Zertifikate für Domains außerhalb tu-braunschweig.de/tu-bs.de

Für die Absicherung von Serverdiensten werden von Ihnen SSL-Zertifikate aus der DFN-PKI eingesetzt. Diese Zertifikate für Ihre Server werden von einer Zertifizierungsstelle, die von der DFN-PKI über GÈANT TCS bereitgestellt wird, signiert (digital unterschrieben). In der Regel setzen Sie diese Zertifikate für Server ein, die Namen unterhalb der Domains „tu-braunschweig.de“ bzw. „tu-bs.de“ haben.

Die Nutzung der DFN-PKI ist jedoch nicht begrenzt auf diese beiden Domains, denn gerade im Bereich der Forschung hat es sich etabliert, dass andere Domains z.B. für Konferenzen durch die ausrichtenden Einrichtungen genutzt werden. Auch einrichtungsübergreifende Forschungskooperationen nutzen übergreifende Domainnamen, um über die Inhalte und Kooperationspartner dieser Verbünde zu informieren. Hier werden Domains der Form www.example.[de|com|eu|org|net] benötigt und damit auch Zertifikate für Domain-Namen, die nicht auf tu-braunschweig.de bzw. tu-bs.de enden.

Dem trägt der DFN mit seinem Angebot dahingehend Rechnung, dass unter bestimmten Voraussetzungen andere Domains der Form "example.com" für das Ausstellen von Zertifikaten innerhalb der DFN-PKI freigeschaltet werden können.

Um für eine andere Domain Serverzertifikate ausgestellt zu bekommen, ist die wichtigste Voraussetzung, dass die jeweilige Domain der TU Braunschweig als Einrichtung gehört. Individuell auf Mitarbeitende registrierte Domains erfüllen diese Anforderung nicht. Die Überprüfung erfolgt in zwei Schritten. Zunächst erbitten wir Einblick in die Vertragsdaten mit dem Provider, über den Sie die Domain registriert haben, bevor wir die betreffende Domain in der DFN-PKI eintragen. Anschließend erfolgt eine automatisierte Überprüfung durch die DFN-PKI, ob die Domain tatsächlich Ihnen gehört. Diese Validierung basiert auf einem Challenge-Response Verfahren.

Das Challenge-Response Verfahren setzt darauf auf, dass die Eigentümer einer Domain unter bestimmten E-Mail Adressen erreichbar sein sollten. Die vom Verfahren nutzbaren E-Mail Adressen sind von der Struktur wie folgt fest vorgegeben: hostmaster@example.net, webmaster@example.net, postmaster@example.net, admin@example.net, administrator@example.net. Domains werden aktuell für ein Jahr validiert bevor das Challenge-Response Verfahren erneut durchlaufen werden muss.

Sollten Sie Domains validieren lassen wollen oder weitere Fragen zum Thema Validierung von Domains in der DFN-PKI haben, können Sie sich an noc@tu-braunschweig.de wenden.

Revision #3
Created 25 January 2024 10:36:01 by Tina Strauf
Updated 24 April 2024 09:41:48 by Carolin Thiele