So beantragen Sie ein Zertifikat

Wenn Sie ein Gruppen- oder Serverzertifikat beantragen möchten, so müssen Sie im Besitz eines gültigen Personenzertifikats der KIT-CA sein. Sie können alternativ gleichzeitig mit einem Gruppen- oder Serverzertifikat auch ein Nutzer- oder Pseudonymzertifikat beantragen.

Details des Beantragungsprozesses können Sie auf der Webseite der KIT-CA nachlesen. Hier wird daher der Ablauf nur grob skizziert:

1. Sie stellen auf der Webseite der KIT-CA einen Zertifikatantrag. Dabei erzeugt Ihr Webbrowser einen geheimen Schlüssel.
2. Sie laden Ihren Zertifikatantrag als PDF-Datei von der Webseite der KIT-CA herunter.
3. Sie bringen den vollständig ausfüllten Antrag zusammen mit einem gültigen Lichtbildausweis persönlich zum SCC-Servicedesk (siehe »Kontakt« rechts).
4. Die KIT-CA prüft Ihre Identität und stellt Ihr Zertifikat aus.
5. Ihr Zertifikat wird Ihnen per E-Mail zugestellt.
6. Nun müssen Sie den Link aus der E-Mail mit dem gleichen Browser und Computer öffnen, mit dem Sie in Schritt 1 den geheimen Schlüssel erzeugt haben.
7. Sie erzeugen eine Sicherungskopie Ihres geheimen Schlüssels und Ihres Zertifikats.

Ausführliche Anleitungen der KIT-CA finden Sie unter folgender Adresse:

https://www.ca.kit.edu/p/anleitungen

KIT Certification Authority

Kontakt

Karlsruher Institut für Technologie (KIT)
Steinbuch Centre for Computing
Servicedesk

Campus Süd: Gebäude 20.21 Erdgeschoss, rote Theke
Campus Nord: Gebäude 441, Raum 165

Telefon: +49 721 608-8000
Fax: +49 721 608-992008
E-Mail: servicedesk@scc.kit.edu
www.scc.kit.edu

Herausgeber

Karlsruher Institut für Technologie (KIT)
Kaiserstraße 12
76131 Karlsruhe
www.kit.edu

Stand: 2018-09-24 (Revision 36/a98fe29)

Zertifikat seit 2010 audit familiengerechte hochschule

Karlsruher Institut für Technologie

X.509-Zertifikate

Personen- und Serverzertifikate zur Absicherung von E-Mail und Kommunikation

STEINBUCH CENTRE FOR COMPUTING

Was bieten Ihnen X.509-Zertifikate?

X.509-Zertifikate bilden die Grundlage für viele Formen verschlüsselter Kommunikation im Internet. Zwei wichtige Anwendungen sind abgesicherte E-Mails und Webseiten.

Die KIT-CA stellt kostenlos Zertifikate für KIT-Mitglieder (unter anderem Studierende sowie Gäste & Partner) aus. Sie kennt Nutzer-, Pseudonym-, Gruppen- und Serverzertifikate. Nutzer- und Pseudonymertifikate sind ausschließlich einem einzelnen Anwender zugeordnet (Personenzertifikate). Gruppenzertifikate »gehören« einer Gruppe von Anwendern, während Serverzertifikate für Serversysteme und Dienste verwendet werden.

Nutzerzertifikate

Nutzerzertifikate sind für einzelne Personen bestimmt und dürfen nur von ihnen persönlich genutzt werden. Typischerweise benötigen Sie ein Nutzerzertifikat, um die Kommunikation über Ihre KIT-E-Mail-Adresse abzusichern.

Gruppenzertifikate

Gruppenzertifikate werden für namentlich definierte Gruppen ausgestellt, etwa Sekretariate, Forschungs- oder Arbeitsgruppen. Sie können von allen Mitgliedern der Gruppe verwendet werden, etwa zur Absicherung der Kommunikation einer gemeinsamen E-Mail-Adresse.

Pseudonymzertifikate

Benötigen Sie ein Zertifikat, das nicht auf Ihren eigenen Namen ausgestellt ist, wie er im Ausweis steht, so müssen Sie ein Pseudonymzertifikat beantragen. Häufige Anwendungsfälle hierfür sind etwa Zertifikate für Logon (Name im Ausweis: »Beate Beispiel«, Name im Zertifikat: »PN: Beate Beispiel/Logon«) oder Zertifikate für Codesigning (Name im Zertifikat: »PN: Beate Beispiel/Codesigning«).

E-Mail absichern

Mit Hilfe von X.509-Zertifikaten können Sie E-Mails signieren und verschlüsseln.

Signierte E-Mails sind authentisch und integer. Die E-Mail kann also nicht durch einen Angreifer verändert worden sein (Integrität), außerdem kann sich der Empfänger über die Identität des Absenders sicher sein (Authentizität).

Verschlüsselte E-Mails können nur vom Sender und vom Empfänger gelesen werden. Verschlüsselung bietet sich daher zur Übermittlung vertraulicher und schützenswerter Daten an.

Um verschlüsselte E-Mails zu verschicken, benötigen Sie das Zertifikat des Empfängers. Als Outlook-Benutzer bekommen Sie dies automatisch aus dem globalen Addressbuch des KIT. Wenn Sie andere E-Mail-Clients verwenden, können Sie es durch Lesen signierter E-Mails des Empfängers oder Einbinden des zentralen Verzeichnisdienstes (Active Directory via LDAP) beziehen.

Zum Signieren Ihrer eigenen E-Mails benötigen Sie nur Ihren eigenen geheimen Schlüssel sowie Ihr Zertifikat. Wir empfehlen, Ihre E-Mails immer zu signieren. Die KIT-CA bietet Ihnen dazu Nutzerzertifikate für Ihre Mailadressen an, die auf `kit.edu` enden.

`https://www.ca.kit.edu/p/nutzer`

Es gibt neben S/MIME (dem hier verwendeten Verfahren zur Absicherung von E-Mail) noch PGP/MIME. X.509-Zertifikate sind dafür nicht geeignet; vielmehr werden sogenannte PGP-Schlüsselpaare benötigt. Sollten Sie PGP verwenden, signiert das KIT-CERT gerne auch Ihre PGP-Schlüssel.

Netzwerkdienste absichern

Wenn Sie einen Server betreiben, können Sie zur Verschlüsselung der Kommunikation der von Ihnen angebotenen Dienste ebenfalls Zertifikate der KIT-CA nutzen. Der häufigste Anwendungsfall ist der Betrieb eigener Webserver und -dienste. Prinzipiell können Sie bei jedem Protokoll, das SSL/TLS unterstützt, Zertifikate der KIT-CA verwenden. Für die Übermittlung sensibler oder personenbezogener Daten ist eine solche Absicherung zwingend vorgeschrieben.

Wenn Ihre Webseite beim SCC gehostet wird, bekommt sie automatisch ein passendes Zertifikat und ist immer auch über eine gesicherte Verbindung erreichbar.

Sie können Serverzertifikate der KIT-CA beantragen, wenn:

- Sie ein gültiges Personenzertifikat der KIT-CA besitzen und
- Ihr Server sich im Namensraum des KIT befindet. Insbesondere sind Servernamen zertifizierbar, die auf `kit.edu` enden. Neue Domains können bei Bedarf durch die KIT-CA freigeschaltet werden, wenn sie administrativ dem KIT (noch besser: dem SCC) gehören.

Weitere Details zur Beantragung finden Sie auf der Webseite der KIT-CA:

`https://www.ca.kit.edu/p/server`