TCS wrt Digicert

TCS und Digicert - TCS neu seit 01.07.2015

Da der Vertrag mit der bisherigen CA des Zertifikatsservice, nämlich Comodo, mit 30.06.2015 endete, wurde bereits 2014 eine Ausschreibung zur Nachfolge durchgeführt, die Digicert gewonnen hat. Somit ist Digicert seit 01.07.2015 die neue CA für das Zertifikatsservice. Allerdings macht die neue CA auch eine neue Version (v3.0) der "Zusatzvereinbarung zur Teilnahme am ACOnet Zertifikatsservice" nötig. Sobald diese unterschrieben bei uns einlangt, können wir die notwendigen Schritte bei Digicert setzen, um den produktiven Einsatz des Digicert Portals zur Ausstellung von Zertifikaten zu ermöglichen.

Dokumentation

Abgesehen von der offiziellen Dokumentation von Digicert (siehe Hauptseite), gibt es die gemeinsame Anstrengung mit Kollegen von anderen Wissenschaftsnetzen, in einem Wiki, das von der GEANT Association gehostet wird, eine detaillierte, bebilderte Step-by-Step Anleitung für das Digicert Portal zu erstellen. Dies wird allerdings noch ein wenig dauern, soll aber spätestens zum 01.07.2015 zur Verfügung stehen. Auch das GEANT Association Repository mit diversen Dokumenten und Links zu Digicert Dokumenten steht bereits zur Verfügung.

Weiters werden wir die Informationen und auch die Dokumentation an dieser Stelle (ie. hier im Wiki) kontinuierlich erweitern und anpassen.

Neuerungen bzw. Änderungen

- Zusatzvereinbarung (aktualisierte Zusatzvereinbarung)
    - Wie schon oben erwähnt macht die neue CA auch eine neue Zusatzvereinbarung notwendig. Neben einigen kleineren Änderungen gibt es 2 Punkte, die sich massiv zur vorherigen Version unterscheiden
        - keine Beilage 3 - das neue Portal und die Validierung durch Digicert machen es obsolet, dass die zulässigen Domains durch das ACOnet Team geprüft werden müssen. Damit entfällt auch die Notwendigkeit für (die bisherige) Beilage 3.
        - Rolle als RA (Registration Authority) - bisher fiel diese Rolle dem ACOnet Team zu, was auch oben erwähnte Beilage 3 notwendig machte. Wie einige von euch, die Code-Signing oder Organisation Validated Zertifikate beantragt haben, jedoch leidvoll erfahren mussten, war diese Rolle bei Comodo nicht ganz klar zugeordnet, sondern je nach Zertifikatstyp, einmal beim Teilnehmer und einmal beim ACOnet Team. Bei Digicert ist diese Rolle ganz klar dem Teilnehmer (Subscriber in der Nomenklatur von Digicert) zugeordnet, was den gesamten Validierungsprozess (s.u.) stark vereinfacht und verbessert. Diese neue Rollenverteilung macht einen Grossteil der Änderungen aus, da hier auch einige Vorgaben bez. Vertragswerk von Digicert umzusetzen sind.
- neues Portal
    - Das Portal zur Beantragung und Administration von Zertifikaten wird von Digicert betrieben. Leider ist dieses Portal nicht föderiert und es sind deshalb Benutzerkonten für diese Portal anzulegen.
    - **Administratoren**
        - Sobald die neue Zusatzvereinbarung ordnungsgemäß unterschrieben bei uns eingelangt ist, legen wir die Adminstratoren für das Portal an. Obwohl technisch möglich, ist es dem Teilnehmer nicht erlaubt weitere Administratoren anzulegen, die nicht in der Zusatzvereinbarung angeführt sind.
    - **Beantragung von Zertifikaten**
        - Auch für das Beantragen von Zertifikaten ist es prinzipiell notwendig sich am Portal anzumelden. Als Ausweg, falls der anonyme Upload von CSRs unbedingt notwendig ist, gibt es die Möglichkeit 'guest URLs' zu erstellen, die dann je nach Konfiguration den anonymen Request für einen definierten Zertifikatstyp erlauben.
- Validierung
    - Im Gegensatz zu Comodo werden die notwendigen Informationen bei Digicert vorab validiert und diese Validierung hält im Normalfall für 3 Jahre (also die normale Laufzeit eines Zertifikats). Natürlich behält sich Digicert das Recht auf neuerliche Validierung zu jeder Zeit vor.
    - **Organisation**
        - Die Validierung der Organisation ist der erste Schritt. Nach Anlegen der Organisation und zugehörigen Kontakten validiert Digicert diese Informationen. Abhängig von der gewählten Art

von Zertifikaten, die für diese Organisation ausgestellt können werden sollen, ist dabei auch telefonische Rückfrage von Digicert notwendig.

- **Domain**
  - Sobald die Organisation validiert bzw. angelegt ist, können auch zugehörige Domains angelegt werden. Diese werden per DCV validiert, wobei Digicert hier (im Gegensatz zu Comodo) keine Auswahl der DCV Adresse erlaubt, sondern das Validierungsmail an alle möglichen Adressen versendet. Dies passiert allerdings nur einmal, nämlich nach dem Anlegen der Domain. DCV per angefordertem Zertifikat ist nicht mehr notwendig.

- TLS/SSL Zertifikate
  - **Zertifikatstypen**
    - DV - Domain Validated Zertifikate (Standard bei Comodo) gibt es bei Digicert nicht. Jedes Zertifikat ist zumindest OV (s.u.).
    - OV - Organisation Validated: Standard Zertifikat bei Digicert
    - EV - Extended Validation: auch dieser Zertifikatstyp ist ohne weitere Kosten

Auflistung und Beschreibung bei Digicert: https://www.digicert.com/ssl-certificate.htm

- Code Signing Zertifikate
  - **Zertifikatstypen**
    - OV - wie gehabt
    - EV - mit Hardware Token
- persönliche (Email-) Zertifikate (Premium/Client Certificates)
  - **neues Portal** - auch das Portal für persönliche Zertifikate wird von Digicert betrieben
    - Integration in die ACOnet Identity Federation - wie auch bisher ist der Login zum Portal mittels 'federated login' möglich
    - das Portal ist im Übergangszeitraum noch nicht in vollem Funktionsumfang verfügbar. Notfalls können persönliche Zertifikate auch über das Standard-Webportal von Digicert (Certificates -> Requests -> Client Certificates) beantragt werden.
- Support
  - der Vertrag mit Digicert beinhaltet auch den direkten Support von Endbenutzern durch Digicert (support@digicert.com) https://www.digicert.com/contact-digicert-inc.htm
- Sonstiges
  - **Vielzahl von Zertifikatstypen**
    - im Gegensatz zu Comodo, wo die Anzahl der Zertifikatstypen überschaubar war, gibt es bei Digicert in jeder Kategorie mehrere Auswahlmöglichkeiten. Darüberhinaus sind auch GRID Zertifikate Teil des Portfolios.