To:
Atos Information Technology GmbH
Trustcenter
Lohberg 10
49716 Meppen

Sender:

0. Preamble

The Atos Trustcenter (ATC) is registered as a Trusted Root Certification Authority and is conformant to ETSI EN 319 411-1 V1.3.1.
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 ATC: https://pki.atos.net

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

1. Information for the requestor

1.1 Certificate Practice Statement

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

1.2 Publication of Information

ATC publishes certificates and Revocation Lists (CRL) it issues in a 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 is requested by the affected person
- Requested by court order other legal authorization

The ATC is authorized to share information about the Applicant, signed application, Certificate, and surrounding circumstances with other CAs or industry groups, including the CA/Browser Forum if

- The Certificate or the Applicant is identified as a source of Suspect Code
- The authority to request the Certificate cannot be verified
- The Code Signing Certificate is revoked for reasons other than Subscriber request (e.g. as a result of private key compromise, discovery of malware, etc.)

1.3. Necessary products

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

1.4 Certificates' usage

The ATC 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 authorization

CodeSigning-Certificates:

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

1.5 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.
- Review and verify the Certificate contents for accuracy
- 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 ATC'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 ATC, without any unreasonable delay, if
    - any of the above described violations occur up to the end of the validity period indicated in the Certificate, or
    - the Subscribers Private Key – or the control over it - has been potentially or actually lost, stolen or compromised, or
    - certificate(s) issued to him by the ATC became compromised.
    - it is discovered that Code submitted to the Signing Service for Code Signature contained Suspect Code.
- If the Subscriber Certificate is use for a high-traffic FQDN, the Subscriber has to "staple" the OCSP response for the Certificate in its TLS handshake, see RFC4366
- The Subscriber shall promptly cease all use of the Private Key corresponding to the Public Key included in the Certificate upon expiration or revocation of the Certificate.
- The Subscriber uses the Certificate and associated Private Key only for authorized and legal purposes, including not using the Certificate to sign Suspect Code and to use the Certificate and Private Key solely in compliance with all applicable laws and solely in accordance with the Subscriber Agreement or Terms of Use.

If subscriber and certificate owner are different persons or subjects, the subscriber has to inform the certificates owner about his duties.

1.6 Certificate Revocation

The 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.
(xi) if CA becomes aware that the private key has been communicated to an unauthorized person or a non-affiliated organization.

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

1.7 Certificate Validation

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

1.8 Event Logs and Life Cycle Information

ATC 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.

2. Terms and Conditions

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

3. Fees

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

4. Privacy of personal information

The Atos Trustcenter ensures it meets all applicable statutory requirements (including requirements of the German “Datenschutz-Grundverordnung (DSGVO)”) for protecting records from loss, destruction and falsification.

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

The Atos Trustcenter ensures that the requirements of the EU General Data Protection Regulation, as implemented through National German Legislation in the “DSGVO”, are met.

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.

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

The Atos Trustcenter ensures that privacy of subject information is maintained.

_____

Subscriber (last name, first name)

_____

Location, date

_____

Signature subscriber