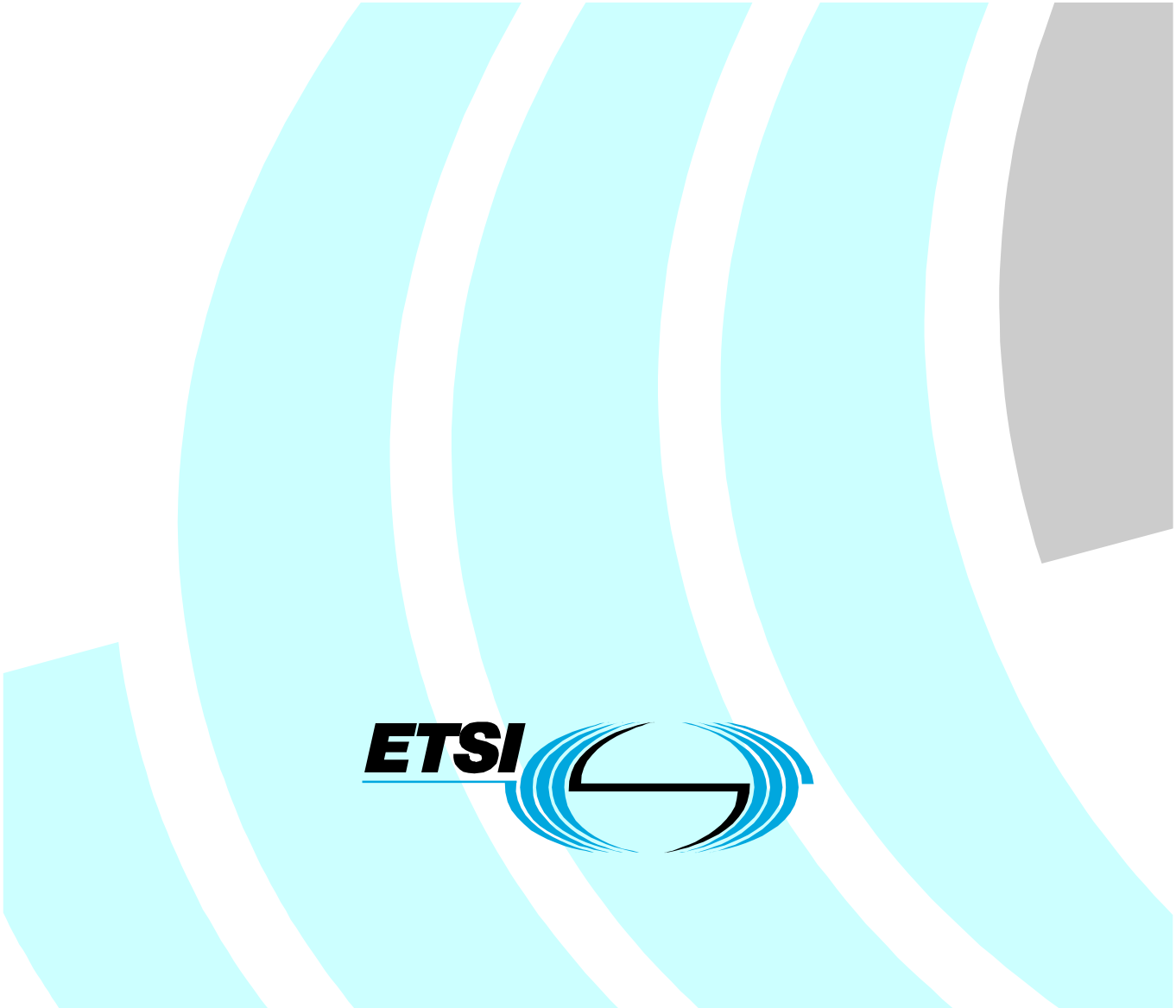
ETSI TS 102 158 V1.1.1 (2003-10)

Technical Specification

Electronic Signatures and Infrastructures (ESI); Policy requirements for Certification Service Providers issuing attribute certificates usable with Qualified certificates



Reference
DTS/ESI-000012

Keywords
e-commerce, electronic signature, IP, 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

Important notice

Individual copies of the present document can be downloaded from:
http://www.etsi.org

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
http://portal.etsi.org/tb/status/status.asp

If you find errors in the present document, send your comment to:
editor@etsi.org

Copyright Notification

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://webapp.etsi.org/IPR/home.asp).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

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

Introduction

Electronic commerce is emerging as a way of doing business and communicating across public and private networks.

Directive 1999/93/EC [1] of the European Parliament and of the Council on a Community framework for electronic signatures [1] does not explicitly cover the use of attribute certificates, since it only mentions the possibility to include attributes in Public Key Certificates (PKCs) (see Annex I, clause d) which refers to the "provision for a specific attribute of the signatory to be included if relevant, depending on the purpose for which the certificate is intended".

An important requirement of electronic commerce is the ability to identify, not only the originator of electronic information in the same way that documents are signed using a hand-written signature, but also their attribute(s), e.g. their role(s) in an organization. This may be achieved using certification services in two ways:

- using attributes included in Public Key Certificates (PKCs);
- using attributes included in Attribute Certificates (ACs).

Only the later case is covered in the present document.

A certification-service-provider issuing Attribute Certificates is called an Attribute Authority (AA). For users of electronic signatures to have confidence in the authenticity of the attributes contained in the electronic signatures they need to have confidence that the AA has properly established procedures and protective measures in order to minimize the operational and financial threats and risks.

The present document specifies baseline policy requirements on the operation and management practices of Attribute Authorities issuing Attribute Certificates that can be used in support of Qualified Electronic Signatures, and thus which are available for use by the public and are linked to a Qualified Certificate supporting the "QCP public + SSCD" Certification Policy.

Attribute Certificates that can be used in such a context can also be used for other reasons, e.g. for authorization. In this respect they may be used in a Privilege Management Infrastructure (PMI).

1 Scope

The present document specifies policy requirements relating to Attribute Authorities (AAs) which are a type of certification-service-providers as defined in Directive 1999/93/EC [1]. The present document specifies policy requirements on the operation and management practices of Attribute Authorities issuing Attribute Certificates such that subscribers, subjects and relying parties may have confidence in the applicability of the Attribute Certificate in support of electronic signatures.

These policy requirements are defined in terms of:

a) the specification of two Attribute Certificate policies for Attribute Certificates issued to the public;

b) a framework for the definition of other Attribute Certificate policies enhancing the above policies or for Attribute Certificates issued to non-public user groups.

The policy assertions relating to the AA include requirements on the provision of services for attribute registration, AC acquisition, AC generation, dissemination, attribute revocation management and AC revocation status. Other certification-service-provider functions are outside the scope of the present document.

These policy requirements are specifically aimed at Attribute Certificates issued to the public, and used in support of qualified electronic signatures (i.e. electronic signatures that are legally equivalent to hand-written signatures in line with article 5.1 of Directive 1999/93/EC [1]). These policy requirements specifically address the requirements for CSPs issuing Attribute Certificates.

Attribute certificates issued under these policy requirements may be used to establish the attributes associated with a natural person who acts on his own behalf or on behalf of another natural person, or legal person it represents.

The present document only addresses the requirements for AAs issuing ACs linked to persons. ACs issued for other purposes are not covered, as these fall outside the scope of Directive 1999/93/EC [1].

The present document may be used by competent independent bodies as the basis for confirming that an AA meets the requirements for issuing Attribute Certificates.

Although the present document is targeted for Attribute Certificates usable for electronic signatures, they could also be used for access control purposes.

It is recommended that subscribers and relying parties consult the attribute certification practice statement of the issuing AA to obtain further information and notice on precisely how a given Attribute Certificate policy is implemented by the particular AA.

The present document does not specify how the requirements identified may be assessed by an independent party, including requirements for information to be made available to such independent assessors, or requirements on such assessors.

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication and/or edition number or version number) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

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

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

[3] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

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

[5] ISO/IEC 15408 (parts 1 to 3): "Information technology - Security techniques - Evaluation criteria for IT security".

[6] CEN Workshop Agreement 14167-2: "Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 2 Cryptographic Module for CSP Signing Operations - Protection Profile (MCSO-PP)".

[7] Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts.

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

[9] CEN Workshop Agreement 14167-3: "Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 3".

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

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 containing Attribute Certificates

Attribute Certificate (AC) validity period: time period during which an Attribute Certificate is deemed to be valid

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

Attribute Certification Disclosure Statement (ACDS): supplemental to ACP and ACPS and simplified document that can assist Attribute Certificates users in making informed trust decisions

Attribute Certification Practice Statement (ACPS): statement of practices which a Attribute Authority employs in issuing Attribute Certificates

Attribute Granting Authority (AGA): authoritative source of an attribute

NOTE: The Attribute Granting Authority was called in TR 102 044 the Attribute Issuing Authority (AIA).

Certification Authority (CA): authority trusted by one or more users to create and assign Public Key Certificates

Certification-Service-Provider (CSP): entity or a legal person who issues certificates or provides other services related to electronic signatures [see Directive 1999/93/EC [1]]

NOTE: The present document is only concerned with certification service providers issuing Attribute Certificates. The present document is not concerned with other types of CSP functions.

electronic signature: data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication of that data [see Directive 1999/93/EC [1]]

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

Public Key Certificate (PKC): Public Key of a user, together with some other information, rendered un-forgeable by encipherment with the private key of the Certification Authority which issued it [see ITU-T Recommendation X.509 [2]].

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

qualified electronic signature: advanced electronic signature which is based on a Qualified Certificate and which is created by a secure-signature-creation device, as defined in article 5.1 of Directive 1999/93/EC

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

relying party: recipient of a certificate which acts in reliance on that certificate and/or digital signatures verified using that certificate [see IETF RFC 2527, bibliography]

subject: entity identified in an Attribute Certificate as the holder of the attributes included in that certificate

subscriber: entity subscribing with an Attribute Authority

NOTE: The subscriber may be a subject or an AGA.

3.2 Abbreviations

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

AA	Attribute Authority
AC	Attribute Certificate
ACP	Attribute Certificate Policy
ACPS	Attribute Certification Practice Statement
ACDS	Attribute Certification Disclosure Statement
ACRL	Attribute Certificate Revocation List
AGA	Attribute Granting Authority
CA	Certification Authority
CSP	Certification Service Provider
EESSI	European Electronic Signature Standardization Initiative
ISO	International Organization for Standardization

OID	Object Identifier
PKC	Public Key Certificate
PKI	Public Key Infrastructure
QC	Qualified Certificate
SSCD	Secure Signature Creation Device
XML	eXtended Mark up Language

4 General concepts

When a signer signs a document it is of primary importance to be able to identify such signatory in the interest of accountability. This enables the transaction to be traceable. However, in many cases, in order to accept a signature, the acceptance criteria may not necessarily be based on the identity of the signer but instead, or additionally, on the qualification(s) of the signer. Qualifications in this context have the meaning of specific features or attributes that the signatory might possess in order to perform a certain act.

Such a qualification may be obtained using Attribute Certificates included in electronic signatures.

4.1 Certified attributes

Attributes are certified by an Attribute Authority (AA) using Attribute Certificates (ACs).

Before being granted, attributes shall be verified as specified in clauses 7.2.1 p) and 7.2.2 c) in a way that the issuing authority is satisfied as to their authenticity. It shall be verified that, at the time of registration for an attribute, the individual was entitled to claim that attribute.

The Attribute Authority is responsible for verifying the correct attribution of attributes to subjects.

4.2 Attribute Authority

An Attribute Authority is a certification-service-provider, as defined in Directive 1999/93/EC [1], which issues Attribute Certificates.

The Attribute Authority has overall responsibility for the provision of the certification services identified in clause 7.1. The Attribute Authority may make use of other parties to provide parts of its service. However, the Attribute Authority always maintains overall responsibility and ensures that the policy requirements identified in the present document are met. For example, an Attribute Authority may sub-contract all the component services, including the Attribute Certificate generation service. However, the key used to generate the Attribute Certificates is identified as belonging to the AA, and the AA maintains overall responsibility for meeting the requirements defined in the present document and liability for the issuing of Attribute Certificates to the public.

4.3 Attribute certification services

The service of issuing Attribute Certificates is broken down in the present document into the following component services for the purposes of classifying requirements:

- **Attribute registration service:** upon subscribers' request, verifies and registers specific attributes to be included in one or more Attribute Certificates later issued to requesting subjects.
- **AC Acquisition service:** upon subjects' request, triggers issuance by the AC generation service of Attribute Certificates that include attributes previously registered by the attribute registration service. If subject authentication is required, verifies that the subject is the rightful owner of the Public Key Certificate, Attribute Certificates point to. Subjects may receive the requested ACs along this service.
- **AC generation service:** when triggered by the AC Acquisition service or the Dissemination service, it creates and signs Attribute Certificates based on information registered by the Attribute registration service. This service feeds both the Dissemination service and the AC Acquisition service.

- **Dissemination service:** if the subject consents, it disseminates ACs to relying parties. Subjects may fetch their own ACs along this service. This service also disseminates the AA's terms and conditions, and any published policy and practice information, to subscribers, subjects and relying parties.
- **Attribute revocation management service:** processes requests and reports relating to AC revocation coming from subscribers, and optionally subjects and parties authorized by the subscriber to determine the necessary action to be taken. The results of this service are distributed through the AC revocation status service.
- **AC revocation status service:** provides AC revocation status information to relying parties. This service may be a real-time service (OCSP) or may be based upon ACRLs which is updated at regular intervals.

This subdivision of services is only for the purposes of clarification of policy requirements and places no restrictions on any subdivision of an implementation of the AA services.

The following diagram illustrates the interrelationship between the services.

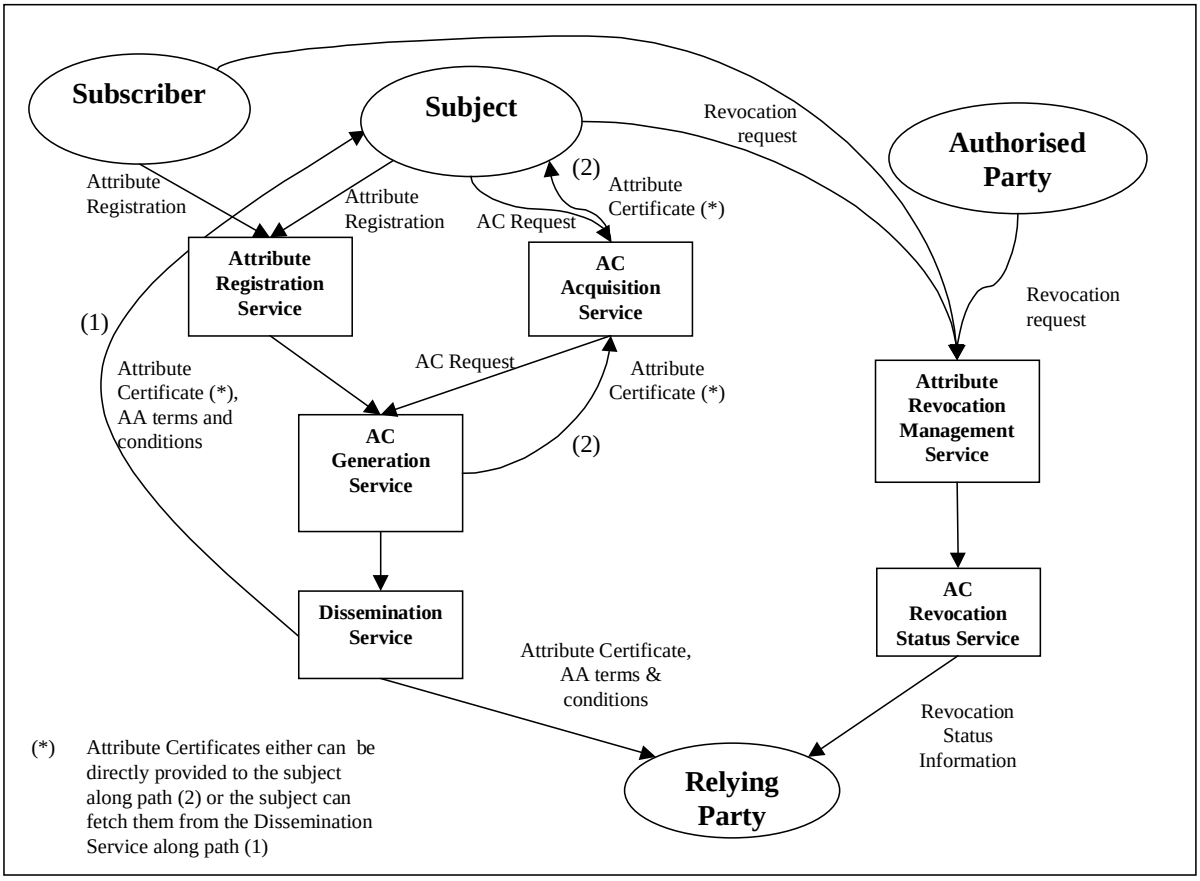


Figure 1: Interrelationship between the services

Subscribers first need to contact the Attribute Registration service. Thereafter attributes may be obtained by subjects in two ways:

- using the AC acquisition service; or
- accessing the Dissemination service.

Attributes are delivered in Attribute Certificates. Attribute Certificates are distributed to relying parties by means of the Dissemination service if subjects give their consent.

Subjects may either receive their own ACs along the AC Acquisition service, or fetch them with the Dissemination service.

The AA's terms and conditions, and any published policy and practice information are available from the Dissemination service.

Attribute and Attribute Certificate revocation is handled by the Attribute Revocation Management service which receives request for revocation from subscribers and optionally subjects and parties authorized by the subscriber. The revocation information is made available by the AC Revocation Status Service.

4.4 Attribute certificate policy and attribute certification practice statement

This clause explains the relative roles of Attribute Certificate policies and attribute certification practice statements. It places no restriction on the form of an Attribute Certificate policy or an attribute certification practice statement specification.

4.4.1 Purpose

In general, the purpose of the Attribute Certificate policy, referenced by a policy identifier in an Attribute Certificate, states "*what* is to be adhered to", while a certification practice statement states "*how* it is adhered to", i.e. the processes it will use in creating and maintaining the certificate. The present document specifies Attribute Certificate policies to meet the requirements for Attribute Certificates. AAs specify in attribute certification practice statements how these requirements are met.

4.4.2 Level of specificity

An Attribute Certificate policy is a less detailed document than an attribute certification practice statement. An attribute certification practice statement is a more detailed description of the terms and conditions as well as business and operational practices of an Attribute Authority in issuing and otherwise managing Attribute Certificates. An attribute certification practice statement defines how a specific Attribute Authority meets the technical, organizational and procedural requirements identified in an Attribute Certificate policy.

NOTE: An ACPS will go in detail as far as necessary to provide sufficient information to users who need to assess the trustworthiness of AA operation. In no case will the ACPS include confidential or sensitive security related information.

4.4.3 Approach

The approach of an Attribute Certificate policy is significantly different from an attribute certification practice statement. An Attribute Certificate policy is defined independently of the details of the specific operating environment of an Attribute Authority, whereas a certification practice statement is tailored to the organizational structure, operating procedures, facilities, and computing environment of an Attribute Authority. An Attribute Certificate policy may be defined by the user of certification services, whereas the attribute certification practice statement is always defined by the provider of certification services.

4.4.4 Other AA statements

In addition to the policy and practice statements an AA may issue terms and conditions of general commercial purpose. They must follow the requirements of general conditions and comply with the requirements set out in Directive 93/13/EEC [7] as implemented in the national legislation of the member states. In specific, general conditions are non-negotiable and binding to a non-determined number of end users. They have, however, to be brought to the attention of contracting counter parties and especially to consumers. Terms and conditions will only be effective against relying parties, who have no other contractual arrangement with the AA if:

- they are easily accessible; and
- their existence together with information as to how they can be accessed is brought to their attention in a conspicuous manner; and
- they remain in line with the member state law regarding general conditions.

An Attribute Disclosure Statement is a summary of those matters which are considered to be essential information regarding the issuance and use of an Attribute Certificate and which must be brought to the attention of subscribers, subjects and relying parties. If a model Attribute Disclosure Statement is used it must be properly adapted to the legal framework prevailing in the member state an AA operates from.

4.5 Subscriber and subject

In some cases ACs are issued directly to individuals for their own use. However, there commonly exist other situations where the party requiring the issuance of ACs is different from the subject to whom the AC applies. For example, a company may require ACs for its employees to allow them to participate in electronic business on behalf of the company. In such situations the entity subscribing to the Attribute Authority for the issuance of ACs is different from the entity which is the subject of the AC.

As another example, the AGA may be a subscriber. It asks an AA to issue ACs for the attributes that are directly managed by it.

In the present document to clarify the requirements which are applicable to the two different roles that may occur two different terms are used. The **"subscriber"** contracts with the Attribute Authority for the issuance of Attribute Certificates while the **"subject"** is the entity to whom the Attribute Certificate applies.

In the case of ACs issued to individuals for their own use the subscriber and subject can be the same entity. In other cases, such as ACs issued to employees the subscriber and subject are different and the subscriber is acting on behalf of the subject. The subscriber would be, for example, the employer. The subject would be the employee.

In the cases where the subscriber is an Attribute Granting Authority, the subject has to give his consent to the Attribute Granting Authority for acting as the subscriber.

Within the present document these two terms are used with this explicit distinction wherever it is meaningful to do so, although in some cases the distinction is not always crystal clear.

Two cases are being considered:

- whether the subscriber is the subject or acting on behalf of a subject.
- when the subscriber is the AGA.

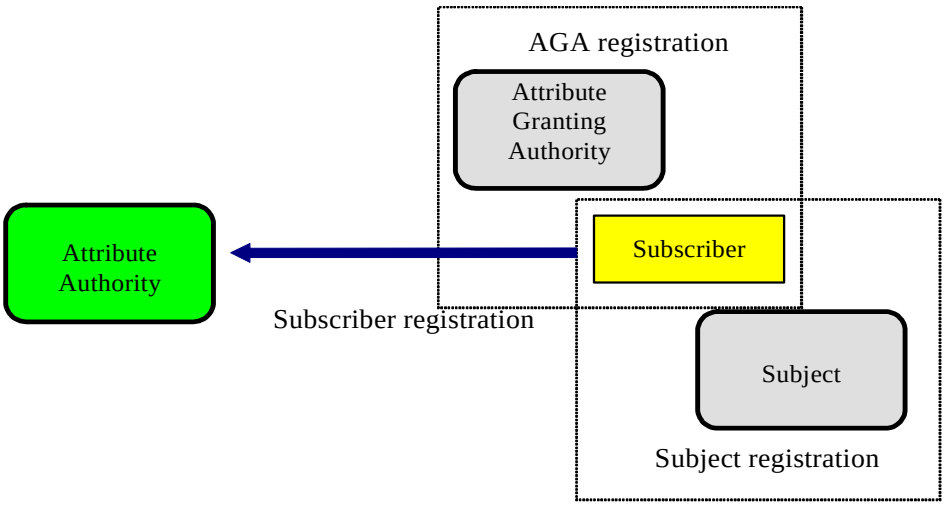


Figure 2: Subject registration and AGA registration

The subscriber is always entitled to ask for the revocation of an attribute that it has registered. When the subscriber is an AGA, then the AGA is able to revoke the attribute.

4.6 Attribute semantics

The semantics of an attribute may be either defined in a standard (e.g. by ISO) or defined by any organization.

When the attribute is defined in a standard, it may be used in an open community.

NOTE: It may be specified using an OID that has a global international definition. This is in this way that X.509 has defined a set of standard attributes. When it is locally defined by any organization, two approaches are possible:

- use an OID located under the OID of the organization,
- define the OID of the "issuing authority" (e.g. as called in ISO/TS 17090-2, see bibliography) and add a definition of the attribute in any syntax (e.g. character string, XML).

When the attribute is locally defined by an organization, its use may be restricted to a close community. The semantics of the attribute has then to be interpreted using the identifier of the granting authority (also called sometimes "issuing authority") in combination with the definition of the attribute by that authority.

5 Introduction to Attribute Certificate policies

5.1 Overview

An Attribute Certificate policy is a "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".

The policy requirements are specified in the present document in terms of Attribute Certificate policies. These Attribute Certificate policies are for Attribute Certificates, and hence are called Attribute Certificate policies. Attribute Certificates issued in accordance with the present document include an Attribute Certificate policy identifier which can be used by relying parties in determining the certificates' suitability and trustworthiness for a particular application.

The present document specifies two Attribute Certificate policies suitable to be used in conjunction with qualified certificates as indicated below.

5.2 Identification

The identifiers for the two Attribute Certificate policies specified in the present document are:

1) **Subject as subscriber:** This policy is used when the subscriber is either the subject or a person acting on behalf of the subject:

   itu-t(0) identified-organization(4) etsi(0) attribute-certificate-policies(2158) ac-policy-identifiers(1) subject-as-subscriber(1)

   Using the subject-registration identifier, only attributes that have been registered by the subject shall be placed in the AC.

2) **AGA as subscriber:** This policy is used when the subscriber is an AGA:

   itu-t(0) identified-organization(4) etsi(0) attribute-certificate-policies(2158) ac-policy-identifiers(1) aga-as-subscriber(2)

   Using the AGA-registration identifier, only attributes that have been registered by AGAs shall be placed in the AC.

By including one of these object identifiers in an Attribute Certificate, the AA claims conformance to the identified Attribute Certificate policy for that AC.

An AA may support both policies.

5.3 User community and applicability

Attribute certificates issued under this policy may be used to support electronic signatures which "satisfy the requirements of a signature in relation to data in electronic form in the same manner as a hand-written signature satisfies those requirements in relation to paper based data", as specified in article 5.1 of Directive 1999/93/EC [1].

5.4 Conformance

The AA shall only use the identifiers for the Attribute Certificate policies as given in clause 5.2:

a) if the AA claims conformance to the identified Attribute Certificate policy and makes available to subscribers and relying parties on request the evidence to support the claim of conformance; or

b) if the AA has been assessed to be conformant to the identified Attribute Certificate policy by a competent independent party.

NOTE: See clause 8 if the present document is used as a framework for other Attribute Certificate policies.

6 Obligations and liability

6.1 Attribute authority obligations

The AA shall ensure that all requirements, as detailed in clause 7, are implemented as applicable to the Attribute Certificate policy.

The AA has the responsibility for conformance with the procedures prescribed in this policy, even when the AA functionality is undertaken by subcontractors.

The AA shall provide all its attribute certification services consistent with its attribute certification practice statement.

6.2 Subscriber obligations

1) The AA shall oblige, through agreement (see clause 7.2.3.1 a)), the subscriber to ensure that the subscriber fulfils the following obligations:

   a) submit accurate and complete information to the AA in accordance with the requirements of this policy, particularly with regards to registration;

   b) notify the AA without any unreasonable delay, if any of the following occur up to the end of the registration period indicated at the time of registration:

      - inaccuracy to the registration information content, as notified to the subscriber;

      - changes to the registration information content, as notified to the subscriber.

NOTE: Subscribers might incur liability toward any third party including relying parties for any delay to contact the AA.

6.3 Subject obligations

The AA shall oblige, through agreement (see clause 7.2.3.1 a)), the subscriber to agree with the subject that the subject is bound to:

- use the Attribute Certificate solely for the usage specified in the ACPS;

- notify the subscriber without any unreasonable delay, when there is an inaccuracy in the content of an AC, whatever the reason maybe, including a change in the ownership of an attribute.

6.4 Information for relying parties

The ACDS shall include a notice that if it is to reasonably rely upon an Attribute Certificate, it shall:

a) verify the validity, suspension or revocation of the Attribute Certificate using current revocation status information as indicated to the relying party; and

NOTE: Depending on AA's practices and the mechanism used to provide revocation status information, there may be a delay in disseminating the revocation status information. This delay will depend on the nature of the attribute information being certified.

b) take account of any limitations on the usage of the Attribute Certificate communicated to the relying party either in the Attribute Certificate or the terms and conditions supplied; and

c) take any other precautions prescribed in agreements or elsewhere.

It is the responsibility of the Attribute Authority to ensure that any limitations governing the reliance on Attribute Certificates or limitations conditions on liability are clearly brought to the attention of any relying party.

6.5 Liability

The liability of AAs issuing Attribute Certificates applies to parties who "reasonably rely" on an Attribute Certificate. The AA shall specify in its ACPS its liabilities and how it covers its liabilities. See annex B further details.

NOTE: The ACPS may include disclaimers and limitations of liability including the purposes/uses for which the AA accepts or excludes liability. Any term which aims to limit liability is subject to national laws from the country where the AA is established.

7 Requirements on AA practice

The AA shall implement the controls that meet the following requirements.

The present document is concerned with AAs issuing Attribute Certificates. This includes the provision of services for attribute registration, AC acquisition, AC generation, dissemination, attribute revocation management and AC revocation status (see clause 4.3). Where requirements relate to a specific service area of the AA then it is listed under one of these subheadings. Where no service area is listed, or "AA General" is indicated, a requirement is relevant to the general operation of the AA.

These policy requirements are not meant to imply any restrictions on charging for AA services.

The requirements are indicated in terms of the security objectives followed by more specific requirements for controls to meet those objectives where considered necessary to provide the necessary confidence that those objective will be met.

NOTE: The details of controls required to meet an objective is a balance between achieving the necessary confidence whilst minimizing the restrictions on the techniques that a AA may employ in issuing Attribute Certificates. In case of clause 7.4 (AA management and operation) reference is made to other more general standards which may be used as a source of more detailed control requirements. Due to these factors the specificity of the requirements given under a given topic may vary.

7.1 Attribute Certification practice statements

The AA shall ensure that it demonstrates the reliability necessary for providing attribute certification services.

In particular:

a) The AA shall have a statement of the practices and procedures used to address the requirements identified for each of the Attribute Certificate policies it supports.

NOTE 1: These policies make no requirement as to the structure of the attribute certification practice statement.

b) The ACPS shall identify the obligations of all external organizations supporting the AA services including the applicable policies and practices.

NOTE 2: The external organizations need not to be identified in the ACPS.

c) The AA shall make available to subscribers and relying parties its ACPS, and other relevant documentation, as necessary to assess conformance to each Attribute Certificate policy.

NOTE 3: The AA is not generally required to make all details of its practices public, except those that materially affect subscribers, relying parties and any other third party that participate in the AA certificate life cycle, community or applicability.

d) The AA shall disclose to all subscribers, subjects and potential relying parties the terms and conditions regarding use of the Attribute Certificate as specified in clause 7.2.3.1.

e) The AA shall have a high-level management body with final authority and responsibility for approving the ACPS.

f) The senior management of the AA has responsibility for ensuring the practices are properly implemented.

g) The AA shall define a review process for certification practices including responsibilities for maintaining the ACPS.

h) The AA shall give due notice of changes it intends to make in its ACPS and shall, following approval as in (e) above, make the revised ACPS immediately available as required under (c) above.

i) The AA shall specify in its ACPS the details of the information and practices upon which the attributes it certifies are verified, including the sources of information that are used to grant an attribute.

j) The AA shall specify in its ACPS the attribute certification validity periods.

k) The AA shall specify in its ACPS the support or the non-support of attribute revocation. When revocation is supported, the revocation procedures to be followed shall be specified.

l) The AA shall specify in its ACPS whether attributes can be individually acquired in a single AC or acquired together with other attributes. When multiple attributes can be acquired in a single AC, the procedure to be followed shall be specified.

NOTE 4: For example, the set of attributes to be placed in a single AC may be defined by the subject or by the AA. In the former case, ways to select a subset of the attributes should be made available to the subject. In the later case, the subject must have ways to know which attributes a given subset contains.

m) The AA shall specify in its ACPS whether and how a subject can inform the AA that he/she wants to delegate one or more of his/her attributes to another subject.

7.2 Attribute management life cycle

7.2.1 Subject and attribute initial registration

The AA shall ensure that:

1) The subject is the rightful owner of the PKC the AC will make reference to;

NOTE 1: A way to perform this verification is by asking the subject to issue in presence of the AA, or of its delegate, an electronic signature that the AA can verify with the above mentioned PKC. Alternatively the AA can verify that the requesting subject's identity matches the one indicated in the involved PKC.

2) Subjects, subscribers or persons authorized by the subscriber are aware of the procedure to ask for the revocation of one or more attributes of the currently ACs that hold these attributes.

NOTE 2: By limiting the validity period, the AA may avoid the necessity to revoke ACs. This is possible in particular when the latency time to effectuate a revocation exceeds the validity period.

In particular:

a) Before entering into a contractual relationship with a subscriber, the AA shall provide the subscriber with the terms and conditions regarding use of the Attribute Certificates as given in clause 7.1.2.

b) The AA shall communicate this information through a durable (i.e. with integrity over time) means of communication, which may be transmitted electronically, and in readily understandable language.

NOTE 3: A model AC disclosure statement which may be used as the basis of such a communication is given in annex B.

c) The AA shall verify the subject's right to exert the attributes to be registered.

d) The AA shall verify by appropriate means the identity of the subject, either directly or indirectly. The submitted evidence may be in the form of either paper or electronic documentation and shall contain:

- full name (including surname and given names);
- date and place of birth;
- other attributes (e.g. a nationally recognized identity number) which may be used to distinguish the person from others with the same name.

e) If the evidence of the subject's identity is checked indirectly, means shall be used which provide equivalent assurance to physical presence.

NOTE 4: An example of evidence checked indirectly against a physical person is documentation presented for registration which was acquired as the result of an application requiring physical presence.

NOTE 5: If the evidence of the subject's identity is checked using the testimony of a subject representative (e.g. a lawyer) the AA should ascertain the identity of that representative.

f) The subject and the subscriber shall provide a physical address, or other attributes, which describe how they may be contacted.

g) The AA shall record all the information used to verify the subject's identity and the PKC, including any reference number on the documentation used for verification, and any limitations on its validity.

h) The AA shall inform the subscriber on the ways for the subject to receive Attribute Certificates that have been granted by the AA.

i) The AA shall record the signed agreement with the subscriber including:

- agreement to the subscriber's obligations (see clause 6.2);
- the subscriber's and subject's consent to the keeping of a record by the AA of information used in registration (see clause 7.4.11 h), i), j)), and any subsequent revocation (see clause 7.4.11 m)), and passing of this information to third parties under the same conditions as required by this policy in the case of the AA terminating its services;
- whether, and under what conditions, the subscriber requires the subject's consent to the publication of attributes certificates;
- confirmation that the information registered is correct;
- the subject's agreement to any relevant terms, including appropriate consent under data protection legislation.

NOTE 6: Other parties (e.g. the associated person or legal entity) may be involved in establishing this agreement.

NOTE 7: This agreement may be in electronic form, providing all involved parties consent.

j) The records identified above shall be retained for a period of time as indicated to subscriber and subject (see a) and b) above) and as necessary for the purposes of providing evidence of certification in legal proceedings.

k) The AA shall ensure that the requirements of the national data protection legislation are adhered to within their registration process.

l) The confidentiality and integrity of registration data shall be protected especially when exchanged with the subscriber, the subject or within the AA organization.

m) In the event that external registration service providers are used, the AA shall verify that registration data is exchanged with recognized registration service providers, whose identity is authenticated.

n) The AA shall ensure that subjects and/or subscribers are given sufficient information on the means to revoke one or more attributes and, consequently, the ACs that include the attributes to be revoked.

o) The AA shall ensure that subjects' attributes are properly verified.

Attribute Registration:

p) The AA shall verify that, at the time of registration of an attribute, the individual was entitled to that attribute. That verification shall be done by appropriate means and in accordance with national law.

q) The AA shall record all information used to verify the attributes of the subject.

r) The AA shall ensure that the subject consents to the issuance of ACs.

s) The AA shall record the information demonstrating that a subject has accepted to obtain Attribute Certificates using this service.

7.2.2 Attribute renewal

When the time period during which the certified attributes are provided through this service has expired, then a new attribute registration may take place. The AA shall ensure that subjects' attributes to be registered or renewed are properly verified and that they relate to an already registered subject. In particular:

Attribute Registration:

a) If any of the AA terms and conditions have changed, these shall be communicated to the subscriber and agreed to in accordance with clause 7.2.1 a), b) and j).

b) If any information has changed, this is verified, recorded, agreed to by the subscriber in accordance with clause 7.2.1 c) to i).

c) The AA shall check by appropriate means that subject is the rightful owner of the public key certificate the Attribute Certificate will make reference to and that he/she is entitled to the attributes requested to be certified.

d) The AA shall verify the correctness of subscriber and subject address information in its records and update these records if necessary.

e) The AA shall record all information used to verify the subjects' rights (see item c), including any reference number on the documentation used for verification, and any limitations on its validity.

f) The records identified in this clause 7.2.2 shall be retained for the period of time as indicated to the subscriber (see a) and b) above) and longer in case the AA has been informed, before the end of that time period, of the existence of a legal proceeding.

g) The confidentiality and integrity of registration data shall be protected especially when exchanged with the subscriber, subject or within the AA organization.

h) The AA shall verify that registration data is exchanged with recognized registration service providers, whose identity is authenticated, in the event that external registration service providers are used.

i) The AA shall verify by appropriate means in accordance with national law, the attributes of the person for which Attribute Certificates may be requested.

j) The AA shall record all information used to verify the attributes of the subject.

k) The AA shall record the signed agreement with the subscriber including:

- whether, and under what conditions, the subscriber requires the subject's consents to the inclusion in ACs of the attributes that have been registered;
- confirmation that the information registered is correct.

NOTE 1: Other parties (e.g. the associated person or legal entity) may be involved in establishing this agreement.

NOTE 2: This agreement may be in electronic form.

l) The AA shall ensure that the subject consents to be granted attributes using this service.

7.2.3 Dissemination of Terms and Conditions

7.2.3.1 Terms and Conditions for subscribers and subjects

The AA shall ensure that the terms and conditions are made available to subscribers, subjects, and relying parties.

In particular:

Dissemination

a) The AA shall make available to subscribers, subjects and relying parties the ACP and/or ACPS as well as any applicable terms and conditions regarding the provision and the use of the Attribute Certificates:

1) the identifier(s) for the certificate policy (or policies) being supported and to which it claims conformance;

2) a clear description of the meaning of each type of attribute that is supported. That description shall be given in readily-understandable terms, and, if appropriate, the law or regulation that defines or assigns the attribute shall be indicated;

3) the list of documents the subject must exhibit to prove his/her right to register an attribute and the procedures used by the AA for the verification of such right;

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

5) any limitations on their use;

6) the subscriber's and subject's obligations as defined in clause 6.2;

7) how Attribute Certificates will be provided;

8) how revocation of attributes and of Attribute Certificates will be handled (if applicable);

9) information on how to validate the Attribute Certificate, including information related to checking the revocation status of the Attribute Certificate, when that service is provided, such that relying parties can "reasonably rely" on the Attribute Certificate (see clause 6.4);

10) disclaimers and limitations of liability including the purposes/uses for which the AA accepts or excludes liability;

11) the period of time during which registration information (see clauses 7.2.1 j) and 7.2.2 f)) is retained;

12) the period of time which AA event logs (see clause 7.4.11 e)) are retained;

13) procedures for complaints and dispute settlement;

14) the applicable governing laws; and

15) if the AA has been certified to be conformant with the identified Attribute Certificate policy, and if so through which scheme.

b) The information identified in a) above shall be available through a durable (i.e. with integrity over time) means of communication, which may be transmitted electronically, and in readily understandable language.

NOTE: A model AC disclosure statement which may be used as the basis of such a communication is given in annex B. Alternatively this may be provided as part of a subscriber/relying party agreement. These terms and conditions may be included in an attribute certification practice statement provided that the reader's attention is drawn to this by conspicuous means.

7.2.4 Attribute Certificate acquisition

The AA shall ensure that requests to obtain Attribute Certificates for issuance to a subject who has already previously registered are duly authorized.

In particular:

AC acquisition

a) The AA shall issue an Attribute Certificate which contains the information described in annex A.

NOTE 1: A standard format for Attribute Certificates is defined in X.509 [2] and in RFC 3281 (see bibliography).

b) The AA shall issue an Attribute Certificate only to the legitimate public key certificate holder.

NOTE 2: This can be done using a subject's previously registered QC.

NOTE 3: The AA may decide to check or not the revocation status of a subject's QC, since the AC will be unusable if the QC to which it is linked is revoked.

c) When more than one attribute may be certified by an AA, subscribers and/or subjects shall be allowed to specify the attributes to be included.

NOTE 4: Attributes may be provided in a single AC or in several ACs.

7.2.5 Attribute Certificate dissemination

ACs may also be distributed to users using the dissemination service.

Dissemination

a) Attribute Certificates shall be available for retrieval by relying parties in only those cases for which the subscriber's consent has been obtained;

b) the information identified in a) above shall be publicly and internationally available.

7.2.6 Attribute Certificate generation

The AA shall ensure that Attribute Certificates are issued securely.

In particular:

a) The AC generation service shall generate ACs that contain at least the fields described in annex A. AC Profiles shall be included in the ACP and/or ACPS.

b) The AC generation service shall ensure that only AC requests are accepted which originate from within the AA organization and are in accordance with the AA procedures.

7.2.7 Attribute and AC revocation and suspension

The AA shall ensure that either attributes and/or ACs are revoked in a timely manner based on authorized and validated certificate revocation requests.

In particular:

Revocation management

a) The AA shall document as part of its certification practice statement (see clause 7.1) the procedures for revocation of attributes and/or ACs including:

   1) who may submit revocation reports and requests;

   2) how they may be submitted;

   3) any requirements for subsequent confirmation of revocation reports and requests;

NOTE 1: For example, a confirmation may be required from the subscriber if a compromise is reported by a third party.

   4) whether and for what reasons attributes may be suspended;

   5) whether and for what reasons Attribute Certificates may be suspended;

   6) the mechanism used for distributing revocation status information;

   7) the maximum delay between receipt of a revocation request or report and the change to revocation status information being available to all relying parties.

NOTE 2: Planned-in-advance revocations may also be possible. Such revocations come in force at a requested time.

b) The AA shall ensure that the individuals or the authorities entitled to ask for the revocation of any registered attribute are nominated.

c) Requests and reports relating to revocation (e.g. due to death of the subject, unexpected termination of a subscriber's or subject's agreement or business functions, violation of contractual obligations) shall be processed on receipt.

d) Requests and reports relating to revocation shall be authenticated and checked to originate from an authorized source. Such reports and requests will be confirmed as required under the AA's procedures.

e) An Attribute Certificate's revocation status may optionally be set to suspended whilst the revocation is being confirmed. The AA shall ensure that an Attribute Certificate is not kept suspended for longer than is necessary to confirm its status.

f) The subject, and where applicable the subscriber, of a revoked or suspended Attribute Certificate, shall be informed of the change of status of that Attribute Certificate.

g) Once an Attribute Certificate is definitively revoked (i.e. not suspended) it shall not be reinstated.

h) Where Attribute Certificate Revocation Lists (ACRLs) including any variants (e.g. delta ACRLs) are used, these shall be published at least daily and:

   1) every ACRL shall state a time limit for next ACRL issuance;

   2) a new ACRL may be published before the stated time limit of the next ACRL issuance;

   3) the ACRL shall be signed by the Attribute Authority or an authority designated by the AA.

NOTE 3: ACRLs are defined in [2] and in [3].

i) Attribute revocation management services shall at least be available during business hours and during working days. Upon system failure, service or other factors which are not under the control of the AA, the AA shall make best endeavours to ensure that this service is not unavailable for longer than a maximum period of time as denoted in the ACPS.

Revocation status

j) AC Revocation status information, shall be available 24 hours per day, 7 days per week. Upon system failure, service or other factors which is not under the control of the AA, the AA shall make best endeavours to ensure that this information service is not unavailable for longer than a maximum period of time as denoted in the attribute certification practice statement.

NOTE 4: Revocation status information may be provided, for example, using on-line certificate status service or through distribution of ACRLs through a repository.

k) The integrity and authenticity of the status information shall be protected.

l) Revocation status information shall be publicly and internationally available.

7.3 Attribute Authority keys management life cycle

7.3.1 Attribute Authority keys generation

Attribute Authority keys may be used for three different purposes:

- signing ACs;
- signing ACRLs (revocation status information signing key);
- signing OCSP responses (revocation status information signing key).

A different key should be used for each different purpose.

Certificate generation

The AA shall ensure that AA signing keys are generated in controlled circumstances.

In particular:

a) AA key generation shall be undertaken in a physically secured environment (see clause 7.4.4) by personnel in trusted roles (see clause 7.4.3) under, at least, dual control. The number of personnel authorized to carry out this function shall be kept to a minimum and be consistent with the AA's practices.

b) AA key generation shall be carried out within a device which:

- meets the requirements identified in CEN Workshop Agreement 14167-1 [8]; or
- meets the requirements identified in CEN Workshop Agreement 14167-3 [9]; or
- is a trustworthy system which is assured to EAL 4 or higher in accordance to ISO/IEC 15408 [5] or equivalent security criteria. This shall be to a security target or protection profile which meets the requirements of the present document, based on a risk analysis and taking into account physical and other non-technical security measures.

NOTE: The rules of clause 7.3.1 (b to d) apply also to key generation even if carried out in a separate system.

c) AA key generation shall be performed using an algorithm recognized as being fit for the purposes of Attribute Certificates.

d) The selected key length and algorithm for AA signing key shall be one which is recognized as being fit for the purposes of Attribute Certificates as issued by the AA.

7.3.2 Attribute Authority keys storage, backup and recovery

Certificate generation

The AA shall ensure that AA private keys remain confidential and maintain their integrity. In particular:

a) The AA private signing key shall be held and used within a secure cryptographic device which:

- meets the requirements identified in CEN Workshop Agreement 14167-1 [8]; or
- meets the requirements identified in CEN Workshop Agreement 14167-2 [6]; or
- is a trustworthy system which is assured to EAL 4 or higher in accordance to ISO/IEC 15408 [5] or equivalent security criteria. This shall be to a security target or protection profile which meets the requirements of the present document, based on a risk analysis and taking into account physical and other non-technical security measures.

b) Where the keys are stored in a dedicated key processing secure cryptographic device, access controls shall be in place to ensure that the keys are not accessible outside the secure cryptographic device.

Keys backup and recovery

AA signing keys may be backed up. If back up is supported, then the following applies:

c) If and when outside the secure cryptographic device the AA private signing keys shall be protected using an algorithm and, where applicable, a key-length that, according to the state of the art, are capable to withstand crypto analytic attacks for the residual life of the encrypted key or key component.

d) AA private signing keys shall be backed up, stored and recovered only by personnel in trusted roles using, at least, dual control in a physically secured environment (see clause 7.4.4). The number of personnel authorized to carry out this function shall be kept to a minimum and be consistent with the AA's practices.

e) Backed-up copies or components of the AA private signing keys shall be subject to the same or greater level of security controls as keys currently in use.

f) Where the keys are stored within a back-up security module, access controls shall be in place to ensure that the security module is not usable by unauthorized personnel and can only be activated under at least dual control.

7.3.3 Attribute Authority public keys distribution

Certificate generation and Dissemination

The AA shall ensure that the integrity and authenticity of the AA signature verification (public) keys and any associated parameters are maintained during its distribution to relying parties. In particular:

a) AA signature verification public keys shall be made available to relying parties in a manner that assures their integrity and authenticates their origin.

NOTE: Attribute Authority public keys may e.g. be distributed in PKCs signed by CAs.

7.3.4 Attribute authority keys usage

The AA shall ensure that AA private signing keys are not used inappropriately. In particular:

a) AA signing key(s) used for generating Attribute Certificates, as defined in clause 7.3.1, shall not be used for any other purpose, except for signing ACRLs and/or OCSP responses, as specified in clause 7.3.1.

b) AA signing key(s) used for generating Attribute Certificates shall only be used within physically secure premises.

7.3.5 End of AA key life cycle

The AA shall ensure that AA private signing keys are not used beyond the end of their life cycle. In particular all copies of the AA private signing keys shall be destroyed such that the private keys cannot be retrieved.

7.3.6 Life cycle management of cryptographic hardware used to sign ACs, ACRLs or OCSP responses

The AA shall ensure the security of cryptographic hardware throughout its lifecycle.

In particular the AA shall ensure that:

a) the cryptographic hardware is not tampered with during shipment;

b) the cryptographic hardware is not tampered with while stored;

c) the installation and activation of the AA's certificate signing cryptographic hardware shall require simultaneous control of at least two trusted employees;

d) the generation, activation, back-up and recovery of the AA's signing keys in cryptographic hardware shall require simultaneous control of at least two trusted employees;

e) the cryptographic hardware is functioning correctly; and

f) AA private signing keys stored on AA cryptographic hardware are destroyed upon device retirement.

7.4 AA management and operation

7.4.1 Security management

The AA shall ensure that administrative and management procedures are applied which are adequate and correspond to recognized standards.

In particular:

AA General

a) The AA shall ensure that a risk assessment is carried out to evaluate business risks and determine the necessary security requirements and operational procedures.

b) The AA shall retain responsibility for all aspects of the provision of certification services, even if some functions are outsourced to subcontractors. Responsibilities of third parties shall be clearly defined by the AA and appropriate arrangements made to ensure that third parties are bound to implement any controls required by the AA. The AA shall retain responsibility for the disclosure of relevant practices of all parties.

c) The AA management shall provide direction on information security through a suitable high level steering forum that is responsible for defining the AA's information security policy and ensuring publication and communication of the policy to all employees who are impacted by the policy.

d) The information security infrastructure necessary to manage the security within the AA shall be maintained at all times. Any changes that will impact on the level of security provided shall be approved by the AA management forum.

NOTE 1: See ISO/IEC 17799 (bibliography) for guidance on information security management including information security infrastructure, management information security forum and information security policies. Other alternative guidance documents are given in bibliography.

e) The security controls and operating procedures for AA facilities, systems and information assets providing the certification services shall be documented, implemented and maintained.

NOTE 2: It is recommended that the present documentation (commonly called a system security policy) identifies all relevant targets, objects and potential threats related to the services provided and the safeguards required to avoid or limit the effects of those threats. It is recommended that the documentation describes the rules, directives and procedures regarding how the specified services and the associated security assurance are granted in addition to stating policy on incidents and disasters.

f) AA shall ensure that the security of information shall be maintained when the responsibility for AA functions has been outsourced to another organization or entity.

7.4.2 Asset classification and management

The AA shall ensure that its assets and information receive an appropriate level of protection.

In particular:

AA General

a) The AA shall maintain an inventory of all information assets and shall assign a classification for the protection requirements to those assets consistent with the risk analysis.

7.4.3 Personnel security

The AA shall ensure that personnel and hiring practices enhance and support the trustworthiness of the AA's operations.

In particular:

AA General

a) The AA shall employ personnel which possess the expert knowledge, experience and qualifications necessary for the offered services and as appropriate to the job function.

NOTE 1: It is recommended that AA personnel fulfils the requirement of "expert knowledge, experience and qualifications" through formal training and credentials, actual experience, or a combination of the two.

b) Security roles and responsibilities, as specified in the AA's security policy, shall be documented in job descriptions. Trusted roles, on which the security of the AA's operation is dependent, shall be clearly identified.

c) AA personnel (both temporary and permanent) shall have job descriptions defined from the view point of separation of duties and least privilege, determining position sensitivity based on the duties and access levels, background screening and employee training and awareness. Where appropriate, these shall differentiate between general functions and AA specific functions. It is recommended that the job descriptions include skills and experience requirements. AA personnel shall commit to observing the requirements for the confidentiality and data protection of personal data.

d) Personnel shall exercise administrative and management procedures and processes that are in line with the AA's information security management procedures (see clause 7.4.1).

NOTE 2: See ISO/IEC 17799 (bibliography) for guidance.

Registration, Attribute Certificate generation, revocation management

e) Managerial personnel shall be employed who possess expertise in the electronic signature technology and familiarity with security procedures for personnel with security responsibilities and experience with information security and risk assessment.

f) All AA personnel in trusted roles shall be free from conflicting interests that might prejudice the impartiality of the AA operations. As an example, the AA personnel should not be involved in AGA related activities.

g) Trusted roles include roles that involve the following responsibilities:

- Security Officers: Overall responsibility for administering the implementation of the security practices. Additionally approve the generation/revocation/suspension of Attribute Certificates;

- System Administrators: Authorized to install, configure and maintain the AA trustworthy systems for registration, Attribute Certificate generation, and revocation management;
- System Operators: Responsible for operating the AA trustworthy systems on a day to day basis. Authorized to perform system backup and recovery;
- System Auditors: Authorized to view archives and audit logs of the AA trustworthy systems.

h) AA personnel shall be formally appointed to trusted roles by senior management responsible for security.

i) The AA shall not appoint to trusted roles or management any person who is known to have a conviction for a serious crime or other offence which affects his/her suitability for the position. Personnel shall not have access to the trusted functions until any necessary checks are completed.

NOTE 3: In some countries it may not be possible for AA to obtain information on past convictions. However, the employer may be able to ask the candidate to provide such information and turn down an application in case of refusal.

7.4.4 Physical and environmental security

The AA shall ensure that physical access to critical services is controlled and physical risks to its assets minimized.

In particular:

AA General

a) Physical access to facilities concerned with Attribute Certificate generation, and revocation management services shall be limited to properly authorized individuals;

b) Controls shall be implemented to avoid loss, damage or compromise of assets and interruption to business activities; and

c) Controls shall be implemented to avoid compromise or theft of information and information processing facilities.

Attribute Certificate generation and revocation management

e) The facilities concerned with Attribute Certificate generation and revocation management shall be operated in an environment which physically protects the services from compromise through unauthorized access to systems or data.

f) Physical protection shall be achieved through the creation of clearly defined security perimeters (i.e. physical barriers) around the Attribute Certificate generation and revocation management services. Any parts of the premises shared with other organizations shall be outside this perimeter.

NOTE 1: An acceptable exception to this requirement is the sharing of facilities with PKC issuance and management operations.

g) Physical and environmental security controls shall be implemented to protect the facility housing system resources, the system resources themselves, and the facilities used to support their operation. The AA's physical and environmental security policy for systems concerned with Attribute Certificate generation and revocation management services shall address the physical access control, natural disaster protection, fire safety factors, failure of supporting utilities (e.g. power, telecommunications), structure collapse, plumbing leaks, protection against theft, breaking and entering, and disaster recovery, etc.

h) Controls shall be implemented to protect against equipment, information, media and software relating to the AA services being taken off-site without authorization.

NOTE 2: See ISO/IEC 17799 (bibliography) for guidance on physical and environmental security.

NOTE 3: Other functions may be supported within the same secured area provided that the access is limited to authorized personnel.

7.4.5 Operations management

The AA shall ensure that the AA systems are secure and correctly operated, with minimal risk of failure.

In particular:

AA General

a) The integrity of AA systems and information shall be protected against viruses, malicious and unauthorized software.

b) Damage from security incidents and malfunctions shall be minimized through the use of incident reporting and response procedures.

c) Media used within the AA shall be securely handled to protect media from damage, theft and unauthorized access.

d) Procedures shall be established and implemented for all trusted and administrative roles that impact on the provision of certification services.

Media handling and security

e) All media shall be handled securely in accordance with requirements of the information classification scheme (see clause 7.4.2). Media containing sensitive data shall be securely disposed of when no longer required.

System Planning

f) Capacity demands are monitored and projections of future capacity requirements made to ensure that adequate processing power and storage are available.

Incident reporting and response

g) The AA shall act in a timely and co-ordinated manner in order to respond quickly to incidents and to limit the impact of breaches of security. All incidents shall be reported as soon as possible after the incident according to specific procedures.

Attribute Certificate generation, revocation management

Operations procedures and responsibilities

h) AA security operations shall be separated from normal operations.

NOTE: AA security operations' responsibilities include:

- operational procedures and responsibilities;
- secure systems planning and acceptance;
- protection from malicious software;
- housekeeping;
- network management;
- active monitoring of audit journals, event analysis and follow-up;
- media handling and security;
- data and software exchange.

These responsibilities will be managed by AA security operations, but may actually be performed by non-specialist, operational personnel (under supervision), as defined within the appropriate security policy and roles and responsibility documents.

7.4.6 System Access management

The AA shall ensure that AA system access is limited to properly authorized individuals.

In particular:

AA General

a) Controls (e.g. firewalls) shall be implemented to protect the AA's internal network domains from external network domains accessible by third parties.

NOTE 1: It is recommended that firewalls be configured to prevent protocols and accesses not required for the operation of the AA.

b) Sensitive data shall be protected when exchanged over networks which are not secure.

NOTE 2: Sensitive data includes registration information.

c) The AA shall ensure effective administration of user (this includes operators, administrators and any users given direct access to the system) access to maintain system security, including user account management, auditing and timely modification or removal of access.

d) The AA shall ensure that access to information and application system functions is restricted in accordance with the access control policy and that the AA system provides sufficient computer security controls for the separation of trusted roles identified in AA's practices, including the separation of security administrator and operation functions. Particularly, use of system utility programs shall be restricted and tightly controlled.

e) AA personnel shall be successfully identified and authenticated before using critical applications related to Attribute Certificate management.

f) AA personnel shall be accountable for their activities, for example by retaining event logs (see clause 7.4.11).

g) Sensitive data shall be protected against being revealed through re-used storage objects (e.g. deleted files) being accessible to unauthorized users.

NOTE 3: Sensitive data includes registration information.

h) The AA shall ensure that local network components (e.g. routers) are kept in a physically secure environment and their configurations periodically audited for compliance with the requirements specified by the AA.

i) Continuous monitoring and alarm facilities shall be provided to enable the AA to detect, register and react in a timely manner upon any unauthorized and/or irregular attempts to access its resources.

NOTE 4: This may use, for example, intrusion detection systems, access control monitoring and alarm facilities.

Attribute Certificate acquisition service

j) Attribute Certificate acquisition service application shall enforce access controls on subjects' attempts to obtain ACs.

Dissemination

k) Dissemination application shall enforce access control on attempts to add or delete Attribute Certificates and modify other associated information.

Revocation management

l) Revocation management application shall enforce access control to prevent unauthorized attempts to activate or prevent Attribute Certificates functions.

Revocation status provision

m) Revocation status provision application shall enforce access control on attempts to modify revocation status information.

7.4.7 Trustworthy Systems deployment and maintenance

The AA shall use trustworthy systems and products that are protected against modification.

In particular:

AA General

a) An analysis of security requirements shall be carried out at the design and requirements specification stage of any systems development project undertaken by the AA or on behalf of the AA to ensure that security is built into IT systems.

b) Change control procedures shall exist for releases, modifications and emergency software fixes for any operational software.

7.4.8 Business continuity management and incident handling

The AA shall ensure that in the event of a disaster, including compromise of the AA's private signing key, operations are restored as soon as possible.

In particular:

AA General

AA key compromise

a) The AA's business continuity plan (or disaster recovery plan) shall address the compromise or suspected compromise of a AA's private signing key as a disaster.

Revocation status

b) In the case of AA private signing key compromise the AA shall as a minimum provide the following undertakings:

- inform all subscribers, relying parties and AGAs with which it has agreements or other forms of established relations of the compromise;
- indicate that Attribute Certificates and revocation status information issued using this AA key may no longer be valid.

NOTE: The public key certificate corresponding to the compromised AA private key shall be revoked, thus the validation path of any AC issued by the AA and pointing to the mentioned PKC will no longer be valid.

7.4.9 AA termination

The AA shall ensure that potential disruptions to subscribers and relying parties are minimized as a result of the cessation of the AA's services. The AA shall ensure continued maintenance of records required to provide evidence of certification for the purposes of legal proceedings.

In particular:

AA General

a) Before the AA terminates its services the following procedures shall be executed as a minimum:

- the AA shall inform all subscribers, subjects, relying parties, AGAs and other entities with which it has agreements or other form of established relations;

NOTE: The AA is not required to have a prior relationship with relying parties.

- the AA shall terminate all authorization of subcontractors to act on behalf of the AA in the performance of any functions related to the process of issuing Attribute Certificates;

- the AA shall perform necessary undertakings to transfer obligations for maintaining registration information (see clause 7.2.1) and event log archives (see clause 7.4.11) for their respective period of time as indicated to the subscriber and relying party (see clause 7.2.3.1);

- the AA shall destroy, or withdraw from use, its private keys, as defined in clause 7.3.5.

b) The AA shall have an arrangement to cover the costs to fulfil these minimum requirements in case the AA becomes bankrupt or for other reasons is unable to cover the costs by itself.

c) The AA shall state in its practices the provisions made for termination of service. This shall include:

- the notification of affected entities;

- the transfer of its obligations to other parties;

- the handling of the revocation status for unexpired Attribute Certificates that have been issued.

d) The AA shall continue to observe data protection and confidentiality conditions applying to its operations with regard to the issuance of ACs. In particular attribute and Attribute Certificate databases shall remain confidential and shall only be disclosed to designated recipients that fulfil the same service conditions of confidentiality and data protection as the terminating CA.

7.4.10 Compliance with Legal requirements

The AA shall ensure compliance with legal requirements.

In particular:

AA General

a) Records shall be protected from loss, destruction and falsification. Some records may need to be securely retained to meet statutory requirements, as well as to support essential business activities (see clause 7.4.11).

b) The AA shall ensure that the requirements of the European data protection Directive [3] as implemented through national legislation, are met.

c) Appropriate technical and organizational measures shall be taken against unauthorized or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

d) The information that users contribute to the AA shall be protected from disclosure without the user's agreement, a court order or other legal authorization.

7.4.11 Recording of information concerning Attribute Certificates

The AA shall ensure that all relevant information concerning an Attribute Certificate is recorded for an appropriate period of time, in particular for providing evidence of certification for the purposes of legal proceedings.

NOTE 1: Records concerning Attribute Certificates include registration information (see clause 7.2.1) and information concerning significant AA environmental, key management and Attribute Certificate management events.

In particular:

General

a) The confidentiality and integrity of current and archived records concerning Attribute Certificates shall be maintained.

b) Records concerning Attribute Certificates shall be completely and confidentially archived in accordance with disclosed business practices.

c) Records concerning Attribute Certificates shall be made available if required for the purposes of providing evidence of certification for the purpose of legal proceedings. The subject, and within the constraints of data protection requirements (see clause 7.4.10 b)) the subscriber, shall have access to registration and other information relating to the subject.

NOTE 2: This may be used, for example, to support the link between the Attribute Certificate, the subject's public key certificate it relates to, and, where applicable, the subject.

d) The precise time of significant AA environmental, key management and certificate management events shall be recorded.

NOTE 3: It is recommended that the AA states in its practices the accuracy of the clock used in timing of events, and how this is accuracy ensured.

e) Records concerning Attribute Certificates shall be held for a period of time as appropriate for providing necessary legal evidence in support of electronic signatures.

NOTE 4: The duration of the record retention period is difficult to pinpoint, and requires weighting the need for reference to the records against the burden of keeping them. The records could be needed at least as long as a transaction relying on a valid certificate can be questioned. For most transactions, statutes of limitation will eventually place a transaction beyond dispute. However, for some transactions such as real property conveyances, legal repose may not be realized until after a lengthy time elapses, if ever.

NOTE 5: Where differing periods of times are applied to Attribute Certificates being used for different purposes, they shall be clearly identified and they should have different specific Attribute Certificate policy identifiers. Where differing periods are applied to different parts of the registration and event log records, this shall be indicated to the subscriber and relying party as specified in clause 7.1.

f) The events shall be logged in a way that they cannot be easily deleted or destroyed (except after having been transferred to long term media) within the period of time that they are required to be held.

NOTE 6: This may be achieved, for example, through the use of write only media, a record of each removable media used and the use of off site backup.

g) The specific events and data to be logged shall be documented by the AA.

Registration

h) The AA shall ensure all events relating to registration including requests for Attribute Certificate renewal, are logged.

i) The AA shall ensure that all registration information, including the following, is recorded:

- type of document(s) presented by the applicant to support registration, including the proof of possession of the private key corresponding to the related public key certificate;
- record of unique identification data, numbers, or a combination thereof (e.g. applicant's drivers license number) of identification documents, if applicable;
- storage location of copies of applications and identification documents, including the signed subscriber agreement (see clause 7.2.1 i));
- any specific choices in the subscriber and subject agreement (e.g. consent to publication of Attribute Certificate);
- identity of entity accepting the application;
- methods used to validate attribute requests and, if applicable, identification documents;
- name of receiving AA and/or submitting Registration Authority, if applicable.

j) The AA shall ensure that privacy of subject information is maintained.

Attribute Certificate generation

k) The AA shall log all events relating to the life-cycle of AA keys and public key certificates.

NOTE 7: The responsibility of logging the AA public key certificate life-cycle related events is also on the CA that issues the AA PKC.

l) The AA shall log all events relating to the life-cycle of Attribute Certificates it issues.

Revocation management

m) The AA shall ensure that all requests and reports relating to ACs suspension and revocation, as well as the resulting action, are logged.

7.5 Organizational

The AA shall ensure that its organization is reliable.

In particular that:

AA general

a) Policies and procedures under which the AA operates shall be non-discriminatory.

b) The AA shall make its services accessible to all applicants whose activities fall within its declared field of operation.

c) The AA is a legal entity according to national law.

d) The AA has a system or systems for quality and information security management appropriate for the certification services it is providing.

e) The AA has adequate arrangements to cover liabilities arising from its operations and/or activities.

f) The AA has the financial stability and resources required to operate in conformity with this policy.

g) The AA employs a sufficient number of personnel having the necessary education, training, technical knowledge and experience relating to the type, range and volume of work necessary to provide certification services.

h) The AA has policies and procedures for the resolution of complaints and disputes received from customers or other parties about the provisioning of electronic trust services or any other related matters.

i) The AA has a properly documented agreement and contractual relationship in place where the provisioning of services involves subcontracting, outsourcing or other third party arrangements.

Attribute Certificate generation, revocation management

j) The parts of the AA concerned with Attribute Certificate generation and revocation management shall be independent of other organizations for its decisions relating to the establishing, provisioning and maintaining and suspending of services; in particular its senior executive, senior staff and staff in trusted roles, must be free from any commercial, financial and other pressures which might adversely influence trust in the services it provides.

k) The parts of the AA concerned with Attribute Certificate generation and revocation management shall have a documented structure which safeguards impartiality of operations.

8 Framework for the definition of other Attribute Certificate policies

This clause provides a general framework for other policies for AAs. An AA may claim conformance to this general framework as defined in clause 8.2. In general terms this requires conformance to the requirements in clauses 6 and 7 excluding those listed in clause 8.2, if applicable.

8.1 Attribute Certificate policy management

The AA shall ensure that the attribute certificate policy is effective.

In particular:

a) There shall be a body (e.g. a policy management authority) with final authority and responsibility for specifying and approving the attribute certificate policy.

b) A risk assessment shall be carried out to evaluate business requirements and determine the security requirements to be included in the attribute certificate policy for all the areas identified above.

c) Attribute certificate policy(s) shall be approved and modified in accordance with a defined review process, including responsibilities for maintaining the attribute certificate policy.

d) A defined review process shall exist to ensure that the attribute certificate policies are supported by the Attribute Certification Practices Statement (ACPS).

e) The AA shall make available the attribute certificate policies supported by the AA to all appropriate subscribers and relying parties.

f) Revisions to attribute certificate policies supported by the AA shall be made available to subscribers and relying parties.

g) The attribute certificate policy shall incorporate, or further constrain, all requirements identified in clauses 6 and 7 with the exclusions indicated below. In the case of any conflict, the requirements of the present document prevail.

a) A unique object identifier shall be obtained for the attribute certificate policy of the form required in ITU-T Recommendation X.509 [2].

8.2 Exclusions for AC not issued to the public

Attributes Certificates not issued to the public need not apply the following policy requirements:

NOTE: An AA is not considered to be issuing attributes certificates to the public if the attribute certificates are restricted to uses governed by voluntary agreements under private law among participants.

a) Liability as defined in clause 6.3.

b) Independence of providers of certificate generation and revocation management services as specified in clauses 7.5 j) and k).

c) Public dissemination of attribute certificates as specified in clause 7.3.5 f).

d) Public availability of revocation status information as specified in clause 7.3.6 k).

8.3 Additional requirements

Subscribers and relying parties shall be informed, as part of implementing the requirements defined in clause 7.3.4:

a) If the policy is not for public use and whether exclusions identified in clause 8.2 apply.

b) The ways in which the specific policy adds to or further constrains the requirements of the policies as defined in the present document.

8.4 Conformance

The AA shall only claim conformance to the present document and the applicable attribute certificate policies:

a) if the AA claims conformance to an identified attribute certificate policy and makes available to subscribers and relying parties on request the evidence to support the claim of conformance; or

b) if the AA has been assessed to be conformant to an identified attribute certificate policy by an independent party.

A conformant AA must demonstrate that:

c) it meets its obligations as defined in clause 6.1;

d) it has implemented controls which meet the requirements specified in clause 7, excluding those clauses specified in clause 8.2 if the AA is not providing a service to the public;

e) uses an attribute certificate policy which meets the requirements specified in clause 8.1.

Annex A (normative): Requirements for the format of Attribute Certificates

Attribute certificates must contain at least:

a) an indication that the Attribute Certificate is issued under one of the two Attribute Certificate Policies identified in clause 5.2.;

NOTE 1: An extension suitable to host the Attribute Policy OID is proposed to be specified in the IETF PKIX WG: Attribute Certificate Policy extension.

b) the identification of the certification-service-provider and the State in which it is established;

c) specific attributes of the subject as identified in the Qualified Certificate to which the AC is linked;

d) an unambiguous link to a Qualified Certificate;

e) an indication of the beginning and end of the period of validity of the Attribute Certificate;

f) a unique serial number of the Attribute Certificate;

NOTE 2: This number does not need to be sequential, but must be unique for the certification-service-provider that has issued it.

g) the advanced electronic signature of the certification-service-provider issuing it.

Annex B (informative): Liability assertions

For CSPs issuing ACs within a closed user group the principle of contractual freedom (party autonomy) applies and thus liability clauses are only addressed through agreement under private law.

For CSPs issuing ACs to the public, a primary liability provision in Directive 1999/93/EC [1] is included in Recital 22, which links the liability of an AA with member state law. This recital reads: 'certification-service-providers providing certification services to the public are subject to national rules regarding liability'.

No other liability requirements for AAs issuing ACs (or certification-service-providers issuing attribute certificates) to the public are stated in Directive 1999/93/EC [1].

National rules regarding liability must be considered not only for the member state where the AA is established but also for the member states where the ACs are allowed to be used.

With regard to Directive 1999/93/EC [1], the question of CSPs issuing attribute certificates that are linked to qualified certificates is whether these CSPs carry a degree of liability than is lower, equivalent or higher to CAs issuing Qualified Certificates that include attributes. There is an implicit expectation for a level similar to the level prescribed in Article 6.

Article 6 stipulates the liability conditions for CSPs issuing qualified certificates. The provisions of Article 6 could be projected to CSPs issuing attribute certificates with regard to the following requirements, namely:

> Unless the CSP proves that he has not acted negligently, the CSP is liable for damage caused to any entity or legal or natural person who reasonably relies on the certificate:
>
> – as regards the accuracy at the time of issuance of all information contained in the ~~qualified~~ certificate;
> – for failure to register revocation of the certificate.
>
> The CSP shall not be liable for damage arising from use of a ~~qualified~~ certificate which exceeds the limitations placed on it, when these limitations are recognizable to third parties, i.e.:
>
> – the limitations on the use of that certificate, and
> – the limit on the value of transactions for which the certificate can be used.

With regard to potential liability for inaccurate information listed in an attribute certificate may relate to the subscriber (which may be an Attribute Granting Authority) and/or to the Attribute Authority itself. If the AA can prove that has not acted negligently when verifying the information then it is not liable for the damages, but the subscriber then can be.

With regard to the failure of registering the suspension or revocation of an AC at the request of the subject or the subscriber (which may be an Attribute Granting Authority), the Attribute Authority issuing attribute certificates that are linked to qualified certificates is likely to incur liability much like any other CSP that registers revocations and or suspension requests of qualified certificates.

With regard to the limitations on the use of an attribute certificate or to the limit on the value of transactions for which the certificate can be used, this implicitly means that the CSP is liable when the attribute certificate has been used for an allowed use or below a given amount of money.

Under some EU member states laws in order for negligence to give rise to damages, the negligence must be the cause of the loss. Other EU member states require that loss be linked to a cause which prevailed in the contractual relationship in order for damage to be proved. Any inaction of the relying party to fulfil its own obligation will constitute a reason for the CA to limit its own liability towards such party.

It might be difficult to offer an unlimited warranty for relying parties with which the CSP does not even have a contract with. If the liability is limited, it might then be difficult to state the criteria to be applied.

To limit its liability, an Attribute Authority might opt for a warranty plan supported by a maximum value per transaction, an aggregate limit or a variation thereof, for example:

- each claim is handled independently, but no individual claim can exceed a warranty amount;
- the warranty will be aggregated, and once the value of fulfilled claims reaches the warranty amount, then no further claim will be fulfilled;
- the warranty will be aggregated, and once the time period to collect all the claims will be ended the maximum warranty amount will be divided among the claimants.

The CSP may also state a limit per AC or a limit per QC (irrespective of the number of ACs that have been issued).

None of these cases seems however to be easily applicable for large amounts of money, since (or if) the CSP is kept ignorant of the existence of every individual transaction.

Then, a limit for the time period to present a claim should be indicated.

Finally, it should be noted that all limitations of liability likely to prevail be documented and communicated to subscribers and relying parties by means of an ACPS or a document of similar scope.

Annex C (informative): Model AC disclosure statement

C.1 Introduction

The proposed model AC disclosure statement is designed for use by a AA issuing Attribute Certificates as a supplemental instrument of disclosure and notice. An AC disclosure statement may assist an AA to respond to regulatory requirements and concerns. Further, the aim of the model AC disclosure statement is to foster industry "self-regulation" and build consensus on those elements of an Attribute Certificate policy and/or attribute certification practice statement that require emphasis and disclosure.

Although Attribute Certificate policy and attribute certification practice statement documents are essential for describing and governing certificate policies and practices, many AC users, especially consumers, find these documents difficult to understand. Consequently, there is a need for a supplemental and simplified instrument that can assist AC users in making informed trust decisions. Consequently, an AC disclosure statement is not intended to replace an Attribute Certificate policy or attribute certification practice statement.

This annex provides an example of the structure for an AC disclosure statement, illustrating the harmonized set of statement types (categories) that would be contained in a deployed.

C.2 The PDS structure

The PDS contains a clause for each defined statement type. Each clause of a PDS contains a descriptive statement, which MAY include hyperlinks to the relevant certificate policy/certification practice statement sections.

Table C.1

Statement types	Statement descriptions	Specific Requirements of Attribute Certificate policy (see clause 7.1.1)
AA contact info	The name, location and relevant contact information for the AA	
Attribute Certificate type, validation procedures and usage	A description of each class/type of Attribute Certificate issued by the AA, corresponding validation procedures, and any restrictions on Attribute Certificate usage	Any limitations on its use Whether the policy is for Attribute Certificate issued to the public
Reliance limits	The reliance limits, if any	Indication that the Attribute Certificate is only for use with electronic signatures, the period of time which registration information and AA event logs (see clause 7.4.11) are maintained (and hence are available to provide supporting evidence)
Obligations of subscribers	The description of, or reference to, the critical subscriber obligations	The subscriber's obligations, as defined in clause 6.2
Attribute Certificate status checking obligations of relying parties	The extent to which relying parties are obligated to check Attribute Certificate status, and references to further explanation	Information on how to validate the Attribute Certificate, including requirements to check the revocation status of the Attribute Certificate, such that the relying party is considered to "reasonably rely" on the Attribute Certificate (see clause 6.3)
Limited warranty and disclaimer/Limitation of liability	Summary of the warranty, disclaimers, limitations of liability and any applicable warranty or insurance programs	Limitations of liability (see clause 6.4)
Applicable agreements, attribute certification practice statement, Attribute Certificate policy	Identification and references to applicable agreements, attribute certification practice statement, Attribute Certificate policy and other relevant documents	Attribute certificate policies being applied
Privacy policy	A description of and reference to the applicable privacy policy	NOTE: AAs under this policy are required to comply with the requirements of Data Protection Legislation
Refund policy	A description of and reference to the applicable refund policy	
Applicable law, complaints and dispute resolution	Statement of the choice of law, complaints procedure and dispute resolution mechanisms (anticipated to often include a reference to the International Chambers of Commerce's arbitration services)	The procedures for complaints and dispute settlements. The applicable legal system
AA and repository licenses, trust marks, and audit	Summary of any governmental licenses, seal programs; and a description of the audit process and if applicable the audit firm	If the AA has been certified to be conformant with specific Attribute Certificate policies, and if so through which scheme

Annex D (informative): Bibliography

TTP.NL Part 1: "Requirements and Guidance for the Certification of the Public Key Infrastructure of Certification Service Providers".

TTP.NL Part 2: "Requirements and Guidance for the Certification of Information Security Management of Certification Service Providers".

TTP.NL Part 3: "General Requirements and Guidance for the Accreditation of Certification Service Providers issuing Qualified Certificates".

BSI IT-Grundschutzhandbuch: "Bundesamt für Sicherheit in der Informationstechnik - IT-Grundschutzhandbuch Standard-Sicherheitsmaßnahmen", January 2000.

"Scheme approval profiles for Trust Service Providers". See http://www.tscheme.org/.

ISO/IEC 17799 (2000): "Information technology - Code of practice for information security management".

ITU-T Recommendation X.843|ISO/IEC 15945: "Information technology - Security techniques - Specification of TTP services to support the Application of Digital Signatures".

ITU-T Recommendation X.842|ISO/IEC 14516: "Information technology - Security techniques - Guidelines on the use and management of Trusted Third Party services".

ISO/IEC TR 13335-1 (1996): "Information technology - Guidelines for the management of IT Security - Part 1: Concepts and models for IT Security".

ISO/IEC TR 13335-2 (1997): "Information technology - Guidelines for the management of IT Security - Part 2: Managing and planning IT Security".

ISO/IEC TR 13335-3 (1998): "Information technology - Guidelines for the management of IT Security - Part 3: Techniques for the management of IT Security".

ISO/IEC TR 13335-4 (2000): "Information technology - Guidelines for the management of IT Security - Part 4: Selection of safeguards".

ISO/TS 17090-1. Health informatics - Public Key infrastructure. Part 1: Framework and overview.

ISO/TS 17090-2. Health informatics - Public Key infrastructure. Part 2: Certificate profile.

ISO/TS 17090-3. Health informatics - Public Key infrastructure. Part3: Policy Management of certification authority.

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

Directive 97/7/EC of the European Parliament and of the Council of 20 May 1997 on the protection of consumers in respect of distance contracts - Statement by the Council and the Parliament re article 6 (1) - Statement by the Commission re article 3 (1), first indent.

CEN Workshop Agreement 14172: "EESSI Conformity Assessment Guidance".

ETSI TR 102 041: "Signature policies report".

ETSI TR 102 044: "Electronic Signatures and Infrastructures (ESI); Requirements for role and attribute certificates"

IETF RFC 2527 (1999): "Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practices Framework".

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

IETF RFC 3280: "Internet X.509 Public Key Infrastructure – Certificate and CRL Profile". R.Housley, W. Ford, W. Polk, D. Solo. April 2002.

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

Attribute Certificate Policies Extension – draft-ietf-pkix-acpolicies-extn-01.txt

History

Document history		
V1.1.1	October 2003	Publication