aconet
Austrian Academic Computer Network

ACOnet-Teiln.-Nr.

Zusatzvereinbarung
zur ACOnet-Teilnahmevereinbarung
betreffend die Nutzung des Trusted Certificate Service

Die Universität Wien, vertreten durch den Zentralen Informatikdienst, als Betreiber des österreichischen akademischen Computernetzes ACOnet, im Folgenden kurz „Betreiber“ genannt, und

_____

Name der an ACOnet teilnehmenden Institution

im Folgenden kurz „Teilnehmer“ genannt, treffen zusätzlich zur bestehenden ACOnet-Teilnahmevereinbarung die folgende Zusatzvereinbarung zum Zweck der Ausstellung von digitalen Zertifikaten im Rahmen des Trusted Certificate Service:

§ 1 Grundlagen

(1) Der Betreiber ist Mitglied der GÉANT Association, Amsterdam, Niederlande, dem Dachverband der europäischen Wissenschaftsnetze. Die GÉANT Association hat im Auftrag ihrer Mitglieder das Trusted Certificate Service ins Leben gerufen und zu diesem Zweck mit einem geeigneten Zertifikatsanbieter einen entsprechenden Reseller-Vertrag abgeschlossen.

(2) Durch den Vertrag betreffend das TCS, abgeschlossen am 20.04.2020 zwischen der GÉANT Association und der Universität Wien, nimmt der Betreiber am Trusted Certificate Service (TCS) teil. Alle relevanten Dokumente, wie z.B. die Certification Practice Statements, Terms of Use und weitere Agreements, bzw. Verweise darauf, sind unter https://tcs.aco.net/ zu finden bzw. von dort verlinkt.

(3) Sollte der in Abs. 2 genannte Vertrag betreffend das TCS erlöschen, so erlischt auch die gegenständliche Zusatzvereinbarung. In diesem Fall wird der Betreiber den Teilnehmer zum frühest möglichen Zeitpunkt über die Konsequenzen für die weitere Bereitstellung von digitalen Zertifikaten informieren.

§ 2 Vertragsgegenstand

(1) Der Betreiber ermöglicht dem Teilnehmer die unentgeltliche Ausstellung von digitalen Zertifikaten im Rahmen des TCS unter den in dieser Vereinbarung beschriebenen Voraussetzungen (siehe § 3).

(2) Insbesondere folgende Arten digitaler Zertifikate werden ausgestellt:
- Server-Zertifikate, zur Authentifizierung von Servern und TLS/SSL-Verschlüsselung der Kommunikation zwischen Client und Server;
- persönliche Zertifikate zur Identifikation individueller Benutzer und Verschlüsselung der Email-Kommunikation;
- Code-Signing Zertifikate zur Authentifizierung von Software, die über das Internet verteilt wird.

(3) Der Teilnehmer ernennt zumindest eine Person als „TCS Admin Kontakt“, die gegenüber dem Betreiber ermächtigt ist, Anträge auf Ausstellung von Zertifikaten im Namen des Teilnehmers zu validieren (siehe § 5). Darüber hinaus hat der „TCS Admin Kontakt“ weitere administrative Rechte im Portal des Zertifikatsanbieters. Dazu zählen z.B. das Anlegen von Benutzern inkl. Rechteverwaltung, die Angabe von zu validierenden Organisationen und Domains, so wie die Administration etwaiger Federation Parameter.

(4) Ausstellung von Zertifikaten:

- Server Zertifikate: Der jeweilige Antragsteller aus dem Zuständigkeitsbereich des Teilnehmers stellt seinen Antrag auf Ausstellung eines Zertifikats online im Webportal des Zertifikatsanbieters (weiterführende Links auf https://tcs.aco.net/). Die Ausstellung des Zertifikats erfolgt automationsunterstützt, sobald der „TCS Admin Kontakt“ den Antrag bestätigt und dieser vom Zertifikatsanbieter validiert wurde. Der betreffende Antragsteller erhält das signierte Zertifikat per Email bzw. direkt im Webportal.
- Persönliche Zertifikate: Der jeweilige Antragsteller aus dem Zuständigkeitsbereich des Teilnehmers stellt seinen Antrag auf Ausstellung eines Zertifikats online im Webportal des Zertifikatsanbieters. Die Ausstellung des Zertifikats erfolgt automationsunterstützt. Der betreffende Antragsteller erhält das signierte Zertifikat per Email bzw. direkt im Webportal.
- Code Signing Zertifikate: Der jeweilige Antragsteller aus dem Zuständigkeitsbereich des Teilnehmers stellt seinen Antrag auf Ausstellung eines Zertifikats online im Webportal des Zertifikatsanbieters. Die Ausstellung des Zertifikats erfolgt automationsunterstützt, sobald der „TCS Admin Kontakt“ den Antrag bestätigt und dieser vom Zertifikatsanbieter validiert wurde. Der betreffende Antragsteller erhält das signierte Zertifikat per Email bzw. direkt im Webportal.

§ 3 Voraussetzungen

(1) Der Teilnehmer erklärt, die Bestimmungen aller relevanten Dokumente (siehe §1, Abs. 2) zu kennen und einzuhalten und ist insbesondere dafür verantwortlich, den bzw. die von ihm, als „TCS Admin Kontakt“ ermächtigten Personen, zur Einhaltung dieser Bestimmungen zu verpflichten.

(2) Server-Zertifikate dürfen nur für Services des Teilnehmers ausgestellt werden, die im Einklang mit der ACOnet Acceptable Use Policy stehen.

(3) Der Teilnehmer ist für die Richtigkeit der dem Betreiber im Zusammenhang mit der Zertifikatsausstellung übermittelten Daten verantwortlich und wird den Betreiber unverzüglich darüber informieren, wenn sich während der Gültigkeitsdauer eines Zertifikats allfällige Daten, die im Zuge der Zertifikatsausstellung angegeben wurden, geändert haben.
Insbesondere gilt das für jene Daten, die bei Beantragung eines persönlichen Zertifikats zur Bestätigung der Identität des Antragsstellers übermittelt werden. Die Richtigkeit dieser Daten muss durch entsprechende Maßnahmen (z.B. Bestätigung der Identität durch Ausweiskontrolle vor der Berechtigungsvergabe zur Nutzung des Service) sichergestellt sein und auch fortlaufend, für die Dauer der Gültigkeit des ausgestellten Zertifikates, gewährleistet werden.

(4) Der Teilnehmer ist verantwortlich, geeignete Maßnahmen gegen den Missbrauch von Zertifikaten zu setzen und den Widerruf („Revocation“) eines Zertifikats durchzuführen, wenn die Sicherheit eines Zertifikats substantiell beeinträchtigt ist (z.B. durch Kompromittierung des betreffenden „private key“).

(6) Der Betreiber ist berechtigt, ausgestellte Zertifikate gegebenenfalls zu widerrufen.

§ 4 Rechtspersönlichkeit des Teilnehmers

(1) Voraussetzung für die Ausstellung von digitalen Zertifikaten im Wege des Betreibers ist der schriftliche Nachweis der Rechtspersönlichkeit des Teilnehmers mit der Angabe der vertretungsbefugten Personen (Firmenbuchauszug, Vereinsregisterauszug oder dgl.). Das entsprechende Dokument zum Nachweis der Rechtspersönlichkeit des Teilnehmers bildet die Beilage 1 zur gegenständlichen Zusatzvereinbarung.

(2) Die Universitäten gemäß § 6 UG 2002 sind von der Beibringung eines schriftlichen Nachweises ihrer Rechtspersönlichkeit befreit, da ihre Rechtspersönlichkeit durch Gesetz geregelt ist. Als vertretungsbefugt für die Universität gilt im Zusammenhang mit der gegenständlichen Vereinbarung neben dem Rektor (Vizerektor), auch der Leiter des Zentralen Informatikdiensts der betreffenden Universität.

(3) Für die Einrichtung und Validierung der Teilnehmer-Organisation beim Zertifikatsanbieter sind die Details in Beilage 2 anzugeben. Als Name der Organisation ist ein in qualifizierten Informationsquellen (z.B. Firmenbuch, Gesetz) angeführter Name zu verwenden.

(4) Jede Änderung der Rechtspersönlichkeit des Teilnehmers oder seiner vertretungsbefugten Personen ist dem Betreiber unverzüglich durch ein gültiges Dokument im Sinne von Abs. 1 zu melden.

§ 5 Autorisierte Vertreter des Teilnehmers

(1) Gemäß § 2 Abs. 3 ernennt der Teilnehmer zumindest einen persönlichen autorisierten Vertreter („TCS Admin Kontakt“), der in Beilage 3 angegeben ist.

(2) Tritt hinsichtlich der in Beilage 3 genannten autorisierten Vertreter eine Änderung ein, ist dies unverzüglich dem Betreiber zu melden. Die Änderung der Vertretungsbefugnisse erfolgt durch Übermittlung einer neuen, vollständig ausgefüllten und vom Teilnehmer unterzeichneten Beilage 3, welche die aktuellen Vertretungsbefugnisse dokumentiert.

(3) Der Betreiber ist berechtigt, die vom Teilnehmer in der Beilage 3 genannten autorisierten Vertreter periodisch mit den Berechtigten im Portal der Zertifikatsanbieters abzugleichen und gegebenenfalls anzupassen.

§ 6 Domains des Teilnehmers

(1) Es dürfen nur Domains zur Validierung beantragt werden, die dem Teilnehmer über die Registrierung eindeutig zuzuordnen sind.

§ 7 Email-Adressen für persönliche Zertifikate

(1) Persönliche Zertifikate dürfen ausschließlich für ‘institutionelle’ Email-Adressen ausgestellt werden, also jene Email-Adressen, die dem Antragsteller vom Teilnehmer als dessen Heimatorganisation und „Identity Provider (IdP)“ zur Verfügung gestellt werden.

(2) Wenn die E-Mail-Adresse des Antragsstellers vom Teilnehmer automatisiert übermittelt wird, hat der Teilnehmer dafür Sorge zu tragen, dass nur jene Email-Adressen übertragen werden, die im Verantwortungsbereich des Teilnehmers liegen.

§ 8 Vertragsdauer

(1) Diese Zusatzvereinbarung wird auf unbestimmte Zeit abgeschlossen und kann von beiden Partnern jederzeit ohne Angabe von Gründen schriftlich gekündigt werden. Für den Betreiber gilt hierbei jedoch eine Kündigungsfrist von drei Monaten.

(2) Mit Beendigung der ACOnet-Teilnahmevereinbarung endet gleichzeitig auch jede Zusatzvereinbarung.

(3) Aus wichtigen Gründen (z. B. im Falle von groben Verstößen des Teilnehmers oder im Falle des Erlöschens der Verträge nach § 1, etc.) kann der Betreiber die Zusatzvereinbarung sofort, ohne Einhaltung einer Frist, kündigen.

(4) Bei Beendigung dieser Vereinbarung werden ausgestellte Zertifikate nach Ablauf von 30 Tagen widerrufen.

Beilagen zur Zusatzvereinbarung:

Beilage 1: Nachweis der Rechtspersönlichkeit des Teilnehmers (siehe § 4 Abs. 1)
Beilage 2: Details zur Teilnehmer-Organisation (siehe § 4 Abs. 3)
Beilage 3: Autorisierte Vertreter des Teilnehmers (siehe § 5 Abs. 1)

Für den Teilnehmer:

_____

Datum Name Unterschrift

Für den Betreiber:

_____

Datum Name Unterschrift

aconet
Austrian Academic Computer Network

ACOnet-Teiln.-Nr.

Beilage 2

zur Zusatzvereinbarung betreffend die Nutzung des Trusted Certificate Service

Details zur Teilnehmer-Organisation[1]

Name der Organisation: _____

Adresse: _____

Stadt: _____

Postleitzahl: _____

Bundesland: _____

Der Teilnehmer hat die Möglichkeit, die privaten Schlüssel von im Portal erzeugten persönlichen Zertifikaten von TCS Administratoren des Teilnehmers wiederherstellen zu lassen. Da diese Möglichkeit beim Anlegen der Organisation festgelegt werden muss und nachträglich nicht mehr geändert werden kann, muss eine der beiden folgenden Optionen gewählt werden:

☐ **Wir wollen die Möglichkeit haben, private Schlüssel von persönlichen Zertifikaten im Notfall wiederherstellen zu können.**

☐ **Wir verzichten auf die Möglichkeit, private Schlüssel von persönlichen Zertifikaten im Notfall wiederherstellen zu können.**

Für den Teilnehmer:

_____

Datum Name Unterschrift

[1] Nähere Informationen zu den Optionen und Feldern finden sie unter https://tcs.aco.net/

Austrian Academic Computer Network

ACOnet-Teiln.-Nr.

Beilage 3

zur Zusatzvereinbarung betreffend die Nutzung des Trusted Certificate Service

TCS Admin Kontakt:

Vor- und Zuname: _____

E-Mail-Adresse: _____

Telefonnummer: _____

EPPN[2] (für federated login): _____

Unterschrift des Admin Kontakt: _____

TCS Admin Kontakt:

Vor- und Zuname: _____

E-Mail-Adresse: _____

Telefonnummer: _____

EPPN[2] (für federated login): _____

Unterschrift des Admin Kontakt: _____

Für den Teilnehmer:

_____

Datum Name Unterschrift

[2] optional – *eduPersonPrincipalName* für Teilnehmer der ACOnet Identity Federation (https://eduid.at)