



# **Certificate Practice Statement**

**of the  
Atos Trusted CA**

**Version 1.9.1**

**31.10.2018**

## 1 DOCUMENT ADMINISTRATION

### 1.1 Document control

Document-Nr.:	DED-CLE-1010	Owner:	Matthias Mönter
Version:	1.9.1	Document-Date:	31.10.2018
Status:	Final	Valid from:	31.10.2018

### 1.2 Version control

Version	Date	Section/ Page	Reason
1.2	01.10.2010	All	Creation
1.2.1	24.11.2010		Small changes
1.3	16.03.2011	All	Finalizing
1.3.1	04.04.2011		Small changes
1.3.2	04.05.2011	2.3, 5.9	Corrections after audit
1.4	16.12.2011	All	Changed company name to Atos
1.4.1	02.02.2012	4.2	Added IDN check
1.5	01.03.2012	2.1	Changed Policy Identifier
1.6	17.06.2013	All	Added DVCP and OVCP, Added CAB Req, Changed CA names to Atos
1.7	29.10.2013	4.2	Update clause 77
1.7.1	05.11.2013	4.2	Update clause 75/76
1.8	05.04.2016	All	Changes regarding mailbox certificates
1.8.1	30.06.2017	6.3	Changes in Personnel controls
1.8.2	19.08.2017	4.2	Update clause 7,57,60,77 and 256
1.8.3	30.01.2018	4.4, 7.1, 9.5	Update clause 87,194 and 266

1.9.0	31.05.2018	5.12	Change to ESTI EN 319 411-1 Update clause 1, 7, 9, 79, 107, 108, 160, 134, 171, 194, 235, 239, 259
1.9.1	31.10.2018	4.2, 5.1, 5.6, 10.4	Change to DSGVO Update clause 77, 92, 114, 281, 283, 284

**Table 1 – Document history**

## Contents

<b>1</b>	<b>DOCUMENT ADMINISTRATION .....</b>	<b>2</b>
1.1	Document control .....	2
1.2	Version control.....	2
<b>2</b>	<b>INTRODUCTION .....</b>	<b>8</b>
2.1	Document name and identification.....	9
2.2	PKI participants .....	9
2.3	Certificate usage .....	11
2.4	Policy administration.....	11
2.5	Definitions and acronyms .....	13
<b>3</b>	<b>PUBLICATION AND REPOSITORY RESPONSIBILITIES .....</b>	<b>15</b>
3.1	Repositories .....	15
3.2	Publication of certification information.....	15
3.3	Time or frequency of publication .....	16
3.4	Access controls on repositories.....	17
<b>4</b>	<b>IDENTIFICATION AND AUTHENTICATION .....</b>	<b>18</b>
4.1	Naming .....	18
4.2	Initial identity validation .....	18
4.3	Identification and authentication for re-key requests .....	21
4.4	Identification and authentication for revocation request.....	22
<b>5</b>	<b>CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS.....</b>	<b>23</b>
5.1	Certificate application .....	23
5.2	Certificate application processing .....	23
5.3	Certificate issuance .....	23
5.4	Certificate acceptance .....	24
<b>5.5</b>	<b>Key pair and certificate usage .....</b>	<b>25</b>

5.6	Certificate renewal .....	26
5.7	Certificate re-key .....	26
5.8	Certificate modification .....	26
5.9	Certificate revocation and suspension.....	27
5.10	Certificate status services .....	28
5.11	End of subscription.....	29
5.12	Key escrow and recovery .....	29
6	<b>FACILITY, MANAGEMENT AND OPERATIONAL CONTROLS.....</b>	<b>30</b>
6.1	Physical controls .....	30
6.2	Procedural controls .....	31
6.3	Personnel controls .....	32
6.4	Audit logging procedures.....	34
6.5	Records archival .....	35
6.6	Key changeover.....	35
6.7	Compromise and Disaster Recovery .....	35
6.8	CA or RA termination .....	36
7	<b>TECHNICAL SECURITY CONTROLS .....</b>	<b>37</b>
7.1	Key pair generation and installation .....	37
7.2	Private Key Protection and Cryptographic Module Engineering Controls.....	37
7.3	Other aspects of key pair management.....	38
7.4	Activation data.....	39
7.5	Computer security controls.....	39
7.6	Life cycle technical controls .....	40
7.7	Network security controls.....	41
7.8	Time-stamping .....	41
8	<b>CERTIFICATE, CRL, AND OCSP PROFILES.....</b>	<b>42</b>

8.1	Certificate profile .....	42
8.2	CRL profile .....	42
8.3	OCSP profile .....	43
9	COMPLIANCE AUDIT AND OTHER ASSESSMENTS .....	44
9.1	Frequency or circumstances of assessment .....	44
9.2	Identity/qualifications of assessor .....	44
9.3	Assessor's relationship to assessed entity .....	44
9.4	Topics covered by assessment .....	44
9.5	Extern Requirements.....	44
9.6	Actions taken as a result of deficiency.....	44
9.7	Communication of results.....	44
10	OTHER BUSINESS AND LEGAL MATTERS .....	45
10.1	Fees .....	45
10.2	Financial responsibility .....	45
10.3	Confidentiality of business information .....	45
10.4	Privacy of personal information.....	46
10.5	Intellectual property rights .....	46
10.6	Representations and warranties .....	46
10.7	Disclaimers of warranties .....	46
10.8	Limitations of liability.....	46
10.9	Indemnities.....	47
10.10	Term and termination .....	47
10.11	Individual notices and communications with participants.....	47
10.12	Amendments .....	47
10.13	Dispute resolution provisions .....	47
10.14	Governing law .....	47



<b>10.15</b>	<b>Compliance with applicable law.....</b>	<b>47</b>
<b>10.16</b>	<b>Other provisions.....</b>	<b>48</b>
<b>11</b>	<b>Annex - Referenced Documents.....</b>	<b>49</b>

## 2 INTRODUCTION

- 1 This document on hand contains the Certificate Practice Statement (CPS) of the Atos Trusted CA. The PKI-hierarchy consists of for three subordinate CA types and a Root CA for different purposes:
  1. Atos Root CA
  2. Atos SSL Server CA
  3. Atos Client CA
  4. Atos CodeSigning CA
- 2 This CPS describes the organisation, the processes and the security level of all Public Key Infrastructure (PKI) services provided by the Atos Trusted CA. It is intended that this CPS covers the requirements as specified by the ETSI specification EN 319 411-1 “Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates” [ETSI\_319411]. The structure of this CPS is equivalent to the structure of RFC3647. The RFC3647 suggests an optional Certificate Policy document (CP). A CP is not implemented for the Atos Trusted CA because all relevant information is part of this CPS.
- 3 This document has the following attributes:
  - Definition of policy requirements on operation and management practices.
  - Goal: Subscribers to gain confidence in the applicability of certificates in support of cryptographic algorithms.
  - Basic level: Normalized Certificate Policy (NCP), providing a level of quality the same as that offered by qualified certificates, without being tied to the legal constraints of the Electronic Signature Directive (1999/93/EC). No secure user device (SUD).
- 4 As Service Provider adopting the ETSI standard EN 319 411-1 as a framework for this Atos Trusted CA certificate practice statement Atos makes the explicit choice between the three alternatives (LCP, NCP, NCP+, DVCP, OVCP) and states clearly which alternative was adopted:

NCP, DVCP and OVCP for Atos SSL Server CANCP, DVCP and OVCP for Atos SSL Server CA

NCP, DVCP and OVCP for Atos Client CA and

NCP, DVCP and OVCP for Atos CodeSigning CA.



- 5 Certificates issued by the Atos Trusted CA include a certificate policy identifier which can be used by relying parties in determining the certificates suitability and trustworthiness. The identifier for each CA is declared in the following section.

### 2.1 Document name and identification

- 6 This document is named: Certificate Practice Statement “Atos Trusted CA”, Version 1.9.1, Date 31.10.2018.
- 7 This document follows the requirements as specified in statement 5 and 266. And therefore the appropriate policy identifier is included into each certificate for the three subordinate CA types and the Root CA:

Root CA	Identifier
Atos Root CA	iso(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) atos(6189) Atos Origin Trustcenter(3) Atos Origin Trusted Root CA(4) cps(1) Root(1)
Subordinate CA	Identifier
Atos SSL Server CA	iso(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) atos(6189) trustcenter(5) trusted-root(1) policy-identifiers(1) cps(1) Server(3)
Atos Client CA	iso(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) atos(6189) trustcenter(5) trusted-root(1) policy-identifiers(1) cps(1) Client(1)
Atos CodeSigning CA	iso(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) atos(6189) trustcenter(5) trusted-root(1) policy-identifiers(1) cps(1) CodeSigning(2)

### 2.2 PKI participants

- 8 No constraints are placed on the user community. The following subsections describe the type of entities that fill in the roles of participants within a PKI.

## 2.2.1 Certification Authorities

9 This CPS covers those three subordinate CA and the Root CA which are introduced above:

- Atos Root CA
- Atos SSL Server CA
- Atos Client CA
- Atos CodeSigning CA

10 The subsections below describe their purpose.

### 2.2.1.1 Atos SSL Server CA

11 The purpose of the Atos SSL Server CA is to issue end certificates for SSL applications. These end certificates can be used by applications using an SSL client server communication. If in any subsequent section a CPS statement refers only to this CA, the corresponding section is marked with: [SSL-CA].

### 2.2.1.2 Atos Client CA

12 The purpose of the Atos Client CA is to issue end-user certificates for S/MIME applications. These end-user certificates can be used by applications like emailing tools or for client authentication. If in any subsequent section a CPS statement refers only to this CA, the corresponding section is marked with: [Client-CA].

### 2.2.1.3 Atos CodeSigning CA

13 The purpose of the Atos CodeSigning CA is to issue certificates for software products for proving their integrity. If in any subsequent section a CPS statement refers only to this CA, the corresponding section is marked with: [CodeSigning-CA].

## 2.2.2 Registration Authorities

14 The registration authority performs the identification and authentication of end certificate applicants. Subordinate organizations within or a dedicated group of authorized employees of a larger organization can act as RAs for the CA serving the entire organization, but RAs may also be external to the CA.

## 2.2.3 Subscribers

15 [SSL-CA] The subscribers are organizational entities, which apply a SSL certificate.

16 [Client-CA] The subscribers are individual persons, who want to receive a Client certificate.

17 [CodeSigning-CA] The subscribers are organizational entities, which sign their software product with a CodeSigning certificate.

## 2.2.4 Relying parties

- 18 [SSL-CA] All users of web server pages using SSL certificates of the Atos SSL Server CA rely on the authenticity of the web server and the encryption of the connection.
- 19 [Client-CA] For the Atos Client CA the community of all subscribers is able to communicate via digitally signed or encrypted emails or use client authentication tools for a secure communication.
- 20 [CodeSigning-CA] Users of a software product signed with a certificate of the Atos CodeSigning CA rely on the authenticity of the originator of the software and the integrity of a software received.

## 2.2.5 Other participants

- 21 None

## 2.3 Certificate usage

- 22 The policies defined in the present document place constraints on the applicability of the certificates.

### 2.3.1 [SSL-CA]

- 23 Authentication of a domain name and encryption of the communication channel.

### 2.3.2 [Client-CA]

- 24 The following items list the types of applications for which the issued Client certificates are suitable:
  - Digitally sign messages or files to confirm the authorship and enable to verify if the signed messages or files have not been changed or corrupted.
  - Digitally encrypt messages or files to keep them confidential.
  - Usage in client authentication tools for secure identification and authorization.

### 2.3.3 [CodeSigning-CA]

- 25 The following items list the types of applications for which the issued CodeSigning certificates are suitable:
  - Confirm the author of a software.
  - Enable to confirm that the software has not been changed or corrupted.

## 2.4 Policy administration

- 26 See section 1.1 "Document control", entry Source.

#### 2.4.1 Organization administering the document

27 See section 1.1 “Document control”, entry Owner.

#### 2.4.2 Contact person

28 See section 1.1 “Document control”, entry Document owner or <http://pki.atos.net>.

#### 2.4.3 Person determining CPS suitability for the policy

29 The Atos Trusted CA is responsible for determine CPS suitability for the policy.

#### 2.4.4 CPS approval procedures

30 As outlined in section 2 “INTRODUCTION” the three CAs covered by this document follow the denoted ETSI standard. The document on hand is the certification policy statement (CPS) describing the practices and procedures.

31 The conformance of the present CPS with the ETSI-requirements is demonstrated in every section of this document. At the beginning of each section the ETSI-requirements are shown, followed by statement of the CPS to fulfil the requirement.

32 The obligations of all external organizations supporting the CA services including the applicable policies and practices are identified in the PKI disclosure statement.

33 This CPS is made available to subscribers and relying parties together with other relevant documentation in the repository see section 3.1.

34 Other relevant documentation are:

- General Terms and Conditions for Services of Atos Information Technology GmbH
- Subscriber Agreement

35 Intended changes of the CPS are announced and the revised document is published after the appropriate approvement is made, see statement 36.

36 The CA has a high level management body with final authority and responsibility for approving the certification practice statement, see section 1.1 “Document control”, entry Owner. The approval process is repeated with every further change of the CPS.

37 The senior management of the CA, see section 1.1 “Document control”, entry Owner, is responsible for ensuring that the certification practices established to meet the applicable requirements specified in the present document are properly implemented.

38 The Atos Trusted CA defines a review process for certification practices including responsibilities for maintaining the certification practice statement, see description in section 1.2.

39 This document specifies the algorithms and parameters employed in section 7.2, especially in statements 196, 198, 198 and 204.

## 2.5 Definitions and acronyms

### 2.5.1 Definitions

#### 2.5.1.1 Definitions:

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

**attribute:** information bound 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

**certificate:** public key of a user, together with some other information, rendered un-forgable by encipherment with the private key of the certification authority which issued it

**certificate policy:** named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements (the certification practice statement on hand acts as the certificate policy)

**Certificate Revocation List (CRL):** signed list indicating a set of certificates that are no longer considered valid by the certificate issuer

NOTE: See ITU-T Recommendation [X.509].

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

**certification practice statement:** statement of the practices which a certification authority employs in issuing managing, revoking, and re-keying certificates

NOTE: See RFC 3647 [12].

**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

**extended normalized certificate policy:** normalized certificate policy requiring use of a secure user device

**lightweight certificate policy:** certificate policy which offers a quality of service less onerous than the qualified certificate policy as defined in TS 101 456 [15]

**normalized certificate policy:** certificate policy which offers a quality of service equivalent to the qualified certificate policy as defined in TS 101 456 [15]

**relying party:** recipient of a certificate who acts in reliance on that certificate and/or digital signatures verified using that certificate, NOTE: See RFC 3647 [12].

**secure user device:** device which holds the user's private key, protects this key against compromise and performs signing or decryption functions on behalf of the user

**subject:** entity identified in a certificate as the holder of the private key associated with the public key given in the certificate

**subscriber:** entity subscribing with a Certification Authority on behalf of one or more subjects,  
NOTE: The subject may be a subscriber acting on its own behalf.

### 2.5.1.2 Additional definitions

**Online Certificate Status Protocol (OCSP):** Internet protocol used for obtaining the revocation status of an X.509 digital certificate.

**Lightweight Directory Access Protocol (LDAP):** Application protocol for querying and modifying directory services running over TCP/IP.

### 2.5.2 Abbreviations

41 For the present document, the following abbreviations apply:

#### 2.5.2.1 Abbreviations:

CA	Certification Authority
CRL	Certificate Revocation List
CSP	Certification Service Provider
DVCP	Domain Validation Certificate Policy
LCP	Lightweight Certificate Policy
NCP	Normalized Certificate Policy
NCP+	Extended Normalized Certificate Policy
OVCP	Organizational Validation Certificate Policy
PDS	PKI Disclosure Statement
PKI	Public Key Infrastructure
RA	Registration Authority

#### 2.5.2.2 Additional abbreviations

IDN	Internationalized Domain Name
LDAP	Lightweight Directory Access Protocol
OCSP	Online Certificate Status Protocol

### 3 PUBLICATION AND REPOSITORY RESPONSIBILITIES

#### 3.1 Repositories

- 42 Atos publishes certificates it issues to subscribers, subjects and relying parties in the repository. The repository maintains an Online Certificate Status Protocol (OCSP) service, a certificate revocation list (CRL) and a Lightweight Directory Access Protocol (LDAP) server and the relevant documents as described in statements 32 through 36.
- 43 [SSL-CA] Upon generation, the subscriber gets a notice via email, that the complete and accurate certificate is issued and can be downloaded by the subscriber. If the subscriber has requested this the certificate is published within the LDAP service of the repository during its validity period.
- 44 [Client-CA] Upon generation, the subscriber gets a notice via email, that the complete and accurate certificate is issued and can be downloaded by the subscriber. If the subscriber has requested this the certificate is published within the LDAP service of the repository during its validity period.
- 45 [CodeSigning CA] Upon generation, the subscriber gets a notice via email, that the complete and accurate certificate is issued and can be downloaded by the subscriber. If the subscriber has requested this the certificate is published within the LDAP service of the repository during its validity period.
- 46 The Subscriber Agreement for each CA of the Atos Trusted CA can be downloaded from the repository. For details on the content of the Subscriber Agreement see section 3.2, statements 48 and 49.
- 47 For a given certificate the applicable Subscriber Agreement is readily identifiable and downloadable within the repository.

#### 3.2 Publication of certification information

- 48 The Subscriber Agreements of the CAs of the Atos Trusted CA are introduced in statement 46 to be downloadable within the CA's repository, see section 3.1.
- 49 They are refined in statements 46 and 47 and have the following content:
- Naming of the certificate practice statement being applied
  - statement as to whether the certificates are issued to the public
  - whether the use of any particular product, application or device is necessary for the purposes of applying the key-pair associated with the certificate being issued
  - limitations on the key pairs' use
  - subscriber's obligations as defined in section 5.5.

- information on how to validate the certificate, including requirements to check the revocation status of the certificate, such that the relying party is considered to "reasonably rely" on the certificate,
- any limitations of liability, including the purposes/uses for which the CA accepts (or excludes) liability;
- the period of time which registration information (see section 4.2) is retained;
- the period of time which CA event logs (see section 6.4) are retained;
- procedures for complaints and dispute settlement;
- the applicable legal system; and
- through which scheme the CA has been assessed to be conformant with the identified certificate policy.

50 The Subscriber Agreement of each CA can be downloaded from the repository, which is based on a web server.

51 Certificates are made available as necessary to subscribers, subjects and relying parties.

52 Certificates are available for retrieval in only those cases for which the subject's consent has been obtained.

53 The public revocation status information is publicly and internationally available, since the CA is issuing certificate to the public. For more details see statement 42.

### 3.3 Time or frequency of publication

54 The general availability of certificates is specified in statements 51 and 52.

55 The temporal availability for the information identified is

**24 hours per day, 7 days per week.**

56 Upon system failure, service or other factors which are not under the control of the CA, the CA applies best endeavours to ensure that this information service is not unavailable for longer than

**3 working days.**

57 Since Certificate Revocation Lists (CRLs) are used, see statement 42, these are published at least every 24 hours for Intermediate CAs. For the Root CA a new CRL will be generated after revocation of an Intermediate CA or at least every 12 month.

58 Revocation status information is available 24 hours per day, 7 days per week.



- 59 Upon system failure, service or other factors which are not under the control of the CA, the CA makes best endeavours to ensure that this information service is not unavailable for longer than 1 working day.
- 60 Revocation status information is provided, using online certificate status service (OCSP) for all Intermediate CAs and by distribution of CRLs through a repository, see statement 42.

### 3.4 Access controls on repositories

- 61 Access to the Atos Trusted CA system is limited to properly authorized individuals. A role-based access control is performed for the repository on OCSP, CRL and LDAP, see statement 42:
- 62 Changes to OCSP, CRL and LDAP are only allowed with CA internal access under a CA specific role, which authorizes writing access to the services.

## 4 IDENTIFICATION AND AUTHENTICATION

### 4.1 Naming

63 This section specifies the naming and identification of the subscribers.

64 The certificates include the name of the subject, which shall be identified as such:

- [SSL-CA] The identifier of the device in form of an internet domain name which will apply the SSL certificate.
- [Client-CA] The full name of the person or functional mailbox identity, who wants to receive a Client certificate under the Atos Client CA.
- [CodeSigning-CA] The full name of the organizational entity, who wants to sign software products with a CodeSigning certificate.

### 4.2 Initial identity validation

65 Section 5.1 describes who can submit a certificate application and how is the processing for certificate application. This section describes the identification and authentication procedures for the initial registration for each subject type. Section 5.4 describes the requirements for certificate acceptance.

66 The identity of an applicant is verified for the different CAs with different evidences:

- [SSL-CA]: Atos collects the necessary evidences for the verification of the subject's identity, requesting an Atos SSL Server CA certificate. More details see statement 77.
- [Client-CA]: Atos collects the necessary evidences either directly for the verification of the subject's identity, requesting an Atos Client CA certificate. Alternatively there exists a registration authority authorized by the CA and operating according to a contractual agreement which is offered to a specific group of subscribers. The registration authority collects the evidences for the verification of the subject's identity belonging to this group of subscribers. More details see statements 69, 73, 74 and 75.
- [CodeSigning-CA]: Atos collects the necessary evidences for the verification of the subject's identity, requesting an Atos CodeSigning CA certificate. More details see statement 76.

67 For all three CAs (Atos Client CA, Atos CodeSigning CA, Atos SSL Server CA) of the Atos Trusted CA the roles "subscriber" and "subject" are assigned as follows:

- [SSL-CA]: Computer system (subject) performing automated commerce on behalf of the owner organization (subscriber)
- [Client-CA]: Individual persons (subjects) using the certificate for electronic communication on behalf of themselves or the subject's organization (subscriber),

- [CodeSigning-CA]: Software (subject) built on behalf of the organization (subscriber)

- 68 Atos Trusted CA's verification policy only requires the capture of evidence of identity sufficient to satisfy the requirements of the intended use of the certificate.
- 69 [Client-CA]: For the Atos Client CA all subjects are natural persons or functional mailbox identities. The identification always takes place with directly or indirectly physical assurance of the subject or the subscriber in case of functional mailbox identity:
- 70 Either the subject introduces him or herself directly at the certification authority.
- 71 Alternatively – if there is a contract for a group of subscribers, of which the specific subject is a member of - the subject appears in person at the appropriate registration authority. An employee of the registration authority assures in written or electronic form that the subject requesting a certificate has the claimed identity. In this case the evidence is checked indirectly against a physical person.
- 72 Alternatively – as another way of evaluating indirectly the identity of a person –documentation is presented for registration which was acquired as the result of an application requiring physical presence.
- 73 [Client-CA]: For natural persons requesting a certificate the identity is evaluated by personal identification, via direct or indirect evaluation. The requester appears in person with a valid identity card or passport at the certification authority or if there is a contractual frame to do so at the registration authority.

Alternatively: The requester presents a documentation for registration which was acquired as the result of an application requiring physical presence, e.g. for the identification and authentication of natural persons in Germany the PostIdent service of Deutsche Post AG can be used to produce such a documentation. In both cases of evaluation evidence is provided of:

- full name (including surname and given names consistent with the applicable law and national identification practices);
  - date and place of birth, reference to a nationally recognized identity document, or other attributes which may be used to, as far as possible, distinguish the person from others with the same name.
- 74 [Client-CA]: A legal entity requesting a certificate is identified and authenticated for the first time via appearance in person of at least one natural person acting as representative for the entity. Identification and authentication of the representative/s is/are performed as described above for a natural person including the indirect evaluation.
- 75 [Client-CA]: In addition to the personal identification and authentication a representative has to provide:

- Evidence that he or she is authorized by the legal entity to request a certificate (the name of the person is included in the certificate as the subject) for it
- Evidence of the existence of the legal entity in form of
  - an excerpt from the commercial register (certificate of registration, in Germany: Handelsregisterauszug), or
  - a registration of a Top Level Domain (which can be found for Germany with [www.denic.de](http://www.denic.de) or international with [www.iana.org](http://www.iana.org)) inclusive verification for homographic IDNs
- If an email address is present in the certificate, evidence by a challenge-response mechanism that he or she owns or controls the email address.

76 [CodeSigning-CA]: A legal entity requesting a certificate is identified and authenticated for the first time via the subject's name of the certificate:

- The legal's entity full name or a verified tradename matches the subject's name or organization name in the certificate.
- The legal entity is authorized by the organisation given in the certificate.
- The existence of the legal entity in form is evident with either
  - an excerpt from the commercial register (certificate of registration, in Germany: Handelsregisterauszug), or
  - a registration as Top Level Domain (which can be found for Germany with [www.denic.de](http://www.denic.de) or international with [www.iana.org](http://www.iana.org)) inclusive verification for homographic IDNs, where the registered full name of the legal entity is registered and it matches the subject's full name.

77 [SSL-CA]: A legal entity, represented by a device or system, which requests a certificate is identified and authenticated for the first time via the subject of the certificate and the registration of an Internet Domain name:

- The legal entity is the Domain Name Registrant or has control over the Internet Domain Names given in the certificate. Following validation methods apply:
  - Constructed Email to Domain Contact: Atos Trusted CA confirms the Applicant's control over the FQDN by sending an email to one or more addresses created by using "admin", "administrator", "webmaster", "hostmaster", or "postmaster" followed by the @-sign, followed by the Domain Name, including a Random Value in the email, and receiving a confirming response utilizing the Random Value. Each random value will be unique and valid only 30 days for confirmation.

- Agreed-Upon Change to Website: The Applicant has to confirm the control over the FQDN by adding a Random Value to a website under a well-known path registered with IANA for domain validation. The Random Value is provided by Atos Trusted CA, unique and valid only 30 days for confirmation.

- DNS Change: The Applicant has to confirm the control over the FQDN by presence of a Random Value or Request Token for either in a DNS CNAME, TXT or CAA record. The Random Value or Request Token is provided by Atos Trusted CA, unique and valid only 30 days for confirmation.

- The legal's entity full name or a verified tradename matches the subject's organization name in the certificate.
- The existence of the legal entity is evident from an excerpt from the commercial register (certificate of registration, in Germany: Handelsregisterauszug).
- Atos Trusted CA will check Certificate Authority Authorization (CAA) records for every certificate application. The check will be done for each Internet Domain Name in the subjectAlt-Name extension of the certificate, according to the procedure in RFC 6844. Atos Trusted CA will allow the Issuer Domain Names "atos.net " as permission to issue.

78 Atos Trusted CA records for all three CAs all the information necessary to verify the subject's identity and, if applicable, any specific attributes of the subject, including any reference number on the documentation used for verification, and any limitations on its validity.

79 The subscribers provide a physical address, or other attributes, which describe how the subscriber can be contacted. The subscriber and TSP organization entity shall be separate entities.

80 The subjects prove possession of the companion private key for the public key being registered by digitally signing the certificate request.

#### 4.3 Identification and authentication for re-key requests

81 The Atos Trusted CA ensures that re-certification requests for certificates issued to a subject who has previously been registered with the same CA (including: certificate re-key following revocation or prior to expiration, or update due to change to the subject's attributes) are complete, accurate and duly authorized.

82 Re-certification requests relating to

- re-keying following revocation or prior to expiration, or
- certification modification (update due to change to the subject's attributes)

are authenticated and checked to be from an authorized source.

83 The Atos Trusted CA performs the following checks for identification and authentication for a re-certification request:

- the re-certification request is digitally signed with the private key whose companion subscriber/subject wants a new (second, third, etc.) certificate, or
- the requester can be identified as the subject belonging to that certificate which shall be re-certified. The identification follows the requirements as described for the initial identity validation for natural persons.

84 If any of the Atos Trusted CA documents have changed, these are communicated to the subscriber and agreed to in accordance, similar to statements 89 and 90.

85 If any certified names or attributes have changed, or the previous certificate has been revoked, the registration information is verified, recorded, agreed to by the subscriber in accordance with sections 4.2 "Initial identity validation", 5.7 "Certificate re-key" and 5.8 "Certificate modification".

#### 4.4 Identification and authentication for revocation request

86 This section describes the practices and procedures concerning the identification and authentication for revocation requests. Practices and procedures concerning the general revocation and suspension requirements are described in section 5.9 and the specific ones on certificate status information in section 5.10.

87 Requests and reports relating to revocation are authenticated, checked to be from an authorized source. The Atos Trusted CA performs the following checks for identification and authentication for a revocation request:

- Revocation request is digitally signed with the private key whose companion public key needs to be revoked, or
- the requester names the revocation passphrase, which was agreed upon the "Certificate application processing", see section 5.2, or
- the requester appears in person and can be identified as the subject belonging to that certificate whose companion public key needs to be revoked. The identification follows the requirements as described for the initial identity validation for natural persons, or
- the requester is a member of the Atos Trusted CA registration authority and is informed about the circumstances which are specified in statement 121 in section 5.9.
- the requester uses self-service portal of the Atos Trusted CA registration authority

## 5 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

### 5.1 Certificate application

- 88 This section describes who can submit a certificate application (in the sense of “certificate request”) and how the processing for certificate application is organized. Section 4.2 describes the identification and authentication procedures for the initial registration for each subject type. Section 5.4 describes the requirements for certificate acceptance.
- 89 Before entering into a contractual relationship with a subscriber, the CA informs the subscriber of the conditions regarding use of the certificate as given in section 5.5. This is done by the Subscriber Agreement of each CA, which can be downloaded from the repository. For details on the content of the Subscriber Agreement see section 3.2, statements 48 and 49.
- 90 [Client-CA]: If the subject is a person and not the same as the subscriber, the subject is informed about his/her obligations. If the subject is a functional mailbox, the corresponding subscriber is informed about his/her obligations. For the content of the obligations see section 5.5.
- 91 [Client-CA]: The subscriber's obligations as defined in section 5.5 are part of the Subscriber Agreement, see above (statement 89). This document is communicated to the users via repository, see statement 33.
- 92 Atos Trusted CA ensures that the requirements of the German “Datenschutz-Grundverordnung (DSGVO)” are adhered to within their registration process.

### 5.2 Certificate application processing

- 93 This section describes how is the processing for certificate application (in the sense of “certificate request”) after the section 5.1 above described who can submit a certificate application.
- 94 The confidentiality and integrity of registration data are protected, especially when exchanged with the subscriber/subject or between distributed CA system components by:
- Web communication via https.
  - If necessary during individual communication: Digitally signed and/or encrypted email communication
- 95 If external registration service providers are used, Atos Trusted CA verifies that registration data is exchanged with recognized registration service providers, whose identity is authenticated, see statement 69 and 73.

### 5.3 Certificate issuance

- 96 This section describes the certificate issuance related elements. Section 4.1 specifies the naming and identification of the subscribers and section 8.1 specifies the certificate profile. Section 5.2 describes how is the processing for certificate application (in the sense of “certificate request”) after section 5.1 described who can submit a certificate application.

- 97 All measures of Atos Trusted CA necessary to prevent forgery are described in this practice statement (see section 4 “Identification and Authentication”).
- 98 The procedure of issuing the certificate is securely linked to the associated registration, certificate re-key, including the provision of any subject-generated public key, see statement 94. The Atos Trusted CA will not issue certificates whose lifetime exceeds that of the CA's signing certificate.
- 99 If the Atos Trusted CA generates the subject's key, this is done in a controlled environment and under controlled circumstances, see section 7.1.

#### 5.4 Certificate acceptance

- 100 Section 5.1 describes who can submit a certificate application and how the processing for certificate application is organized. Section 4.2 describes the identification and authentication procedures for the initial registration for each subject type. This section describes the requirements for certificate acceptance.
- 101 Atos Trusted CA records the signed agreement with the subscriber including:
- agreement to the subscriber's obligations defined in section 5.5;
  - agreement by the subscriber to user secure user device – if used;
  - consent to the keeping of a record by the CA of information used in registration, subject device provision, including whether this is to the subscriber or to the subject where they differ, and any subsequent revocation, see section 6.4 “Audit logging procedures”, the identity and any specific attributes placed in the certificate, and the passing of this information to third parties under the same conditions as required by this policy in the case of the CA terminating its services;
  - whether, and under what conditions, the subscriber requires and the subject consents to the publication of the certificate;
  - confirmation that the information held in the certificate is correct.
- 102 The subscriber may agree to different aspects of this agreement during different stages of registration. For example, agreement that the information held in the certificate is correct may be carried out subsequent to other aspects of the agreement. This agreement may be in electronic form.
- 103 Atos Trusted CA retains the records identified above for the period of time as indicated to the subscriber (see statement 91).



## 5.5 Key pair and certificate usage

104 Atos Trusted CA obliges through agreement the subscriber to address all the following obligations. If the subject and subscriber are separate entities, the subscriber makes the subject aware of those obligations applicable to the subject (as listed below):

- accurate and complete information is submitted to the CA in accordance with the requirements of this policy, particularly with regards to registration,
- the key pair is only used in accordance with any limitations notified to the subscriber (see section 10.11),
- reasonable care is exercised to avoid unauthorized use of the subject's private key.
- The application details provided by the Subscriber shall be truthful, accurate, and not misleading. Failure by a subscriber to comply, or to promptly correct inaccurate information will result in revocation of the certificate.

105 If the subscriber or subject generates the subject's keys:

- subject keys are generated using an algorithm recognized by industry as being fit for the uses of the certified key as identified in the certificate policy (minimum requirements are defined in section 7.1);
- a key length and algorithm is used which is recognized as being fit for the uses of the certified key as identified in the certificate policy during the validity time of the certificate (minimum requirements are defined in section see 7.1)

106 If the subscriber or subject generates the subject's keys and the private key is for creating electronic signatures the subject's private key can be maintained under the subject's sole control.

107 Requirement [ETSI\_319411] 6.3.0.5g is not applicable.

108 Requirement [ETSI\_319411] 6.3.0.5h is not applicable.

109 The subscriber notify the CA without any reasonable delay, if any of the following occur up to the end of the validity period indicated in the certificate:

- the subject's private key has been lost, stolen, potentially compromised; or
- control over the subject's private key has been lost due to compromise of activation data (e.g. PIN code) or other reasons; and/or
- inaccuracy or changes to the certificate content, as notified to the subscriber or to the subject

110 How to contact the CA is documented in section 10.11.

111 Following compromise, the use of the subject's private key is to be immediately and permanently discontinued.

112 In the case that the CA which issued the subject's certificate has been compromised, the CA ensures that the certificates are no more used by the subjects. Depending on the situation, appropriate actions to be taken will be evaluated, e.g. revoking all affected certificates.

113 The Subscriber Agreement - made available to relying parties as specified in section 3.2 - include a notice that if one has to rely upon a certificate, he/she

- verifies the validity, suspension or revocation of the certificate using current revocation status information as indicated to the relying party (see section 7.3.4); and
- takes account of any limitations on the usage of the certificate indicated to the relying party either in the certificate or the Subscriber Agreement supplied as required in statements 48 and 49; and
- takes any other precautions prescribed in agreements or elsewhere.

#### 5.6 Certificate renewal

114 [Client-CA][Codesigning-CA] Renewal ("A new certificate for an existing key pair is generated") is **not** supported by the Atos Trusted CA.

[SSL-CA]: Renewal ("A new certificate for an existing key pair is generated") is supported by the Atos Trusted CA with following conditions:

- the same validation methods apply as for the initial certificate application
- the cryptographic security of subject's previously certified public key is still sufficient for the new certificate's validity period and no indications exist that the subject's private key has been compromised nor that the certificate has been revoked due to any other security breach

#### 5.7 Certificate re-key

115 An existing certificate can be re-keyed. This means: The subscriber generates a new key pair to replace the expiring key pair and obtains a new certificate for the new key pair.

116 The complete, accurate and duly authorization of the requester is performed as specified in section 4.3, statement 82.

#### 5.8 Certificate modification

117 For the subsequent continuity of certificate usage a subscriber must obtain a new certificate if the existing subscriber's actual certificate contains attributes which are changed e.g. company's address, subject name etc.). The complete, accurate and duly authorization of the requester for a certification modification is performed as specified in section 4.3, statement 82.

## 5.9 Certificate revocation and suspension

**118** Requirements concerning the identification and authentication for revocation requests are described in section 4.4. This section describes the practises and procedures concerning the general revocation and suspension requirements; the specific practises and procedures on certificate status information is described in section 5.10. Information on the CRL's profile is given in section 8.2.

**119** Revocation requests can be submitted by

- the subscriber belonging to that certificate whose companion public key needs to be revoked,
- the subject belonging to that certificate whose companion public key needs to be revoked,
- a substitute or representative, who adduces an evidence that he or she acts for the subscriber/subject belonging to that certificate whose companion public key needs to be revoked or
- a member of the Atos Trusted CA registration authority.

**120** Revocation requests are submitted via:

- digitally signed email communication or
- Web communication via https.

**121** The Atos Trusted CA will revoke certificates or a certificate issued to subscribers:

- upon written request (including by electronic means) of any subscriber to whom the subject certificate was issued;
- if Atos Trusted CA becomes aware that any material fact contained in the certificate is no longer true;
- as necessary to comply with the then-current certification standards, operating standards or substitute operating standards.
- subscriber is in material breach of terms of its Subscriber Agreement pertaining to security or of any certification standards;
- the security of a certificate or any associated private key or root(s) has (or may have) been compromised;
- the certificate was not properly issued under this CPS or any applicable certification standards;
- the certificate was issued to persons or entities identified as publishers of malicious software or that impersonated other persons or entities;

- the certificate was issued as a result of fraud or negligence (including fraud or negligence of or within Atos Trusted CA or a browser manufacturer); or
- a certificate, if not revoked, will compromise the trust status of any product(s) it was issued for.
- certificates issued to subscribers who use it to digitally sign hostile code, including spyware or other malicious software (malware) downloaded without user consent.

The Atos Trusted CA will inform the subscriber if by any reason a certificate issued to him has been revoked by the Atos Trusted CA.

**122** Revocation status information is distributed via CRLs and OCSP, see section 5.10 (specific practises and procedures on certificate status information) and section 8.2 (information on the CRL's profile).

**123** Requests and reports relating to revocation are processed promptly on receipt, generally done automatically within minutes, but latest within the maximum delay time of one working day (24 h time) after receipt.

**124** If the CA expects a delay which is longer than in statement 123 defined, the certificate's revocation status set to "suspended" whilst the revocation is being confirmed.

**125** The subject, and where applicable the subscriber, of a revoked or suspended certificate, is informed of the change of status of the certificate via an email.

**126** A revoked certificate will never be reinstated.

#### 5.10 Certificate status services

**127** Requirements concerning the identification and authentication for revocation requests are described in section 4.4. Practises and procedures concerning the general revocation and suspension requirements are described in section 5.9; and this section describes the specific practises and procedures on certificate status information. Information on the CRL's profile is in section 8.2.

**128** Revocation status information is provided through OCSP and CRL as specified in section 3.1. It is available

**24 hours per day, 7 days per week.**

**129** Upon system failure, service or other factors which are not under the control of the CA, the CA makes best endeavours to ensure that this information service is not unavailable for longer than

**1 working day.**

**130** The integrity and authenticity of the status information is protected: CRLs and OCSP-responses are electronically signed.

131 Revocation status information includes information on the status of certificates at least until the certificate expires.

#### 5.11 End of subscription

132 Per default the subscription lasts until the end of the validity of a certificate. If needed, section 5.9 has to be considered.

#### 5.12 Key escrow and recovery

133 The subject's private decrypting keys of the end-users can be held by the CA, for key recovery purposes. The CA ensures that the private key is kept secret and only made available to appropriately authorized persons. The key recovery process follows the same procedures as used for the initial issuance of the certificate.

134 The private keys of Atos Trusted CAs are kept secret. Backups of these keys are only used in case of disaster recovery. The number of duplicate subject's private keys will not exceed the minimum needed to ensure the continuity of the service.

## 6 FACILITY, MANAGEMENT AND OPERATIONAL CONTROLS

135 Atos has implemented an Information Security Management System (ISMS) based upon and certified regarding ISO 27001. The security of the Atos Trusted CA is embedded in this Atos-wide ISMS. This means that safeguards from the Atos-wide ISMS e.g. regarding securing facility and Security-Management are also effective for the Atos Trusted CA.

### 6.1 Physical controls

136 Physical access to facilities concerned with certificate generation, subject device preparation, and revocation management services are limited to authorized individuals only.

137 The risks are assessed to assure continuing business of a potential disaster to its critical business activities. Business continuity plans are developed to provide protection against the loss of assets (hardware, software and information). These plans ensure that possible disasters that pose unacceptable risk are adequately covered by a fully documented and tested plan, such that business impact is minimized and disrupted activities can be resumed as quickly as possible. To ensure that the Atos Trusted CA infrastructure components continue to deliver IT services, line managers are responsible for maintaining the infrastructure and implementing a business continuity plan if a disaster prevents the normal delivery of service. Business continuity plans are capable of delivering the availability requirements stated in this CPS and are tested and audited regularly.

138 To avoid compromise or theft of information and information processing facilities the following controls have been implemented:

- physical access control;
- equipment is protected from physical and environmental threats.

139 The facilities concerned with certificate generation and revocation management are operated in an environment which physically protects the services from compromise through unauthorized access to systems or data.

140 Any persons entering this physically secure area shall not be left for any significant period without oversight by an authorized person.

141 Physical protection is achieved through the creation of clearly defined physical barriers around the certificate generation, subject device preparation and revocation management services. The access to the security perimeter is limited to authorized personnel.

142 Physical and environmental security controls are implemented to protect the facility housing system resources, the system resources themselves, and the facilities used to support their operation. A physical and environmental security policy for systems concerned with certificate generation, subject device preparation and revocation management services is defined, which addresses the physical access control, natural disaster protection, fire safety factors, failure of sup-

porting utilities (e.g. power, telecommunications), structure collapse, plumbing leaks, protection against theft, breaking and entering, and disaster recovery.

143 Controls are implemented to protect against equipment, information, media and software relating to the CA services being taken off-site without authorization.

144 Atos Trusted CA ensures that the CA systems are secure and correctly operated, with minimal risk of failure.

145 Media used are securely handled to protect media from damage, theft and unauthorized access.

## 6.2 Procedural controls

146 To ensure that the administrative and management procedures are adequate and correspond to recognized standards, Atos Trusted CA has implemented the Atos Information Security Management System, which supports the security requirements of this CPS and conforms to the ISO 27001 Standard.

147 Atos Trusted CA carries out a risk assessment to evaluate business risks and determine the necessary security requirements and operational procedures. The risk analysis is regularly reviewed and revised if necessary.

148 Atos Trusted CA is responsible for all aspects of the provision of certification services. Responsibilities of third parties are clearly defined by the Atos Trusted CA and appropriate arrangements are made to ensure that third parties are bound to implement any controls required by the Atos Trusted CA. The Atos Trusted CA retains responsibility for the disclosure of relevant practices of all parties.

149 The Atos Trusted CA management provides direction on information security through a high level steering forum that is responsible for defining the CA's information security policy approach (represented by this CPS and substantiating documents) and ensures publication and communication of relevant information to all employees who are impacted.

150 The Atos Trusted CA has an Information Security Management System (ISMS) based on ISO 27001 for quality and information security management appropriate for the certification services it is providing.

151 The information security infrastructure necessary to manage the security within the Atos Trusted CA is implemented according to the ISO 27001 standard and maintained at all times. Any changes that will impact on the level of security provided are approved by the Atos Trusted CA management forum.

152 The security controls and operating procedures for Atos Trusted CA facilities, systems and information assets providing the certification services are documented, implemented and maintained according to the plan, do, check act cycle of the Atos ISMS.

- 153 The Atos Trusted CA ensures that the security of information shall be maintained when the responsibility for CA functions has been outsourced to another organization or entity.
- 154 Media management procedures are installed to protect against obsolescence and deterioration of media within the period of time that records are required to be retained.
- 155 All procedures follow a documented role-concept, for all trusted and administrative roles that impact on the provision of certification services (see statement 168).
- 156 Capacity demands are monitored and projections of future capacity requirements made to ensure that adequate processing power and storage are available.
- 157 The CA system access is limited to properly authorized individuals.
- 158 Operation procedures are in place to ensure the 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.
- 159 Procedures are in place to ensure that access to information and application system functions are restricted in accordance with the Atos ISMS and that the CA system provides sufficient computer security controls for the separation of trusted roles, including the separation of security administrator and operation functions. Particularly, use of system utility programs is restricted and tightly controlled. Access shall be restricted only allowing access to resources as necessary for carrying out the role(s) allocated to a user.

### 6.3 Personnel controls

- 160 The CA ensures that personnel and hiring practices enhance and support the trustworthiness of the CA's operations.
- Security responsibilities are addressed prior to employment in adequate job descriptions and in terms and conditions of employment.
  - All candidates for employment are adequately screened.
  - Employees are aware of their security roles and responsibilities.
  - The number of personnel authorized to carry out CA key pair generation, backup, storage and recovery of keys is kept to a minimum
  - Employees are made aware of their responsibilities for maintaining effective access controls, particularly regarding the use of passwords and the security of equipment.
- 161 The Atos Trusted CA employs a sufficient number of personnel which possess the expert knowledge, experience and qualifications necessary for the offered services through formal training and actual experience.



162 In the event of a breach of the Atos ISMS disciplinary action may be taken. Such action will vary from a verbal warning (with or without a note in the personnel file) up to and including termination. The severity of the incident shall govern the severity of the action taken.

163 Security roles and responsibilities, as specified in the Atos ISMS, are documented in job descriptions. Trusted roles, on which the security of the Atos Trusted CA's operation is dependent, are clearly identified.

164 Atos personnel in charge of operating the CA (both temporary and permanent) 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.

165 Personnel exercise administrative and management procedures and processes that are in line with the Atos Trusted CA's information security management procedures. These procedures and controls are in line with the ISO 27001 standard.

166 Personnel are employed who possess experience and training in the electronic signature technology and who are familiar with security procedures, information security and risk assessment and who can carry out management functions in these areas.

167 All Atos personnel in trusted roles are free from conflicting interests that might prejudice the impartiality of the Atos Trusted CA operations.

168 All procedures follow a documented role-concept, for all trusted and administrative roles that impact on the provision of certification services.

- Atos Security Officer:  
Overall responsibility for administering the implementation of the security practices.
- CA-Operators:  
Approve the generation/revocation/suspension of certificates.
- System Administrators:  
Authorized to install, configure and maintain the CA trustworthy systems for registration, certificate generation, subject device provision and revocation management.
- System Operators:  
Responsible for operating the CA 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 CA trustworthy systems.

169 Atos personnel responsible for the Atos Trusted CA operation are formally appointed to trusted roles by senior management responsible for security.

170 Atos Trusted CA does 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 do not have access to the trusted functions until all necessary checks are completed.

#### 6.4 Audit logging procedures

171 Atos Trusted CA ensures that all certificates, revocation lists and relevant information concerning, certificates' lifecycle, key management and certificate management events are recorded for a period of: the corresponding certificates' validity, plus seven years, until the next end-of-year. Contractual agreements (like certificate request forms) are stored in accordance to local legislation.

172 Log files are protected using an access control mechanism.

173 Records concerning certificates are 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 the subscriber, will have necessary access to registration and other information relating to the subject.

174 The precise time of significant CA environmental, key management and certificate management events are recorded using a time synchronization protocol.

175 Events are protected from unauthorized deletion and destruction using an access control mechanism.

176 All events relating to registration including requests for certificate re-key are logged.

177 All registration information including the following is recorded:

- document(s) presented by the applicant to support registration;
- record of unique identification data, numbers, or a combination thereof (e.g. applicant's drivers license number) of identification documents;
- storage location of copies of applications and identification documents, including the signed Subscriber Agreement;
- any specific choices in the Subscriber Agreement (e.g. consent to publication of certificate);
- identity of entity accepting the application;
- method used to validate identification documents, if any;
- name of receiving CA and/or submitting Registration Authority, if applicable.

178 All events relating to the life-cycle of CA keys are logged.

179 All events relating to the life-cycle of certificates are logged.

180 All events relating to the life cycle of keys managed by the Atos Trusted CA, including any subject keys generated by the Atos Trusted CA are logged.

181 All requests and reports relating to revocation, as well as the resulting action, are logged.

#### 6.5 Records archival

182 Records concerning certificates are completely and confidentially archived using proper access control mechanisms. Only administrative staff has access to the records and is responsible for:

- Protection against modification of the archive
- Protection against deletion of the archive
- Protection against the deterioration of the media on which the archive is stored
- Protection against obsolescence of hardware, operating systems, and other software
- Archive backup procedures
- Procedures to obtain and verify archive information

183 Records concerning certificates are held for a defined period of time, see statement 171.

#### 6.6 Key changeover

184 CA key generation follows a documented process and happens in a controlled environment and under controlled circumstances. A suitable time before expiration of its CA signing key, the CA generate a new certificate-signing key pair and apply all necessary actions to avoid disruption to the operations of any entity that may rely on the CA key. The new CA key is generated and distributed in accordance with this CPS.

#### 6.7 Compromise and Disaster Recovery

185 A business continuity plan is defined and maintained to enact in case of a disaster.

186 Adequate backup-procedure is provided to ensure that systems software, application software and data can be recovered following a system or media failure. Backup files are stored at a sufficient distance from the main location, and are given an appropriate level of physical protection, consistent with the physical security of the IT-system. The backup and restore process are regularly tested.

187 Backup and restore functions are performed by trusted roles (specified in statement 168).

188 The business continuity plan addresses the compromise or suspected compromise of the Atos Trusted CA's private signing key.

189 Following a disaster, the Atos Trusted CA will, where practical, take steps to avoid repetition of a disaster.

190 In the case of compromise, the Atos Trusted CA will as a minimum provide the following undertakings:

- Inform the following of the compromise: all subscribers and other entities with which Atos Trusted CA has agreements or other form of established relations, among which relying parties and CAs. In addition, this information shall be made available to other relying parties.
- Indicate that certificates and revocation status information issued using this CA key may no longer be valid.

191 Should any of the algorithms, or associated parameters, used by the Atos Trusted CA or its subscribers become insufficient for its remaining intended usage then the Atos Trusted CA will:

- Inform all subscribers and relying parties with whom the CA has agreement or other form of established relations. In addition, this information will be made available to other relying parties.
- Revoke any affected certificate.

#### 6.8CA or RA termination

192 Before Atos Trusted CA terminates its services the following procedures will be executed:

- Atos Trusted CA will inform the following of the termination: all subscribers and other entities with which Atos Trusted CA has agreements or other form of established relations, among which relying parties and CA. In addition, this information will be made available to other relying parties.
- Atos Trusted CA will perform necessary undertakings to transfer obligations for maintaining registration information, revocation status information (see section 5.9) and event log archives (see section 6.5) for their respective period of time as indicated to the subscriber and relying party (see section 3.2).
- Atos Trusted CA will destroy, or withdraw from use, its private keys, as defined in section 7.2.

193 Atos Trusted CA make the following provisions for termination of service:

- All affected entities will be notified.
- This CPS will be binding in case of the transfer of obligations to other parties, including the revocation status for unexpired certificates that have been issued.

## 7 TECHNICAL SECURITY CONTROLS

### 7.1 Key pair generation and installation

- 194** CA key generation follows a documented process and happens in a controlled environment, under controlled circumstances and in a physically secured environment (see section 6.1) by personnel in trusted roles (see section 6.3) under dual control. The procedure is logged and is recorded by video. An additional report is signed by the trusted role responsible for the security of Atos Trusted CA key generation. For Root CA key generation this report is also signed by a trustworthy person independent of the Atos Trusted CA (e.g. Notary, auditor) as witness that the report correctly records the key management ceremony.
- 195** CA key generation is carried out within a device which meets the requirements identified in FIPS PUB 140-2 level 3.
- 196** Certification authority key generation is performed using the RSA algorithm. The selected key length is at least 2048 bits. The hash algorithm used is at least SHA-256.
- 197** The Atos Trusted CA signature verification public keys are made available to relying parties in an SSL session. Additionally the fingerprint of the keys can be verified on the Atos Trusted CA website.
- 198** [ Atos Client CA] Subject keys use the RSA algorithm, have a length of at least 2048 bits and use at least SHA-256 (independent if generated by the subscriber or by the Atos Trusted CA).
- 199** [ Atos Client CA] Subject keys generated by Atos Trusted CA are stored in an encrypted container and secured using a complex password before delivery to the subject. If the password needs to be sent to the subject, this happens in a secure manner e.g. using a separate transport-channel.
- 200** [ Atos Client CA] Subject keys generated by Atos Trusted CA are only used for key recovery purposes and therefore securely stored.
- 201** If a copy of the subject's private key is not required to be kept by the CA, once delivered to the subject, any copies of the subject's private key held by the CA are destroyed.

### 7.2 Private Key Protection and Cryptographic Module Engineering Controls

- 202** Atos Trusted CA ensures that CA keys are generated in controlled circumstances.
- 203** The Atos Trusted CA private signing key is held and used within a secure cryptographic device which meets the requirements identified in FIPS PUB 140-2 level 3.
- 204** The use of the corresponding Atos Trusted CA's private key is limited to be compatible with the hash algorithm, the signature algorithm and signature key length used in the generating certificates, in line with current practice statement 196.
- 205** All copies of the Atos Trusted CA private signing keys are destroyed or put beyond use at the end of their life cycle.

Atos Trusted CA ensures the security of cryptographic device throughout its lifecycle. In particular the Atos Trusted CA ensures that:

206 Certificate and revocation status information signing cryptographic hardware is not tampered with during shipment.

207 Certificate and revocation status information signing cryptographic hardware is not tampered with while stored.

208 The installation, activation, backup and recovery of the Atos Trusted CA's signing keys in cryptographic hardware is done under simultaneous control of two trusted employees, following the documented process in the role concept.

209 Certificate and revocation status information signing cryptographic hardware is functioning correctly.

210 CA private signing keys stored on CA cryptographic hardware are destroyed upon device retirement.

### 7.3 Other aspects of key pair management

211 A suitable time before expiration of the Atos Trusted CA signing key, Atos Trusted CA will generate a new certificate-signing key pair and will apply all necessary actions to avoid disruption to the operations of any entity that may rely on the Atos Trusted CA key. The new CA key will also be generated and distributed in accordance with this policy.

212 The Atos Trusted CA private keys that are held outside the signature-creation device for backup purposes are encrypted using a strong symmetric key algorithm and ensures the same level of protection as provided by the signature creation device.

213 The Atos Trusted CA private signing key is backed up, stored and recovered only by personnel in trusted roles using dual control - following the role concept - in a physically secured environment.

214 Backup copies of the Atos Trusted CA private signing keys are subject to the same level of security controls as keys currently in use (see statement 212).

215 Access control using dual control is in place to ensure that the keys are not accessible outside the hardware module.

216 The Atos Trusted CA signing keys used for generating certificates and/or issuing revocation status information are not used for any other purpose.

217 The certificate signing keys are only used within physically secure premises.

#### 7.4 Activation data

218 The installation, activation, backup and recovery of the Atos Trusted CA's signing keys in cryptographic hardware are under simultaneous control of two trusted employees, following the role concept.

#### 7.5 Computer security controls

219 The integrity of the Atos Trusted CA systems and information is protected against viruses, malicious and unauthorized software.

220 All files on the Atos Trusted CA systems are scanned for viruses on a regular basis.

221 All new software and data files, especially if these files are coming from an unknown or non-trusted source (like the Internet), or unprotected devices such as USB keys or external disk drives, are scanned for viruses before use.

222 Prior to distributing any data file to a third party, the files are scanned for viruses.

223 Security incidents must be reported to Atos Trusted CA management as possible. Atos Trusted CA management is responsible for taking action to resolve incidents. All staff members are made aware of the procedures for reporting security incidents.

224 If a virus is detected and cannot be cleaned automatically by the virus protection software, the local support organization is immediately informed.

225 Security weaknesses must be reported to Atos Trusted CA management. Atos Trusted CA management is responsible for evaluating the security risk and taking action when required and must be aware of the procedures for reporting security incidents.

226 Access restrictions to media are in place to prevent access from unauthorized personnel.

227 The distribution of data is kept to a minimum.

228 When equipment and media containing sensitive information are disposed of, the process ensures that the information cannot be retrieved afterwards.

229 To maintain appropriate protection of assets, all major assets are inventoried (hardware and software) and have a nominated owner (hardware, software and information).

230 To ensure that information receives an appropriate level of protection, information is classified according to Atos's classification standard to realize the appropriate level of protection.

231 Upon creation of information, the creator of that information is responsible for immediate classification. The owner of information is responsible for correct classification and should review the classification in line with Atos document control procedures at least annually to check if it is still correct.

232 Audit processes, meeting requirements specified in paragraph 6.4, are invoked at system startup, and cease only at system shutdown.

233 Audit logs are monitored and reviewed regularly to identify evidence of malicious activity.

234 The security operations of the Atos Trusted CA are integrated into the Atos Security Management. This is separated from normal operations and 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.

235 Atos Trusted CA personnel must be successfully identified and authenticated with multi-factor authentication before using critical applications related to certificate management.

236 Atos Trusted CA personnel are held accountable for their activities, by retaining event logs.

237 Certificate generation: Continuous monitoring and alarm facilities shall be in place to enable the CA to detect, register and react in a timely manner upon any unauthorized and/or irregular attempts to access its resources.

238 Revocation management: Continuous monitoring and alarm facilities are provided to enable the CA to detect, register and react in a timely manner upon any unauthorized and/or irregular attempts to access its resources.

239 The Atos Trusted CA revocation status application enforces access control on attempts to modify revocation status information. Also revocation status requests concerning non-issued certificates on the responder are monitored.

240 Atos Trusted CA uses trustworthy systems and products that are protected against modification (see section 7.6).

## 7.6 Life cycle technical controls

241 All media is handled securely in accordance with requirements of the information classification scheme (see section 7.4.2). Media containing sensitive data is securely disposed of when no longer required.



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

243 Key generation devices are trustworthy systems as described in statement 195. Other systems are hardened according to best practices and protected against modification.

244 An analysis of security requirements is carried out at the design and requirements specification stage of any systems development project undertaken by the Atos Trusted CA to ensure that security is built into IT systems.

245 Change control procedures exist for releases, modifications and emergency software fixes for any operational software.

#### 7.7 Network security controls

246 Atos Trusted CA ensures that CA system access is limited to properly authorized individuals.

247 Firewalls are implemented to protect Atos Trusted CA's internal network domains from external network domains accessible by third parties.

248 Firewalls are configured to prevent protocols and accesses not required for the operation of the CA.

249 Sensitive data is protected against unauthorized access or modification. Sensitive data is protected using encryption and integrity protection when exchanged over networks which are not secure.

250 Atos Trusted CA ensures that local network components (e.g. routers) are kept in a physically secure environment and their configurations periodically audited for compliance.

#### 7.8 Time-stamping

251 The services of the Atos Trusted CA do not cover time-stamping services.

## 8 CERTIFICATE, CRL, AND OCSP PROFILES

### 8.1 Certificate profile

252 Atos Trusted CA ensures that it issues certificates securely to maintain their authenticity.

253 The certificates issued by Atos Trusted CA are defined in ITU-T Recommendation X.509 and shall include:

- identification of the Atos Trusted CA (certification-service-provider) and the country in which it is established;
- the name of the subject, or a pseudonym which shall be identified as such;
- provision for a specific attribute of the signatory to be included if relevant, depending on the purpose for which the certificate is intended;
- the public key which corresponds to the private key under the control of the subject;
- an indication of the beginning and end of the period of validity of the certificate;
- the serial number of the certificate;
- the electronic signature of the certification authority issuing it;
- limitations on the scope of use of the certificate, if applicable;
- limits on the value of transactions for which the certificate can be used, if applicable; and identification of the CA and the country in which it is established

254 The Atos Trusted CA ensures that over the life time of the CA a distinguished name which has been used in a certificate by it is never re-assigned to another entity.

### 8.2 CRL profile

255 The CA ensures that certificates are revoked in a timely manner based on authorized and validated certificate revocation requests. Requirements concerning the identification and authentication for revocation requests are described in section 4.4. This section describes the practices and procedures concerning the general revocation and suspension requirements. The specific practices and procedures on certificate status information is described in section 5.10. This section contains the information on the CRL's profile.

256 Certificate Revocation Lists (CRLs) are published at least every 24 hours for Intermediate CAs. For the Root CA a new CRL will be generated after revocation of an Intermediate CA or at least every 12 month.

257 For Certificate Revocation Lists (CRLs) including any variants the following attributes are defined:

- every CRL states a time for next scheduled CRL issue;

- a new CRL may be published before the stated time of the next CRL issue;
- the CRL is signed by the certification authority.

258 In order to maximize interoperability Atos Trusted CA issues Certificate Revocation Lists as defined in ITU-T Recommendation X.509.

### 8.3 OCSP profile

259 The Version of OCSP that is being used as the basis for establishing an OCSP system is Version 1 (v1); The OCSP is conforming to IETF RFC 6960. The OCSP will not respond with a “good” status on certificates which have not been issued by Atos Trusted CA.

## 9 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

### 9.1 Frequency or circumstances of assessment

**260** The Atos Trusted CA claims conformance to the present document as applied in the certificate policy identified in the certificate that it issues. Atos Trusted CA has a current assessment of conformance to the identified certificate policy by a competent independent party. The results of the assessment are made available to subscribers and relying parties on request.

**261** If the Atos Trusted CA is later shown to be non-conformant in a way that significantly affects the ability of the CA to meet the objectives identified in the present document, then it will cease issuing certificates using the identifiers in section 2.1 until it has demonstrated or been assessed as conformant, otherwise the Atos Trusted CA will take steps to remedy the non-conformance within a reasonable period.

**262** The Atos Trusted CA compliance is checked on a regular basis and whenever major change is made to the Atos Trusted CA operations.

### 9.2 Identity/qualifications of assessor

[CWA 14172-3]

**263** The compliance is assessed by a qualified and independent external party.

### 9.3 Assessor's relationship to assessed entity

[CWA 14172-3]

**264** Atos Trusted CA assures that there is no relationship between the assessor and the Atos Trusted CA which may affect the needed independency of the assessor.

### 9.4 Topics covered by assessment

**265** Compliance audits are conducted to meet the requirements that are stated in this CPS.

### 9.5 Extern Requirements

**266** Atos Trusted CA conforms to the version 1.5.7 of the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates published at <http://www.cabforum.org>. In the event of any inconsistency between this document and those Requirements, those Requirements take precedence over this document.

### 9.6 Actions taken as a result of deficiency

**267** Actions taken as a result of deficiency are stated in statement 261.

### 9.7 Communication of results

**268** The communications of the results is done conforming to statement 260.

## 10 OTHER BUSINESS AND LEGAL MATTERS

### 10.1 Fees

269 The fees of the certificates that are issued by the Atos Trusted CA are listed in a separate document and published in the repository.

### 10.2 Financial responsibility

270 The Atos Trusted CA ensures that its organization is reliable. In particular:

271 The Atos Trusted CA is part of Atos Information Technology GmbH, which is a legal entity according to German law.

272 The Atos Trusted CA as part of the Atos Information Technology GmbH has adequate arrangements to cover liabilities arising from its operations and/or activities.

273 The Atos Trusted CA as part of Atos Information Technology GmbH has the financial stability and resources required to operate in conformity with this policy.

274 The parts of the Atos Trusted CA concerned with certificate generation and revocation management are independent of other organizations for its decisions relating to the establishing, provisioning and maintaining and suspending of services in conformance with the applicable certificate policies; in particular its senior executive, senior staff and staff in trusted roles, are free from any commercial, financial and other pressures which might adversely influence trust in the services it provides.

### 10.3 Confidentiality of business information

275 The following information is identified as confidential data:

- Registration data
- CA and subjects private keys
- Current and archived records concerning certificates
- Personal identifiable information

276 Information that are considered to be outside the scope of confidential information are:

- Information included in certificates
- Revocation status

277 Confidential information is not shared with third parties, except if:

- Personal information requested by the affected person
- Requested by court order

- Other legal authorization

278 Parties with which confidential information is shared have to secure it from compromise, and refrain from using it or disclosing it to third parties.

#### 10.4 Privacy of personal information

279 If the subject's key pair is not generated by the Atos Trusted CA, the certificate request process ensures that the subject has possession of the private key associated with the public key presented for certification by digitally signing the certificate request.

280 The CA ensures compliance with legal requirements. In particular:

281 Atos Trusted CA ensures it meets all applicable statutory requirements (including requirements of the German "Datenschutz-Grundverordnung (DSGVO)") for protecting records from loss, destruction and falsification.

282 The contracting parties shall observe the applicable data protection regulations and shall ensure that their employees likewise undertake to observe these obligations.

283 The Atos Trusted CA ensures that the requirements of the EU General Data Protection Regulation, as implemented through National German Legislation in the "DSGVO", are met.

284 Appropriate technical and organizational measures are taken against unauthorized or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data as described in the German „DSGVO“ Art. 32.

285 The information that users contribute to the Atos Trusted CA are completely protected from disclosure without the user's agreement, a court order or other legal authorization.

286 The Atos Trusted CA ensures that privacy of subject information is maintained.

#### 10.5 Intellectual property rights

287 Atos Information Technology GmbH owns or has licensed the intellectual property rights on all the components of the Atos Trusted CA infrastructure and this CPS.

#### 10.6 Representations and warranties

288 The information in the certificate is true to the best of the Atos Trusted CA's knowledge after performing certain identity authentication procedures with due diligence.

#### 10.7 Disclaimers of warranties

289 See the General Terms and Conditions for Services of Atos Information Technology GmbH.

#### 10.8 Limitations of liability

290 See the General Terms and Conditions for Services of Atos Information Technology GmbH.

#### 10.9 Indemnities

[291](#) See the General Terms and Conditions for Services of Atos Information Technology GmbH.

#### 10.10 Term and termination

[292](#) The Atos Trusted CA is entitled to make changes to the CPS. The CPS remains valid until the actual CPS is declared invalid or a new CPS is communicated on the Atos Trusted CA website. A new CPS will be applicable 30 days after publication on the website. The Atos Trusted CA management is entitled to declare a new CPS as immediately valid if changes are required to ensure the proper functioning of the Atos Trusted CA.

#### 10.11 Individual notices and communications with participants

[293](#) The Atos Trusted CA accepts communication in written form or digitally signed emails. The Atos Trusted CA will send a signed email acknowledgement of receipt within 10 days. Written communication should be sent to:

Atos Information Technology GmbH

Atos Trusted CA

Lohberg 10

49716 Meppen

Germany

Email should be sent to [gmde-trustcenter@atos.net](mailto:gmde-trustcenter@atos.net)

#### 10.12 Amendments

[294](#) The CPS can be changed by the Atos Trusted CA. After the change, the new CPS is identified by a new version number and date.

#### 10.13 Dispute resolution provisions

[295](#) The Atos Trusted CA ensures that its organization is reliable. In particular:

[296](#) See the General Terms and Conditions for Services of Atos Information Technology GmbH.

#### 10.14 Governing law

[297](#) See the General Terms and Conditions for Services of Atos Information Technology GmbH.

#### 10.15 Compliance with applicable law

[298](#) See the General Terms and Conditions for Services of Atos Information Technology GmbH.

#### 10.16 Other provisions

- 299 Policies and procedures under which the CA operates are non-discriminatory.
- 300 The Atos Trusted CA makes its services accessible to all applicants whose activities fall within its declared field of operation.
- 301 The CA has a properly documented agreement and contractual relationship in place where the provisioning of services involves subcontracting, outsourcing or other third party arrangements.
- 302 The parts of the CA concerned with certificate generation and revocation management have a structure that safeguards impartiality of operations as documented in this CPS.



## 11 Annex - Referenced Documents

Reference	Document
[CWA 14172-3]	CEN Workshop Agreement CWA 14172-3 March 2004 "EESSI Conformity Assessment Guidance - Part 3: Trustworthy systems managing certificates for electronic signatures"
[ETSI_319411]	ETSI Technical Specification EN 319 411-1 (Actual version can be found at <a href="http://www.etsi.org/standards-search">http://www.etsi.org/standards-search</a> )
[FIPS140-2]	FIPS PUB 140-2 (2001): "Security Requirements for Cryptographic Modules".
[X.509]	ITU-T X.509:  Information Technology – Open Systems Interconnection – The Directory: Authentication Framework, 1997