ACOnet-Teilnehmer-Nummer:

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

Die Universität Wien, vertreten durch den Zentralen Informatikdienst, als Betreiber des österreichischen wissenschaftlichen Datennetzes 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 (TCS):

§ 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, sind unter **www.aco.net/tcs** 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 frühestmöglichen 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*innen und Verschlüsselung der E-Mail-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 Benutzer*innen inkl. Rechteverwaltung, die Angabe von zu validierenden Organisationen und Domains sowie die Administration etwaiger Federation-Parameter.

(4) Ausstellung von Zertifikaten:

- Server-Zertifikate und Code-Signing-Zertifikate: Der*die jeweilige Antragsteller*in aus dem Zuständigkeitsbereich des Teilnehmers stellt seinen*ihren Antrag auf Ausstellung eines Zertifikats online im Webportal des Zertifikatsanbieters (weiterführende Links unter **www.aco.net/tcs**). Die Ausstellung des Zertifikats erfolgt automationsunterstützt, sobald der „TCS Admin-Kontakt“ den Antrag bestätigt und dieser vom

Zertifikatsanbieter validiert wurde. Der*die betreffende Antragsteller*in erhält das signierte Zertifikat per E-Mail bzw. direkt im Webportal.

- Persönliche Zertifikate: Der*die jeweilige Antragsteller*in aus dem Zuständigkeitsbereich des Teilnehmers stellt seinen*ihren Antrag auf Ausstellung eines Zertifikats online im Webportal des Zertifikatsanbieters (weiterführende Links unter **www.aco.net/tcs**). Die Ausstellung des Zertifikats erfolgt automationsunterstützt. Der*die betreffende Antragsteller*in erhält das signierte Zertifikat per E-Mail 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, die von ihm als „TCS Admin-Kontakt“ ermächtigte(n) Person(en) 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 (verfügbar unter **www.aco.net/download**) 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 von persönlichen Zertifikaten zur Bestätigung der Identität der Antragssteller*innen 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 Zertifikats, gewährleistet werden.

(4) Der Teilnehmer ist dafür 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“).

(5) Der Betreiber ist berechtigt, ausgestellte Zertifikate 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 dergleichen). 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*der Rektor*in (Vizerektor*in) auch der*die Leiter*in des Zentralen Informatikdienstes (IT-Abteilung) 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 Vertretungspersonen des Teilnehmers

(1) Gemäß § 2 Abs. 3 ernennt der Teilnehmer zumindest eine persönlich autorisierte Vertretungsperson („TCS Admin-Kontakt“), die in Beilage 3 angegeben ist.

(2) Tritt hinsichtlich der in Beilage 3 genannten autorisierten Vertretungspersonen 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 Beilage 3 genannten autorisierten Vertretungspersonen 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 E-Mail-Adressen für persönliche Zertifikate

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

(2) Wenn die E-Mail-Adressen der Antragssteller*innen vom Teilnehmer automatisiert übermittelt werden, hat der Teilnehmer dafür Sorge zu tragen, dass nur jene E-Mail-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) 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 Vertretungspersonen des Teilnehmers (siehe § 5 Abs. 1)

Für den Teilnehmer:

Datum	Name	Unterschrift

Für den Betreiber:

Datum	Name	Unterschrift

ACOnet-Teilnehmer-Nummer:

Beilage 2
zur Zusatzvereinbarung betreffend die Nutzung des Trusted Certificate Service

Nähere Informationen zu den angeführten Feldern und Optionen finden Sie in den TCS-FAQs (verlinkt unter **www.aco.net/tcs**).

Details zur Teilnehmer-Organisation

Name der Organisation:	
Adresse:	
Postleitzahl, Ort:	
Bundesland:	

Wiederherstellung privater Schlüssel

Der Teilnehmer hat auf Wunsch die Möglichkeit, die privaten Schlüssel von im Webportal des Zertifikatsanbieters erzeugten persönlichen Zertifikaten durch TCS-Administrator*innen des Teilnehmers wiederherstellen zu lassen.

Da diese Möglichkeit beim Anlegen der Organisation festzulegen ist und nachträglich nicht mehr geändert werden kann, muss eine der beiden folgenden Optionen gewählt werden:

☐ **Ja**, wir wollen private Schlüssel von persönlichen Zertifikaten im Notfall wiederherstellen können.

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

Für den Teilnehmer:

Datum	Name	Unterschrift

ACOnet-Teilnehmer-Nummer:

Beilage 3
zur Zusatzvereinbarung betreffend die Nutzung des Trusted Certificate Service

Bitte nennen Sie nachfolgend zumindest eine persönlich autorisierte Vertretungsperson als „TCS Admin-Kontakt“ gemäß § 2 Abs. 3.

Das Feld „ePPN für Federated Login“ ist optional – Teilnehmer der ACOnet Identity Federation (siehe **www.aco.net/federation**) können hier den eduPersonPrincipalName (ePPN) der Vertretungsperson(en) angeben, um ein Federated Login zu ermöglichen.

TCS Admin-Kontakte

Vor- und Nachname:

E-Mail-Adresse:

ePPN für Federated Login:

Vor- und Nachname:

E-Mail-Adresse:

ePPN für Federated Login:

Vor- und Nachname:

E-Mail-Adresse:

ePPN für Federated Login:

Für den Teilnehmer:

Datum Name Unterschrift

Bitte füllen Sie das Formular vollständig aus. Senden Sie dann das digital signierte Formular per E-Mail an **tcs@aco.net** (die Signatur muss mittels **www.signaturpruefung.gv.at** überprüfbar sein) oder senden Sie das ausgedruckte Formular mit Ihrer Originalunterschrift per Post an **Universität Wien, Zentraler Informatikdienst, Abteilung ACOnet & VIX, Universitätsstraße 7, 1010 Wien**. In beiden Fällen retournieren wir das von uns digital gegengezeichnete Dokument per E-Mail an die Adresse unseres administrativen Kontakts bei Ihrer Teilnehmerorganisation.