FAQ

Frequently Asked Questions (work in progress, noch nicht alle FAQs entsprechen dem Service ab 01.07.)

Allgemein

TLS/SSL Zertifikate

Email Zertifikate

Allgemein

Was ist TCS?

TCS steht für Trusted Certificate Service.

GEANT, der Verband europäischer Wissenschaftsnetze, hat einen Rahmenvertrag über die Vergabe und Verwaltung von X.509 Zertifikaten mit der Firma Digicert als CA (Certificate Authority) abgeschlossen und stellt dieses Service als Trusted Certificate Service (TCS) allen teilnehmenden Wissenschaftsnetzen zur Verfügung.

ACOnet ist diesem Vertrag ebenfalls beigetreten und stellt Zertifikate für ACOnet Teilnehmer unentgeltlich und in unlimitierter Anzahl zur Verfügung. ACOnet Teilnehmerorganisationen können, auf Basis der Zusatzvereinbarung zur ACOnet-Teilnahmevereinbarungbetreffend die Nutzung des Trusted Certificate Service, TCS Zertifikate beantragen. Die Zusatzvereinbarung muss von einer für die teilnehmende Institution zeichnungsberechtigten Person im Original unterfertigt und mit den geforderten Beilagen per Post an ACOnet gesendet werden, siehe auch http://tcs.aco.net/.

Was ist ein TCS-Admin?

Jede ACOnet Teilnehmerorganisation die das Zertifikatsservice nutzen will, muss zumindest eine/n, sollte aber mehr als eine/n, TCS Administrator/in angeben und diese/n in die Zusatzvereinbarung eintragen. Für entsprechend authentifizierte und autorisierte TCS AdministratorInnen haben im Digicert Portal die Möglichkeit, beantragte Zertifikate ihrer eigenen Organisation zu sehen, zu bestätigen, abzulehnen oder zu widerrufen.

Was ist DCV (Domain Control Validation)?

Bei der registrierung einer neuen Domain im Digicert Portal, wird durch Digicert mittels DCV automatisiert überprüft, ob die Person, die die Validierung einer Domain angestossen hat (TCS-Admin), auch "Kontrolle" über den bzw die Domain-Namen hat.

Hierzu sendet der DCV Mechanismus ein E-Mail mit einem jeweils eindeutigen Code an einen definierten Satz von Adressen. Dieser Code wird durch den/die Empfänger dieser DCV Mails zur Validierung auf einer Webseite von Digicert (*Link im Mail*) validiert (Email Challenge-Response Verfahren).
Erst nach dieser Validierung (bei Multi-Domain-Zertifikaten je Domain) wird das Zertifikat ausgestellt.

Folgende 5 generische Email-Adressen stehen immer zur Verfügung:

- hostmaster@domain_name
- postmaster@domain_name
- webmaster@domain_name
- administrator@domain_name
- admin@domain_name

Initial wird das DCV Mail jedoch an alle Email-Adressen, die im 'whois-record' der Domain als tech- oder admin-contact gelistet sind, gesandt. Die generischen Email-Adressen können notfalls nachträglich ausgewählt werden, um auch dorthin das DCV Mail gesendet zu bekommen, weiters sind diese Adressen nicht nur für den Domainnamen des Zertifikats verfügbar, sondern auch für Domains "darüber":
z.B. um ein Zertifikat für www.bla.muh.ac.at zu erhalten, stehen folgende Mail-Domains für die DCV Bestätigung zur Verfügung:

- @www.bla.muh.ac.at
- @bla.muh.ac.at
- @muh.ac.at

TLS/SSL Zertifikate

SHA-1 deprecation bzw. Wie komme ich zu einem mit SHA-2 signierten Zertifikat?

siehe Informationen zu SHA-2

Erstellen eines "keypairs"

siehe Erstellen des Keypairs.

Mein fertiges Zertifikat wird vom Browser als ungültig zurückgewiesen. Was kann ich dagegen tun?

Wahrscheinlich haben Sie vergessen, die **Intermediate Zertifikate** mitzugeben (siehe Verwendung des Zertifikats mit Apache HTTP Server). Es ist essentiell wichtig, dass die beiden Intermediate-Zertifikate am Server mitgelinkt werden.

Verwendung des Zertifikats mit Apache HTTP Server

Das ausgestellte Zertifikat müssen Sie mit den sogenannten Intermediate-Zertifikaten in Ihre Applikation einbauen. Beim Apache HTTP Server sieht das beispielsweise folgendermaßen aus:

```
SSLEngine on
SSLCertificateFile /etc/httpd/ssl.crt/certificate.pem
SSLCACertificateFile /etc/httpd/ssl.crt/chain.pem
SSLCertificateKeyFile  /etc/httpd/ssl.crt/certificate.key
```

- certificate.pem ist Ihr neu ausgestelltes und unterschriebenes Zertifikat
- chain.pem ist die Datei mit den benötigten Intermediate-Zertifikaten. Die Intermediate-Zertifikate finden sie auf der selben Webseite, wo sie auch ihr Zertifikat abholen. Das Root CA Zertifikat sollte Ihr SSL CLient (Browser, Mailprogramm, etc) bereits kennen und dieses ist daher nur der Vollständigkeit halber angegeben.
- certificate.key ist Ihr anfangs erstelltes Keyfile.

Verwendung des Zertifikats mit Microsoft IIS

Falls das Intermediate Certificate unter Windows IIS nicht mitausgeliefert wird, hat Digicert eine Anleitung dazu verfasst: Digicert Support

Internet Explorer weist mein Zertifikat als ungültig zurück, Firefox akzeptiert es aber

Browser cachen verschiedene Zertifikate mit unterschiedlichem Verhalten. Wahrscheinlich hatte in diesem Fall Firefox die Intermediate-Zertifikate im Cache und daher konnte er das Zertifikat validieren. Um das Problem zu beheben müssen Sie noch die Intermediate Zertifikate installieren.