATORI

GUIDELINES FOR THE CERTIFICATION OF ROLES IN SUBSCRIPTION CERTIFICATES

Foreword

The present document provides the guidelines for the certification of roles within a subscription certificate and provides a solution that enables the digital signature mechanism to manage the presence of the holder's professional qualifications, public-type duties, or powers conferred by third-parties, which can be pictured within the principle of private and public law representation.

Summary

1 Introduction

Chapter 2 includes definitions of terms used in the present document, unless defined otherwise.

Chapter 3 (partly removed) includes references to the Italian and European Regulations that provide for and regulate the capability of the holder of a subscription certificate to specify his/her role.

Chapter 4 includes the technical specifications of the solution, which are binding on the Certification Authorities adhering to the solution. In consists on the one hand of the definition of the content of the certificate, on the other hand of the specification of the Unique Role Table and of its update procedures (partly removed from the document).

Chapter 5 includes hints and recommendations to Certification Authorities on the matters of liability and content of the Practice Statements.

Chapter 6 illustrates the relations between the Certification Authorities adhering to the solution, the relations with the Certification Authorities members of the association not adhering to the solution for the time being, the relations with the Certification Authorities that are not members of the association, and the relations with third-parties.

Appendix A contains examples of the indication of the role in a certificate drawn up according to the technical specifications provided in the present document.

Appendix B contains the initial version of the Unique Role Table.

Appendix C contains for a better understanding, an excerpt of the Circular AIPA/CR/24, dictating the technical regulation, has also been added.

2 Definitions

Adhering Certification Authorities (ACA): Certification Authorities members of Assocertificatori that adhere to the solution for the certification of roles, and the RUPA (Rete Unitaria della Pubblica Amministrazione, Unitary Public Administration Network) Technical Center

professional association: expression indicates the professional order, college, or any other organization qualified for certifying the subscription to their rolls, lists, or other registers, by a subject that performs a specific professional activity

public registers: public registers where the registration of deeds or events related to juridical or physical persons for the purpose of constitutions, statements, or publications is compulsory

representation: all forms of representation, both public and private, as well as voluntary, organic, or legal

role: both the title of representation powers and the possession of professional qualifications.

third-party involved: physical or juridical person or other entitled subject that testifies with his/her consent the existence of powers of representation or professional titles or a specific function of the certificate holder

3 Regulative references

The Italian and Community Regulations explicitly provide for the capability of a subject (physical person) to obtain a subscription certificate, indicating the role which he/she intends to act using the digital signature.

Article 2, Paragraph 3 of the 99/93/CE Directive alludes to the powers of representation by defining the signatory as the *"… person who detains a purview for the creation of a signature and acts on his/her own behalf or on behalf of the physical or juridical person or entity that he/she represents"*.

In general however we must emphasize that the regulation governing the matter is not complete and much space is left to Practice Statements).

Whatever is provided for on this matter by the general legal system and in particular the civil code and the special laws must be taken into account. Therefor the information related to the roles contained in the certificates is classified as follows:

1) (Voluntary and legal) representation of a physical person.

2) Representation of a juridical person and of other private law bodies.

3) Exercise of public duties, both in representation of Bodies and Offices of the Public Administration, and exercise of delegated public duties.

4 Role certification

4.1 Role certificate profile

4.1.1 Role Location and Structure

The role attributes are inserted in the Role (R) sub-field of the Description field in the part of the certificate reserved to the Subject.

The R field consists of the following parts:

- Brief and accurate description in natural language of the role of the holder.
- Numeric code that facilitates the use of automatic procedures.

Field R is structured as follows: R=<Description in natural language >:< numeric code>

- The colon (:) symbol is used as a separator between the description and the code.
- The role attributes are inserted in public-type certificates on the holder's demand and in this case the description in natural language and the numeric code must also be inserted.
- The description and the corresponding code can be found in the Unique Role Table provided by Assocertificatori and described in clause 4.2 of the present document.

4.1.2 Description in Natural Language

The description in natural language of the role to be inserted in the certificate must perfectly match the one contained in the Unique Role Table and must be associated with the numeric code.

If the Unique Table should not contain the role in question, the Certification Authority can insert a description in natural language free in content without any numeric code, without prejudice to the capability of activating the update procedure described in clause 4.3.

In this case whatever the applicant declares, based on the indications contained in the document issued by the third-party involved to support the role, should be thoroughly copied without using truncated or abbreviated descriptions.

4.1.3 Numeric Code

The role codes associated with the descriptions in natural language are include in the Unique Role Table, and are common and standard for all the Certification Authority members.

The format of the numeric code makes use of dots, following the structure of the current OID's, and must not exceed 16 characters in length (including the dots), while the number of sub-fields and of characters per sub-field is free.

When needed, the code is organized according to a hierarchical structure reflecting the structure, to which the certificate holder belongs.

The initial code field contains one of the digits from 1 to 4 in compliance with the distinction of roles described in clause 3, i.e.:

1) Representation of physical persons.

2) Representation of private law bodies.

3) Exercise of public offices and duties.

4) Professional qualifications

4.1.4 Organization, Organization Unit, and Locality Fields

The insertion of a role implies inserting the data related to the third-party involved.

The Organization (O), Organization Unit (OU) attributes and, as far as geographic information is concerned, the Locality attribute are used for this purpose, according to the procedures described below.

The information related to the represented subject, which is inserted in the attributes described above, must be drawn exclusively from the act of consent of the third-party involved and/or from the certifications sent in by the applicant for the insertion of the role.

The hierarchical structure of the O and OU fields allows reproducing a first detail of the organizational structure of the body specified in them.

A value must always be given to the Organization attribute whenever the role of the holder is specified. It must contain the data that identifies the third-party involved (physical, juridical person or other body) including the fiscal code, according to the following syntax:

- O=Name/Surname/Fiscal Code [for physical persons].
- O=Body Name/Fiscal Code [for juridical persons and other bodies].

The Organization Unit attribute is optionally given a value to provide information in natural language in addition to the information already provided in the Organization attribute, in particular the data related to the structure of the organization represented by the holder (e.g. organizational unit, department, division, etc.).

In this case the information contained in R must be firstly associated with OU that in turn must be connected with O.

Two procedures are available for the use of the OU field:

1) Use of a single OU: any structured information is separated by the slash (/) character.

2) Use of multiple OU extensions.

The application programs that verify the signature must be capable of processing both formats.

Giving the Locality attribute a value in addition to O and OU is optional and serves to provide geographic indications related to the body specified in the Organization field, if this should become necessary for the purpose of defining the role of the holder.

The field provides information on the site or location of the body specified in the Organization attribute and contains a six-digit numeric code consisting of the Province Code (first 2 characters) and the Municipality Code used by the Tax Registry Office (4 characters). For example, a location in the Municipality of Monza is identified by MIF704.

The application programs for signing and verifying must be capable of displaying the information contained in O and eventually in OU and in Locality, in order not to create ambiguities in the interpretation, in particular clearly highlighting the essential data of the holder of the certificate, and of the subject represented.

The value to be given to the Organization, Organizational Unit Name, and Locality attributes and the association of the role with the certificate must be specified in the Practice Statements, when the indication of the role is specified in the certificate.

4.1.5 Relations with the Qualified Certificate

The solution is compatible with the new standard qualified certificate profile described in IETF RFC 3039 [6], and introduced in the Italian system owing to the acknowledgement of the 1999/93/CE Directive.

Therefor the suggested proposal can be used with the identical descriptions of roles and numeric codes, by inserting the same content of field R in the subjectDirectoryAttribute extension, when the migration to this new certificate becomes necessary.

Fields O, OU, and Locality in the qualified certificate serve exactly the same purpose already defined in clause 4.1.4.

4.2 Unique role table

The descriptions in natural language, the numeric codes, and the table where they are inserted are created and managed by Assocertificatori through a special Committee (Role Committee).

The file of the table is written in text format (ASCII) and presents on the first line an increasing serial number indicating the version and the date.

Starting from the next line the table shows the description in natural language in the first column and the numeric code in the second.

The table can be updated only by adding descriptions and codes for new roles, while the existing descriptions and codes are kept even when they become useless.

The association is in charge of making the text file available on an Internet site, once it is subscribed with a digital signature and time-stamped, both for the purpose of distributing it to the adhering Certification Authorities and for publicizing it for the holders and the third-parties.

4.3 Table update procedure

The Role Table update procedure must be managed by a Restricted Committee in charge of evaluating requests for the definitions of the roles and of defining the roles. Since this task is essentially of a legal nature, the following composition of the Committee was agreed:

- Assocertificatori Director, acting as a guarantee on behalf of the missing Certification Authorities;
- 1 jurist (+ 1 substitute) from the Notaries;
- 1 jurist (+ 1 substitute) from the Assocertificatori Management Committee;
- 1 jurist (+ 1 substitute) from the Public Administration (RUPA Technical Center).

The Committee will exploit electronic communication procedures (electronic mail, mailing list, and newsgroup) to execute the evaluation procedures.

When the Restricted Committee receives requests of particular relevance, it must notify the Assocertificatori Director, who must in turn call a meeting extended to the members of the Role Committee to perform an in-depth evaluation.

The Restricted Committee takes its decisions with the valid vote of 2 jurist components.

5 Organizational processes

5.1 Certification authority's liability

5.1.1 Foreword

The Italian Regulation outlines the level of liability that a Certification Authority, which does not comply with the identification and specification obligations of powers of representation, must take.

The combined dispositions of the articles in the Italian Regulation assign the Certification Authority a first principle of liability, if he/she omits verifying the powers of representation, offices held, titles or professional qualifications, or does it incorrectly.

This liability however has two main limitations.

In fact firstly the Certification Authority is allowed to prove that he/she issued the certificate without wrong, so the liability is limited to the cases when the Certification Authority did not behave using the proper care and skill.

Secondly the correctness of the information contained in the certificate is verified only when the certificate is issued, therefor, guaranteeing the availability of the information contained in it even after its date of issue, would constitute a service "with a greater added value" by the Certification Authority, which is not imposed by law and could require enforcing specific contractual clauses for the limitation of liability - for want of specific provisions.

5.1.2 Procedures for the Verification of the Existence of Powers, Offices, or Professional Qualifications

The procedures for the verification of the existence of the powers, offices, or professional qualifications under examination that a Certification Authority must follow, not to incur into liabilities towards third-parties, vary depending on the type of powers or duties or qualifications to be verified, with the understanding that a certificate containing "additional" indications based on mere statements by the holder is a potential source of liability for the Certification Authority, if he/she fails to verify the specific characteristics of the person to whom the certificate is issued.

In brief:

a) Roles resulting from public registers (different from the powers of representation)

   In all cases when the additional information related to the holder comes from public registers, for instance when the holder belongs to professional orders, the verification must be performed controlling the registers or the evidences provided by them. This must necessarily be done when the certificate is issued.

b) Powers of representation resulting from public registers

   In these cases, such as in the representation of enterprises, the public registers must be verified with the additional control that the represented subject gave his/her consent, if applicable. In this case whoever receives and verifies the certificate can legitimately rely on the existence of the power of representation for the specific deed for which the certificate is used.

c) Voluntary powers of representation

   In this case the Certification Authority is simply required to verify the existence of the consent of the represented subject carefully.

d) Indications "with a greater added value"

If the Certification Authority performs a service with a greater added value, which includes a guarantee that the information is correct and updated even during the period after the certificate was issued, the Certification Authority takes particular levels of liability since the services must be regulated by an agreement. In this case each Certification Authority has the possibility of specifying the type of guarantee it provides on the "additional" information or the lack of any guarantee (e.g. "as is"), the sources and verification of the information, as well as of establishing with an agreement any limitations of liability, without prejudice to the validity limits established by article 1229 C.C. for such a clause (invalidity of exclusions or limitations of liability in case of fraud or serious wrong).

In such cases special agreements should be entered with the subjects that provide or verify the information, since it would be rather difficult for the Certification Authority to follow all the changes of offices or titles or professional qualifications directly in the period after the certificate is issued.

5.1.3 Annulment or termination of powers

The matters treated so far have important effects in case the titles or professional qualifications, offices, or powers of representation fail.

As far as titles and offices are concerned, the Certification Authority must extend its verification until their validity terminates (only) if the Certification Authority guaranteed the correctness of the information even in the period after the certificate was issued.

The same problem ensues as far as powers of representation are concerned, for which the Certification Authority is normally not obliged to perform the same constant control, unless it undertakes to do so.

In fact, the powers of representation subsist in all cases towards the third-party until the represented subject annuls the representation. The simple fact that no annulment is notified to the Certification Authority is a good reason to presume that the powers still exist.

Instead the Certification Authority is held liable for not immediately notifying the annulment of the powers immediately, once it is communicated by the represented subject.

5.2 Practice statements

The present clause includes hints and recommendations to define the proper procedures in the Practice Statements for the insertion of the role, with the purpose of guaranteeing a certain level of interoperability also between the organizational procedures, and to limit the liability of the Certification Authority within reasonable limits.

The Practice Statements should regulate the following points:

a) The registration procedures in the holder's Registration Phase, whether they are performed online or during the identification phase:

- If the procedure is online, the application program must process it according to the technical solution. The program must also include a note informing applicants that all roles are subject to verification during the identification phase and that the description of the role in natural language and of the numeric code will be assigned by the employee in charge of identification, since the selection performed in that phase may be merely indicative and is subject to the requirements that the code must be available and the it is proper to assign that code rather than another.

b) The Identification Phase should regulate:

- The procedure for the submission of the documentation supporting the representation, which must be available both on paper and in electronic form, in concurrent or alternative mode, and in compliance with the provision by the regulation that the Certification Authority must keep the documentation for 10 years.

- The type of documents supporting the roles requested by the Certification Authority, which are suitable to guarantee the title of the role with reasonable certainty.

- The period of validity of the supporting documentation requested for the roles, which however should not be prior to 30 days from the request for identification. Further controls by the Certification Authority, if the supporting documentation is dated earlier than a given date, or the faculty of performing further controls whenever required by the circumstances, can be arranged.

c) The following steps should be performed in the Role and Code Attribution Phase:

- Decide who should indicate the code, whether the Certification Authority or the applicant, distinguishing between the cases when a single certificate is requested and when a whole structure (public or private body) requests certificates for its employees.
- Regulate the procedures and schedules for requests of synonyms or of roles not included in the table.
- Regulate the activation of the table update procedure for non-existent roles.
- Regulate the role evaluation process, the liability for making the choice, and any inconsistencies.
- Regulate the period of validity of the certificate in relation to the period of validity of the powers.
- Exclude the possibility of issuing the certificate to juridical persons, since the juridical and regulative scenario is ambiguous and the (IETF RFC 3039 [6]) standard techniques exclude this possibility.

6 Dissemination of the solution

6.1 Relations between certification authority members

6.1.1 Adoption of the Solution

Assocertificatori is an association according to Articles 36 and following of the civil code, therefor the relations between its members are regulated by the law or by the memorandum of association.

The list of activities that Assocertificatori can perform to achieve the object of the association shows that one of its main institutional activities and of the purposes of its members is to define common standards to promote specific behaviors of and between Certification Authorities.

The present proposal produced by the "Gruppo Funzioni, qualifiche e poteri" represents an interoperability standard between Certification Authorities and is binding on them, once it is approved with a resolution of the assembly. The result is that each member is obliged to put the resolution into effect and not to behave incompatibly with the object of the association and its statutory principles.

After all, the approval by the Assocertificatori assembly of the solution recommended by the "Gruppo Funzioni, qualifiche e poteri" represents an interoperability standard intended to facilitate mutual collaboration in the relations between Certification Authorities.

Of course the approval of the present document does not necessarily oblige the Certification Authority members to insert the indications on the roles in their certificates. However, when they decide to include those indications in the services they offer, they must adopt and comply with the standards approved by the association on the matter, in accordance with the integration of the contractual relations established through a resolution by the assembly.

Furthermore the association members must refrain from promoting the adoption of standards alternative to the solution approved by Assocertificatori, and they must in all cases make their applications compliant with the approved solution, in order to be capable of accepting certificates issued by other Certification Authorities and containing the indications.

The special procedure allows all Certification Authorities to request modifications and integrations to the code table.

6.1.2 Interoperability Test

In order to comply with the requirement for interoperability that is one of the Association's main purposes, the members undertake to prearrange technical and organizational solutions enabling whoever performs the verification to display the structured certificate correctly according to the profile outlined in clause 4.1.

6.2 Relations with certification authority non-members

6.2.1 Private Certification Authorities

The Certification Authorities that are not members of the association cannot be prevented from implementing the standards developed and publicized by Assocertificatori, since they are of common and public interest. They actually retain the possibility of adopting the recommended solution. Naturally the Certification Authorities that are not members of the association cannot be obliged to adopt the standards, since they are not subject to the contractual obligations established by the memorandum of association.

The Certification Authorities that are not members of the association may also request modifications and integrations to the Role Table. The Table is updated by the members using the special procedure.

6.2.2 RUPA Technical Center

The certification of roles is of particular interest within e-government, in particular due to the capability of implementing application software for the digital signature extended verification. The application programs could exploit the signatory's role code to verify the validity of the signature in terms of its lawfulness on public deeds in digital format, in addition to the current common verifications of the validity of the signature in terms of data integrity and data origin authentication of the signed document (good cryptographic quality of the signature, period of validity, and lack of annulment of the certificate by the signatory, compliance with the verification scheme by the issuing Certification Authority).

6.3 Assocertificatori relations with third-parties

The above considerations on the Certification Authorities that are not members apply also to third-parties, such as digital signature application developers. In particular these subjects must also be allowed to access the Role Table and its instructions and any information required to develop the recommended solution for the insertion of the role indication in certificates.

Appendix A:
Examples of role indications

Comments are enclosed within square brackets. For the sake of simplicity the terms "representation" and "represented subject" are used also to indicate cases of organic belonging, or of enrolments in professional associations.

NOTE: Please refer to annex 1 for the format and content of the Common Name and Description sub-fields of the Subject field.

1) REPRESENTATION OF PHYSICAL PERSONS

The holder is: Mario Rossi [e.g. guardian]
The represented subject is: Giuseppe Verdi [e.g. a minor]

SUBJECT:
State: IT
Organization: VERDI/GIUSEPPE/VRDGSP91A01H501V
Organization Unit: [in general this field does not seem to require a value]
Locality: [in general this field does not seem to require a value]
Common Name: ROSSI/MARIO/RSSMRO60C01H501D
Description: C=Rossi/N=Mario/D=01-03-1960/R=Guardian:1.2.1.1

2.1) REPRESENTATION OF JURIDICAL PERSONS (mode 1)

The holder is: Mario Rossi [e.g. Purchase Division Director of the Alfa SpA Office in Milan, with registered office in Rome]
The represented subject is: Alfa SpA, with registered office in Rome

SUBJECT:
State: IT
Organization: ALFA SPA/01234567890
Organization Unit: Milan Office/Purchase Division
Locality: RMH501
Common Name: ROSSI/MARIO/RSSMRO60C01H501D
Description: C=Rossi/N=Mario/D=01-03-1960/R=Director:2.10.3.1

2.2) REPRESENTATION OF JURIDICAL PERSONS (mode 2)

The holder is: Mario Rossi [e.g. Purchase Division Director of the Alfa SpA Office in Milan, with registered office in Rome]
The represented subject is: Alfa SpA, with registered office in Rome

SUBJECT:
State: IT
Organization: ALFA SPA/01234567890
Organization Unit: Milan Office
Organization Unit: Purchase Division
Locality: RMH501
Common Name: ROSSI/MARIO/RSSMRO60C01H501D
Description: C=Rossi/N=Mario/D=01-03-1960/R=Director:2.10.3.1

3.1) REPRESENTATION OF PUBLIC BODIES (mode 1)

The holder is: Mario Rossi [e.g. Legal Office Director of the Tax Policies Department of the Ministry of Economy and Finances]
The represented subject is: Ministry of Economy and Finances, with registered office in Rome

SUBJECT:
State: IT
Organization: MINISTRY OF ECONOMY AND FINANCES/01234567890
Organization Unit: Department of Tax Policies/Registered Office
Locality: RMH501
Common Name: ROSSI/MARIO/RSSMRO60C01H501D
Description: C=Rossi/N=Mario/D=01-03-1960/R=Director:3.3.4.1.2.4.

3.2) REPRESENTATION OF PUBLIC BODIES (mode 2)

The holder is: Mario Rossi [e.g. Legal Office Director of the Tax Policies Department of the Ministry of Economy and Finances]
The represented subject is: Ministry of Economy and Finances, with registered office in Rome.

SUBJECT:
State: IT
Organization: MINISTRY OF ECONOMY AND FINANCES/01234567890
Organization Unit: Department of Tax Policies
Organization Unit: Legal Office
Locality: RMH501
Common Name: ROSSI/MARIO/RSSMRO60C01H501D
Description: C=Rossi/N=Mario/D=01-03-1960/R=Director:3.3.4.1.2.4.1

4) PROFESSIONAL QUALIFICATIONS

The holder is Mario Rossi [e.g. Engineer]
The represented subject is the Association of Engineers of Rome

SUBJECT
State: IT
Organization: ASSOCIATION OF ENGINEERS OF ROME/01234567890
Organization Unit: [in general this field does not seem to require a value]
Locality: RMH501
Common Name: ROSSI/MARIO/RSSMRO60C01H501D
Description: C=Rossi/N=Mario/D=01-03-1960/R=Engineer:4.18

Appendix B:
Unique role table

FOREWARD

The present appendix contains the Role Table and the numeric codes currently defined for:

- Individual entrepreneurs and holders of roles related to private law bodies
- Exercise of public offices and duties
- Holders of professional qualifications.

Individual Entrepreneurs and Holders of Roles Related to Private Law Bodies

The following is a list of private law bodies:

- Associations (acknowledged and not acknowledged);
- Foundations;
- Committees;
- Partnerships (non-stock companies);
- Stock companies;
- Consortia;
- Other bodies entered in public registers.

The numeric code has a hierarchical structure in compliance with the directives indicated in clause 4.1.3 of the present document. The first to levels are described in the scheme below. The third level is a detail of the second, and the fourth level is the role.

CODE (first 2 levels)	MEANING
2.1	Associations
2.2.	Foundations
2.3	Committees
2.4	Individual Entrepreneur
2.5	Commercial Companies
2.6	Consortia
2.7	Other registered bodies
2.8	Other Company organs
2.9	Crisis of the enterprise
2.10	Other subjects provided with representations

Exercise of Public Offices and Duties

Since each government body decides the individual professional roles it institutes for the implementation of its duties, the numeric codes must have a hierarchical structure.

Professional Qualifications

This refers to professional qualifications subject to particular legislative rules and related to professional rolls and special rolls.

DEFINITIONS AND CODES

NOTE: The insertion of the complete list would be cumbersome and of little use for the purposes of TR 102 044, therefor only a few items are included as examples.

INDIVIDUAL ENTREPRENEURS AND ROLES RELATED TO PRIVATE BODIES	
President of an association	2.1.1.1
Administrator of an association	2.1.1.2
Legal representative of an association	2.1.1.3
Foundation President	2.2.1.1
Foundation Administrator	2.2.1.2
EXERCISE OF PUBLIC OFFICES AND DUTIES	
President of the Republic	3.1.1.1
President of the Senate	3.1.2.1
Senator	3.1.2.2
President of the Chamber of Deputies	3.1.3.1
Deputy	3.1.3.2
PROFESSIONAL QUALIFICATIONSI	
Stockbroker	4.1
Agronomist	4.2
Architect	4.3
Social Worker	4.4
Registrar	4.5
Lawyer	4.6

Appendix C:
Subject Field Common Name and Description Sub-fields

Excerpt from **19 June 2000 CIRCULAR, No.** ***AIPA/CR/24***

… OMISSION …

…the following mandatory sub-fields have been included in the Subject field:

Common Name (object ID = 2.5.4.3)

Description (object ID = 2.5.4.13).

The value and structure of the sub-fields are specified below.

a) Common Name = <surname>/<given name>/<Subject Fiscal Code>/<Subject Unique Identifier with CA's>.

Angle brackets specify non-terminal fields. The slash (/) character is used as field separator.

All four fields must be coded using the PrintableString character set.

… OMISSION …

The information related to the Subject role, which allows the same Subject to own different certificates issued by the same Certification Authority (article 22, Section 3 DPCM 8 February 1999), may be stored in the Description field (specified below).

EXAMPLE: Common Name = <Rossi/Mario/RSSMRA60D02F22OM/XYZ123456>

b) Description = "C="<extended surname>"/N="<extended given name>"/D="<date of birth>["/R="<subject's role>].

Therefore the value in the Description field consists of the link of four tagged fields, regardless of their order. Tags to be used are highlighted in bold. The four fields must comply with the following rules:

<extended surname> this is the Subject's full surname, multiple surnames can be used, if needed (e.g. <Battistotti Sassi>)

<extended given name> this is the Subject's full given name, multiple given names can be used, if needed (e.g. <Carlo Maria>)

<date of birth> in the format: <DD-MM-YYYY>; leading zeroes can be used, if needed

<subject's role> this is the only optional field: since it is available for specific applications, no rules are provided for its format.

The string resulting from the link of the four fields may be BMPString coded, when the original surname and given name contain special national characters (e.g. in case of French, Spanish, German, etc. names).

EXAMPLE: description = <C Großmann = /N=Günther/D=03-11-1947/R=General Manager>.

Annex C: Bibliography

Study on "Requirements for CSPs issuing Attribute Certificates" - Final Report - 18th September 2000 - Thomas Hueske, Christian Tobias.

History

Document history		
V1.1.1	December 2002	Publication