To:

Eviden Germany GmbH
Trustcenter
Lohberg 10
49716 Meppen
Germany

Sender:

1 Preamble

The Eviden Trustcenter (ETC) is registered as a Trusted Root Certification Authority and is audited and certificated in accordance with 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 ETC: https://pki.atos.net/

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

2 Contact Information

Address of Eviden Trustcenter:

Eviden Germany GmbH
Trustcenter
Lohberg 10
49716 Meppen – Germany

Email: pki-enterprise-tr@eviden.com

Web: https://pki.atos.net/trustcenter/en

Web contact: https://pki.atos.net/trustcenter/en/contact/trustcenter

3 Information for the requestor

3.1 Certificate Practice Statement

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

3.2 Publication of Information

ETC 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 ETC 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.)

3.3 Necessary products

The private keys for Code Signing Certificates shall be stored on a smartcard.

3.4 Certificates' usage

The ETC 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

3.5 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 CA- and subscriber certificate contents for accuracy.
- If you generate the key by yourself, ETC recommends to use a key size not less than 3072bit (RSA) & 256bit (ECC) and a hash functions not less than SHA-256.
- The key pair is only used in accordance with the above limitations and:
    - Use the Client-Certificate only on mailbox addresses listed in the certificate and use the certificate solely in compliance with all applicable laws and solely in accordance with this Subscriber Agreement;
    - Install the Server-Certificate only on servers that are accessible at the subjectAltName(s) listed in the Certificate and use the Certificate solely in compliance with all applicable laws and solely in accordance with this Subscriber Agreement;
    - Use the CodeSigning-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 this Subscriber Agreement.
- Reasonable care is exercised to avoid unauthorized use of the Subscribers Private Key. Provide adequate network and other security controls to protect against misuse of the Private Key. The CA will revoke the Certificate without requiring prior notification if there is unauthorized access to the Private Keys.
- The Subscriber handles a User-ID, Password or PIN, which can be used to access the ETC's Webservice and which give access to the Private Key. The Subscriber must treat this information – including the Private Key itself - as confidential and keep it secret. The subscriber must store the password or PIN distinct from the private key.
- The Subscriber shall notify the ETC, 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
    - control over the subject's private key has been lost due to compromise of activation data (e.g. PIN code) or other reasons, or

- certificate(s) issued to him by the ETC became compromised, or
- inaccuracy or changes to the certificate content, or
- 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 or becoming aware of a compromise of the Issuing CA (except for decryption).
- The subscriber accepts that the ETC is entitled to revoke the certificate immediately if the Applicant were to violate the terms of the Subscriber Agreement or Terms of Use or if revocation is required by the CA's CP, CPS, or these Baseline Requirements.
- The subscriber acknowledges and accepts that the ETC may modify the Subscriber Agreement or Terms of Use when necessary to comply with any changes in the CP/CPS or the Baseline Requirements.

The Applicant make the commitments and warranties in this section for the benefit of the CA and the Certificate Beneficiaries. If subscriber and certificate owner are different persons or subjects, the subscriber has to inform the certificates owner about his duties.

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

3.7 Revocation Reason

The Subscriber is obliged to choose one of the following revocation reasons during the revocation process:

- Unspecified: When the reason codes below do not apply to the revocation request, choose revocation reason "unspecified".
- Key compromised: Choose the "Key compromised" revocation reason when there are reasons to believe that the private key of their certificate has been compromised, e.g., an unauthorized person has had access to the private key of their certificate.
- Affiliation changed: Choose the "Affiliation changed" revocation reason when the organization's name or other organizational information in the certificate has changed.
- Certificate superseded: Choose the "superseded" revocation reason when a new certificate is requested to replace their existing certificate.
- Cessation of operation: Choose the "Cessation of operation" revocation reason when the domain names in the certificate are no longer owned or when the certificate is no longer used because the website is discontinued.

3.8 Certificate Validation

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

3.9 Event Logs and Life Cycle Information

ETC 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 information about certificates, identification, registration and the used CP/CPS and Subscriber agreement versions are archived until the certificate expiration date plus seven years.

4 Terms and Conditions

The General Terms and Conditions are available at the website of the ETC: https://pki.atos.net/trustcenter/en/download/trusted-root-ca

5 Fees

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

6 Availability

The high availability of PKI certification services and up-to-date PKI revocation information is a key requirement for using certificate-based applications in security related business and backup processes.

The service level agreements of the trust center provide:

- PKI Service will be online 7 day, 24 hours per day (“online time”).
- The SLA is contractually stipulated.

7 Privacy of personal information

The Eviden Trustcenter ensures it meets all applicable statutory requirements (including requirements of General Data Protection Regulation (GDPR)) 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.

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 GDPR Art. 32.

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

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

8 Relying party representations and warranties

Relying parties, who rely on Eviden Trustcenter certificates, have the obligation to validate the certificates status. The validation can be done:

- Either via online certificate status validation using the appropriate OCSP responder service

- Or via download of the CRL and offline status validation.

The OCSP responder service may provide more current data about the revocation status then the CRL because CRLs are generated at least every 24 hours. Relying parties should use the OCSP responder to verify the revocation information of a certificate.

Invalid certificates shall not be used. Relying parties shall consider the restrictions for the usage of the cryptographic keys. The restriction is included in the certificate in the extensions “Key Usage” and if existing “Extended Key Usage”. Relying parties shall consider the restrictions for the usage of the certificates.

Relying parties shall inform Eviden Trustcenter in case of suspicion of or really detected misuse of issued certificates.

9 Procedures for complaints and dispute settlement

If any disputes, complaints, or conflicts of opinion arise in connection with the services or CP/CPS, the parties shall make reasonable efforts to reach an out-of-court settlement. Disputes, complaints, or conflicts of opinion shall be submitted in written to Eviden Germany GmbH, Trustcenter, Lohberg 10, 49716 Meppen, Germany. If the parties are unable to resolve disputes, complaints, or differences of opinion at the respective working level, the dispute is escalated to the next highest management level. If no amicable solution can be found at this level either, the dispute is escalated to the executive level of Eviden Germany GmbH.

10 Limitations of liability

See General Terms and Conditions at the website of the ETC:
https://pki.atos.net/trustcenter/en/download/trusted-root-ca

11 Signatures

_____

Subscriber (last name, first name)

_____

Location, date

_____

Signature subscriber