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 (derzeit: DigiCert Inc., Lehi, Utah, USA).

(2) Durch den Vertrag betreffend das TCS, abgeschlossen am 04.05.2015 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.

(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 Administrative Contact“, die gegenüber dem Betreiber ermächtigt ist, Anträge auf Ausstellung von Zertifikaten im Namen des Teilnehmers zu validieren (siehe § 5). Darüber hinaus hat der „TCS Administrative Contact“ 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 des „SAML Organization Mappings“.

(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 Administrative Contact“ 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 Webortal des Zertifikatsanbieters. Die Ausstellung des Zertifikats erfolgt automationsunterstützt, sobald der „TCS Administrative Contact“ 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 des „TCS Model Subscriber Agreement“ (siehe Beilage 3) zu kennen und einzuhalten und ist insbesondere dafür verantwortlich, den bzw. die von ihm, als „TCS Administrative Contact“ 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) Persönliche Zertifikate können nur beantragt werden, wenn der Teilnehmer, als Heimatorganisation und "Identity Provider" (IdP) des Antragstellers, auch an der ACOnet Identity Federation (siehe https://www.eduid.at/) und der Interfederation edugain (siehe https://www.aco.net/edugain.html) teilnimmt.
Um den Antragsteller im Rahmen der ACOnet Identity Federation eindeutig identifizieren zu können, ist ein spezielles SAML Attribut (schacHomeOrganization, urn:oid:1.3.6.1.4.1.25178.1.2.9) nötig, dessen Wert im Portal des Zertifikatsanbieters angegeben werden muss.

(4) 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.

(5) 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 im Einklang mit den Bestimmungen des „TCS Model Subscriber Agreement“ (siehe §3 Abs. 1) 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) 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 Administrative Contact“), der in Beilage 2 angegeben ist.

(2) Tritt hinsichtlich der in Beilage 2 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 2, welche die aktuellen Vertretungsbefugnisse dokumentiert.

(3) Der Betreiber ist berechtigt, die vom Teilnehmer in der Beilage 2 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 werden ausschließlich für ‘institutionelle’ Email-Adressen ausgestellt, also jene Email-Adressen, die dem Antragsteller vom Teilnehmer als dessen Heimatorganisation und „Identity Provider (IdP)“ zur Verfügung gestellt werden.

(2) Da die Email-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: Autorisierte Vertreter des Teilnehmers (siehe § 5 Abs. 1)
Beilage 3: TCS Model Subscriber Agreement

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

TCS Administrative Contact:

Vor- und Zuname: ----------

eMail-Adresse: ----------

Telefon-Nr.: ----------

ACOnet-Portal-UserId: ----------

Unterschrift des Administr. Contact: ----------

TCS Administrative Contact:

Vor- und Zuname: ----------

eMail-Adresse: ----------

Telefon-Nr.: ----------

ACOnet-Portal-UserID: ----------

Unterschrift des Administr. Contact: ----------

Für den Teilnehmer:

_____

Datum Name Unterschrift

aconet
Austrian Academic Computer Network

ACOnet-Teiln.-Nr.

Beilage 3

zur Zusatzvereinbarung betreffend die Nutzung des Trusted Certificate Service

As a Registration Authority, the Subscriber hereby agrees to the following terms:

1. Applicability. The terms cover each digital certificate issued to a Subscriber under the agreement with the GÉANT Association, regardless of (i) the digital certificate type (email, code signing, or TLS/SSL), (ii) when the Subscriber requests the digital certificate, or (iii) when the digital certificate actually issues. The Subscriber may not request a certificate with contents that infringe on the intellectual property rights of another entity.
2. Private Key Generation. The Subscriber must keep all Private Keys confidential and use reasonable measures to protect the Private Key from disclosure. The Subscriber must request revocation of the Certificate within one working day of any suspected misuse or compromise of a Certificate or Private Key. The Subscriber must generate its key pair using one of the following methods: (i) inside a secure hardware token, (ii) using trustworthy cryptographic software on a local computer system where it is the sole user and administrator, (iii) on a computer system administered by its sponsor or a third party if (a) the key material is generated using trustworthy cryptographic software, (b) access is limited to designated individuals, who are subject to and aware of applicable privacy rules and a professional code of conduct, (c) the private key and pass phrase are not sent in clear text over a network, (d) the encrypted private key file is not sent over the network unprotected, (e) the system is located in a secure environment, where access is controlled and limited to only authorized personnel, and (f) a system does not persistently keep pass phrases or plain text private keys for longer than 24 hours.
3. IGTF Private Key Storage. Subscribers of Certificates issued as a 'Grid Certificate' must store and protect Private Keys in accordance with the applicable and current Grid policy.
4. Certificate Transparency. To ensure Certificates function properly throughout their lifecycle, the Subscriber must permit DigiCert to log SSL Certificates with a public certificate transparency database. Because this will become a requirement for Certificate functionality, Subscribers cannot opt out of this process and expressly agree to log their Certificates. Log server information is publicly accessible. Once submitted, information cannot be removed from a log server.
5. **Restrictions**. Subscribers may not (a) share their Certificate or Private Key with another user except where permitted by the CPS, (b) use a Certificate or Private Key to operate nuclear power facilities, air traffic control systems, aircraft navigation systems, weapons control systems, or any other system requiring failsafe operation whose failure could lead to injury, death or environmental damage, (c) modify, sub license, reverse-engineer or create a derivative work of any Certificate (except as required to use the Certificate for its intended purpose) or Private Key, (d) use or make representations about a Certificate except as allowed in the CPS, (e) impersonate or misrepresent your affiliation with any entity or use a Certificate in a manner that could reasonably result in a civil or criminal action being taken against the Subscriber or DigiCert, (f) use a Certificate to send or receive unsolicited bulk correspondence, sign or distribute any files, software, or code that may damage the operation of another's computer or that is downloaded without a user's consent, or breach the confidence of a third party, (g) attempt to use a Certificate to issue other Certificates, except that a Subscriber may use the Certificate to create proxy certificates as defined in RFC 3820, or (h) intentionally create a Private Key that is substantially similar to a DigiCert or third party Private Key. Subscribers are solely responsible for ensuring your Certificates are renewed prior to their expiration.
6. Revocation. DigiCert may revoke a Subscriber's Certificate without notice for the reasons stated in the CPS, including if DigiCert believes that (a) the Subscriber or the Certificate's Subject requested revocation of the Certificate or did not authorize the Certificate's issuance, (b) the Subscriber or the Certificate's Subject breach its obligations under the agreement with the GÉANT Association or an NREN or fail to comply with the CPS, (c) a provision of this agreement containing a representation or obligation related to the issuance, use, management, or revocation of the Certificate terminates or is held invalid, (d) the Subscriber or the Certificate's Subject are added to a government prohibited person or entity list or are operating from a prohibited destination under the laws of the United States, (e) the Certificate contains inaccurate or misleading information, (f) the Certificate was used

outside of its intended purpose or used to sign malicious software; (g) the Private Key associated with a Certificate was disclosed or compromised, (h) this agreement terminates, (i) the Certificate was used or issued, directly or indirectly, contrary to law, the CPS, or industry standards, (j) industry standards or DigiCert's CPS require revocation, or (k) revocation is necessary to protect the rights, confidential information, operations, or reputation of DigiCert or a third party.

7. Relying Party Warranties. DigiCert's Relying Party Warranty (https://www.digicert.com/docs/agreements/DigiCert_RPA.pdf) is only for the benefit of entities other than the Subscriber that act in reliance on a Certificate or a Digital Signature. Subscribers do not have rights under the warranty, including any right to enforce the terms of the warranty or make a claim under the warranty.
8. Remedy. A Subscriber's sole remedy for a defect in a Certificate is to have DigiCert use reasonable efforts to correct the defect. DigiCert is not obligated to correct a defect if (i) the Certificate was misused, damaged, or modified, (ii) the Subscriber did not promptly report the defect to DigiCert, or (iii) Subscriber has failed to abide by the GÉANT Association agreement.
9. Software and Equipment. Subscribers are solely responsible for their own conduct, software, website maintenance, operation, development, security and content, and all computers, telecommunication equipment, software, access to the Internet, and communications networks (if any) required to access and use the Certificates.
10. Warranty Disclaimers. THE CERTIFICATES, AND ANY RELATED SOFTWARE, PRODUCTS, AND SERVICES ARE PROVIDED "AS IS" AND "AS AVAILABLE". TO THE MAXIMUM EXTENT PERMITTED BY LAW, DIGICERT DISCLAIMS ALL EXPRESS AND IMPLIED WARRANTIES, INCLUDING WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT. DIGICERT DOES NOT WARRANT THAT ANY SERVICE OR PRODUCT WILL MEET YOUR EXPECTATIONS OR THAT ACCESS TO THE ACCOUNT WILL BE TIMELY OR ERRORFREE. Use of a SHA-1 Certificate will result in errors displayed by Application Software Vendors.
11. Limitation on Liability. The agreement is not required to limit a party's liability for (i) death or personal injury resulting from the negligence of a party or (ii) fraud or fraudulent statements made by a party. EXCEPT AS STATED ABOVE, THE SUBSCRIBER MUST AGREE TO LIMIT DIGICERT'S MAXIMUM LIABILITY RESULTING FROM THE CERTIFICATE TO THE AMOUNT SPECIFIED IN THIS AGREEMENT. SUBSCRIBER MUST AGREE THAT DIGICERT IS NOT LIABLE FOR ANY INDIRECT, CONSEQUENTIAL, SPECIAL, OR PUNITIVE DAMAGES OR ANY LOSS OF PROFIT, REVENUE, DATA, OR OPPORTUNITY, EVEN IF DIGICERT IS AWARE OF THE POSSIBILITY OF SUCH DAMAGES. The limitations must apply to the maximum extent permitted by law and apply regardless of (i) the reason for or nature of the liability, including tort claims, (ii) the number of claims of liability, (iii) the extent or nature of the damages, or (iv) whether any other provisions of this agreement were breached or proven ineffective.
12. Indemnification. To the extent permitted by law, Subscriber must indemnify, hold harmless, and defend DigiCert against all third party claims and all related liabilities, damages, and costs, including reasonable attorneys' fees, arising from Subscriber's breach of these terms.