Address:

To:
Atos Information Technology GmbH
Trustcenter
Lohberg 10
49716 Meppen

0. Preamble

The AOTCA is registered as a Trusted Root Certification Authority and is conformant to ETSI TS 102 042 V2.1.2.
This Subscriber Agreement on hand gives an overview of necessary information for and obligations of the Subscriber. These are described in detail in the Certification Practice Statement (CPS).

The CPS is available at the website of the AOTCA https://pki.atos.net

Both - Subscriber Agreement and CPS – are binding provisions between the Subscriber and the AOTCA.

5. Informations

5.1 Certificate Practice Statement

This document is valid only with the Certificate Practice Statement (CPS) which is in its actual version available at the AOTCA's website. If the CPS is changed, the Subscriber will be informed about by email sent to the email address registered at the AOTCA.

5.2 Publication of Information

AOTCA publishes certificates and Revocation Lists (CRL) it issues in the repository to the public, for usage by e.g. subscribers, subjects and relying parties.
Confidential information is not shared with third parties, except if:
- Personal information requested by the affected person
- Requested by court order other legal authorization

5.3. Necessary products

There are no particular products needed for applying the key-pair associated with the certificate(s) being issued.

5.4 Certificates' usage

The AOTCA places constraints on the applicability of the certificates.

SSL-Certificates:

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

Client-Certificates:
- 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 autorization

CodeSigning-Certificates:
- Confirm the author of a software
- Enable to confirm that the software has not been changed or corrupted

5.5 Subscriber's obligations

The Subscriber's obligations are:
- 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.
- The key pair is only used in accordance with the above limitations.
- Reasonable care is exercised to avoid unauthorized use of the Subscribers Private Key.
- The Subscriber handles a User-ID, Password or PIN, which can be used to access the AOTCA's Webservice and which give access to the Private Key. The Subscriber shall treat this information – including the Private Key itself - as confidential and keep it secret.
- The Subscriber shall notify the AOTCA, without any unreasonable delay,
  - o if any of the above described violations occur up to the end of the validity period indicated in the Certificate, or if
  - o the Subscribers Private Key – or the control over it - has been potentially or actually lost, stolen or compromised, or if
  - o if certificate(s) issued to him by the AOTCA became compromised.

5.6 Certificate Revocation

CA will revoke certificates or a Certificate issued to Subscribers:
- (i) upon written request (including by electronic means) of any Subscriber to whom the subject Certificate was issued;
- (ii) if CA becomes aware that any material fact contained in the Certificate is no longer true;
- (iii) as necessary to comply with the then-current Certification Standards, Operating Standards or Substitute Operating Standards.
- (iv) Subscriber is in material breach of terms of its Subscriber Agreement pertaining to Security or of any Certification Standards;
- (v) the security of a Certificate or any associated private key or Root(s) has (or may have) been compromised;
- (vi) the Certificate was not properly issued under this Agreement or any applicable Certification Standards;
- (vii) the Certificate was issued to persons or entities identified as publishers of malicious software or that impersonated other persons or entities;
- (viii) the Certificate was issued as a result of fraud or negligence (including fraud or negligence of or within CA or a Browser Manufacturer); or
- (ix) a Certificate, if not revoked, will compromise the trust status of any Product(s).

(x)   Certificates issued to subscribers who use it to digitally sign hostile code, including spyware or other malicious software (malware) downloaded without user consent.

The AOTCA will inform the Subscriber if by any reason a certificate issued to him has been revoked by the AOTCA.

5.7 Certificate validation

The Subscriber is obliged to validate the certificate(s) against the Certificate Revocation List (CRL) available at the AOTCA's website. This should happen prior of each usage, at least monthly.

5.8 Event Logs and Life Cycle Information
AOTCA ensures that event logs and all relevant information concerning certificates' lifecycle, key management and certificate management events is recorded for a period of time in particular for the purpose of providing evidence of certification for the purposes of legal proceedings.
The period of time which the CA event logs and life cycle information are retained is defined in the CPS.

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

7. Fees
Subscriber shall pay to AOTCA the fees associated with the Trustcenter Services. Prices are sent to the Subscriber upon request.