Universität Regensburg

Erklärung zur Zertifizierung eines Servers durch die DFN-PKI

Der Unterzeichner dieser Erklärung wünscht die Zertifizierung eines öffentlichen Schlüssels für den unten beschriebenen Server durch die DFN-PKI und hat ihn zusammen mit den nach den aktuellen Zertifizierungsrichtlinien notwendigen Daten an die Registrierungsstelle des Rechenzentrums für Serverzertifikate übermittelt. Er ist dann der Zertifikatnehmer für das gewünschte Serverzertifikat und erklärt mit seiner Unterschrift sein Einverständnis mit den folgenden Punkten:

1. Der Unterzeichner hat die zum Zeitpunkt der Unterzeichnung gültigen Zertifizierungsrichtlinien der DFN-PKI sowie die Richtlinien für die Beantragung und Nutzung von Serverzertifikaten an der Uni Regensburg zur Kenntnis genommen (siehe http://pki.uni-regensburg.de). Er erklärt sich mit dem Inhalt der Richtlinien einverstanden und verpflichtet sich zur Einhaltung der sich daraus ergebenden Pflichten.

2. Der Unterzeichner versichert, das dem Zertifikat zugrundeliegende Schlüsselpaar persönlich erzeugt zu haben, den privaten Schlüssel geheim zu halten, ihn sorgfältig vor Missbrauch zu schützen und das Zertifikat bei Verlust oder Verdacht auf Kompromittierung des privaten Schlüssels sofort zu widerrufen.

3. Der Unterzeichner versichert, dass der physikalische Zugang (Konsole, USB Ports, etc.) zu dem unten beschriebenen Server, falls er nicht im Maschinensaal des Rechenzentrums aufgestellt ist, vor unberechtigtem Zugang abgesichert ist. Der Unterzeichner stimmt einer angekündigten Kontrolle der Absicherung des Zugangs durch das RZ zu.

4. Dem Unterzeichner ist bekannt, dass die von der DFN-PKI erstellten Zertifikate nur fortgeschrittene Zertifikate im Sinne des Deutschen Signaturgesetzes (§2 SigG), und keine qualifizierten Zertifikate sind. Sie können somit die gesetzlich vorgeschriebene Schriftform nicht ersetzen, können aber dennoch gegebenenfalls im Zuge der freien Beweiswürdigung vor Gericht Beweiseignung erlangen.

5. Der Unterzeichner stimmt der Speicherung und Verarbeitung der bei der Zertifizierung anfallenden Daten zu. Alle anfallenden Daten werden von der Registrierungs- und Zertifizierungsstelle selbstverständlich vertraulich behandelt.

Vom Zertifikatnehmer auszufüllen:

Angaben zur Person	
Vorname, Nachname	
Telefon (dienstlich)	
Büro	
RZ Account	
Email-Adresse (dienstlich)	@ur.de
Name der Einrichtung (gemäß der Liste auf https://pki.uni-regensburg.de/verantwortliche.py)	

Angaben zum Server	
Nummer des Online Zertifizierungsantrags	
IP Adresse des Servers	
Voll qualifizierter IP Name des Servers	
Verwendungszweck des Servers	
Standort des Servers	
Datum	**Unterschrift**

Vom PKI Verantwortlichen (gemäß der Liste auf https://pki.uni-regensburg.de/verantwortliche.py) der Einrichtung/Fakultät auszufüllen:

Einverständniserklärung mit dem Antrag zur Zertifizierung des oben genannten Servers:

Datum, Unterschrift	**Stempel der Einrichtung**