An die:
Atos Information Technology GmbH
Trustcenter
Lohberg 10
49716 Meppen

Absender: _____

_____

_____

_____

_____

0. Präambel

Das Atos Trustcenter (ATC) ist als Trusted Root Certificate Authority registriert, gemäß ETSI EN 319 411-1 V1.2.2.
Das vorliegende Antragsdokument enthält neben den Informationen zur Beantragung eines Zertifikats auch die Verpflichtungen, die für den Antragsteller einhergehen. Diese sind detailliert beschrieben im Certificate Practice Statement (CPS).

Falls Antragsteller und Zertifikatsinhaber unterschiedliche Personen oder Entitäten sind, informiert der Antragsteller den Zertifikatsinhaber über seine Pflichten.

Das CPS ist verfügbar auf der Webseite des ATC unter: https://pki.atos.net

Das vorliegende Antragsdokument bildet zusammen mit dem CPS eine bindende Vereinbarung zwischen Antragsteller und ATC.

1. Informationen für den Antragsteller

1.1 Certificate Practice Statement

Das vorliegende Antragsdokument ist nur in Verbindung mit dem Certificate Practice Statement (CPS) gültig, verfügbar auf der Webseite des ATC. Änderungen des CPS werden dem Antragsteller per E-Mail mitgeteilt. Genutzt wird die dem ATC durch die Registrierung vorliegende E-Mail-Adresse des Antragstellers.

1.2 Veröffentlichung von Informationen

Das ATC veröffentlicht Zertifikate und Sperrlisten (Certificate Revocation Lists, CRL) zur Benutzung bspw. durch Antragsteller, Zertifikatsinhaber und Zertifikatsnutzer.
Vertrauliche Informationen werden generell nicht veröffentlicht, außer

- sie werden von der sie betreffenden Person selbst angefordert, oder
- sie sind auf Basis eines Gerichtsbeschlusses (oder vergleichbarer Legitimierung) einer hierdurch bestimmten Stelle vorzulegen.

1.3 Benötigte Produkte

Es sind keine bestimmten Produkte nötig für die Benutzung oder Anwendung der Schlüsselpaare und vom Trustcenter ausgestellten Zertifikate.

1.4 Benutzung der Zertifikate

Das ATC gibt folgende Nutzungseinschränkungen für die von ihm ausgestellten Zertifikate vor:

SSL-Zertifikate:
- Authentisierung von Domain Namen und Verschlüsselung des Kommunikationskanals

Client-Zertifikate:
- Digitale Signatur von Nachrichten oder Dateien zur Bestätigung der Urheberschaft und zur Ermöglichung der Überprüfung, ob signierte Nachrichten oder Dateien verändert oder verfälscht wurden.
- Digitale Verschlüsselung von Nachrichten oder Dateien zum Schutz ihrer Vertraulichkeit
- Benutzung in Client-Authentisierungen zur sicheren Identifikation und Autorisierung

CodeSigning-Zertifikate:
- Bestätigung des Autors einer Software
- Ermöglichung der Überprüfung, ob eine signierte Software verändert oder verfälscht wurde

1.5 Pflichten des Antragstellers

Die Pflichten des Antragstellers sind:
- Die vom Antragssteller angegebenen Antragsinformationen sind wahrheitsgemäß, fehlerfrei und nicht irreführend. Fehler des Antragstellers bei der Angabe der Informationen oder eine nicht erfolgte unverzügliche Korrektur falscher Angaben führen zur Sperrung des zugehörigen Zertifikats oder zugehöriger Zertifikate.
- Überprüfung des Zertifikatsinhalts auf Richtigkeit.
- Das Schlüsselpaar wird vom Antragsteller nur unter Berücksichtigung obiger Vorgaben zur *„Benutzung der Zertifikate“* genutzt.
- Der Antragsteller wendet angemessene Sorgfalt an, um eine unautorisierte Benutzung des privaten Schlüssels zu verhindern.
- Der Antragsteller verwaltet eine Nutzerkennung, ein Passwort und/oder eine PIN für den Zugriff auf den Webservices des ATC und für den Zugriff auf den privaten Schlüssel. Diese Informationen – und der private Schlüssel selbst – werden vom Antragsteller vertraulich behandelt und insbesondere nicht an Dritte weitergegeben.
- Der Antragsteller informiert das ATC unverzüglich, wenn
  - obige Pflichten innerhalb der Zertifikatslaufzeit verletzt werden,
  - der private Schlüssel des Antragstellers verloren, gestohlen oder kompromittiert wurde, oder die Kontrolle über den privaten Schlüssel nicht mehr gegeben ist oder
  - das/die für ihn ausgestellte Zertifikat(e) kompromittiert ist/sind.
- Wird das Zertifikat des Antragsteller für einen FQDN mit hohem Datenverkehr verwendet, muss der Antragsteller dafür sorgen, dass die OCSP Prüfung vom eingesetzten Server durch OCSP Stapling an den TLS/SSL-Handshake angehängt („stapled“) wird, siehe RFC4366

Falls Antragsteller und Zertifikatsinhaber unterschiedliche Personen oder Entitäten sind, informiert der Antragsteller den Zertifikatsinhaber über seine Pflichten.

1.6 Zertifikatssperrung

ATC sperrt (ein) für den Antragsteller ausgestellte(s) Zertifikat(e) wenn

(i) der Antragsteller einen schriftlichen oder elektronischen Sperrauftrag zum zugehörigen Zertifikat vorlegt;;
(ii) dem ATC bekannt wird, dass Angaben in einem Zertifikat nicht mehr korrekt sind;
(iii) dieses/diese Zertifikat(e) nicht mehr geänderten Standards entsprechen, bspw. Zertifizierungsnormen, Betriebsstandards oder hiervon abhängige Standards;
(iv) der Antragsteller gegen Auflagen des Antragsdokuments verstoßen hat;
(v) die Sicherheit der Zertifikats und/oder zugehörigem Private Key, oder die Sicherheit des Aussteller-CA-Zertifikat und/oder zugehörigem Private Key nicht mehr gegeben ist;
(vi) die Ausgabe des Zertifikats nicht nach den geltenden Anforderungen erfolgte;
(vii) der Antragsteller Malicious Software veröffentlicht oder sich fälschlicherweise für eine andere Identität ausgibt;
(viii) das Zertifikat auf der Grundlage von Betrug oder Fahrlässigkeit ausgestellt wurde (eingeschlossen sind auch Fälle bei Browserherstellern);
(ix) dieses ansonsten die Vertrauensstellung von Produkten beeinträchtigen würde;
(x) dieses für die Signatur und Verbreitung von Schadsoftware (u.a. Spyware, Malicious Software, Malware) genutzt wird.

Das ATC wird den Antragsteller über eine erfolgte Sperrung informieren.

1.7 Gültigkeitsprüfung des Zertifikats

Der Antragsteller ist verpflichtet, von ihm genutzte Zertifikate zunächst gegen die vom ATC bereitgestellte Sperrliste (CRL) zu prüfen. Die Prüfung sollte vor jeder Nutzung, mindestens aber monatlich erfolgen.

1.8 Protokollierung Informationen zum Zertifikatslebenszyklus

ATC erhebt und speichert aus juristischen Gründen Protokollinformationen und alle Informationen zum Zertifikatslebenszyklus, Schlüssel- und Zertifikatsmanagement.
Die Aufbewahrungsdauer dieser Informationen ist festgelegt im CPS.

2. Allgemeine Geschäftsbedingungen

Es gelten die Allgemeinen Geschäftsbedingungen für Dienstleistungen der Atos Information Technology GmbH.

3. Preise

Das ATC stellt dem Antragsteller für seine Dienstleistungen entsprechende Preise in Rechnung. Die Preisliste wird dem Antragsteller auf Anfrage zur Verfügung gestellt.

4. Schutz personenbezogener Daten

Das Atos Trustcenter stellt sicher, dass alle geltenden gesetzlichen Anforderungen (einschließlich der Datenschutz-Grundverordnung (DSGVO)) zum Schutz vor Verlust, Zerstörung und Veränderung der Daten berücksichtigt werden.

Die Vertragspartner beachten alle geltenden Datenschutzbestimmungen und stellen sicher, dass ihre Mitarbeiter zur Einhaltung der Vorschriften verpflichtet werden.

Das Atos Trustcenter stellt sicher, dass alle Anforderungen der EU General Data Protection Regulation zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, in Deutschland umgesetzt durch die DSGVO erfüllt werden.

Angemessene technische und organisatorische Maßnahmen werden zum Schutz vor unautorisierter und nicht gesetzeskonformer Verarbeitung, Verlust oder Zerstörung sowie Beschädigung von personenbezogenen Daten wie in der DSGVO Art. 32 beschrieben ergriffen.

Alle Informationen, die von Benutzern des Atos Trustcenters zur Verfügung gestellt werden, werden nicht ohne das Einverständnis des Betroffenen, eine gerichtliche Anordnung oder anderen rechtlichen Autorisierungen herausgegeben.

Das Atos Trustcenter stellt dauerhaft den Schutz der Privatsphäre von Informationen Betroffener sicher.

_____

Antragsteller (Name, Vorname)

_____

Ort, Datum

_____

Unterschrift Antragsteller