Fraunhofer

Fraunhofer Competence Center PKI

Zertifizierungsstelle für Kontakte der Fraunhofer-Gesellschaft – PKI-Contacts

Richtlinien für die Beantragung und Nutzung von Zertifikaten

Autor[en]:
Uwe Bendisch, Claudia Hirsch

Stand: 18.05.2017

Version 1.1

Dokumenthistorie:

VERSION	DATUM	ÄNDERUNG	AUTOR
1.1	18.05.2017	Überarbeitung der Einleitung, sowie der Kapitel 2, 4, 5, 6, 7 und Abschnitte 1.2, 1.3, 3.1 und 3.2	CC-PKI
1.0	18.05.2011	Dokumenterstellung und Freigabe	CC-PKI

Verteiler/Zielgruppe:

In diesem Dokument werden die Richtlinien für die Beantragung und Nutzung, sowie der Lebenszyklus von digitalen Zertifikaten der PKI-Contacts der Fraunhofer Gesellschaft beschrieben. Die Richtlinien gelten für Zertifikate und Nutzer der PKI-Contacts.

Bemerkungen/Hinweise:

Anmerkungen oder Änderungswünsche zum Dokument können Sie dem CC-PKI jederzeit gerne über unsere Kontaktmöglichkeiten mitteilen, die unter http://www.pki.fraunhofer.de/kontakt angegeben sind.

Kontakt:

Fraunhofer Competence Center PKI
Schloss Birlinghoven
53757 Sankt Augustin

http://www.pki.fraunhofer.de

Interne Angaben:

Dateiname: Richtlinien PKI Contacts (V 1.1).docx
Zeitpunkt: 23.05.2017
Bearbeiter: Bendisch, Uwe

Inhalt

Einleitung

Fraunhofer betreibt bereits seit mehr als zehn Jahren eine Public Key Infrastruktur, die Fraunhofer-PKI [FhG-PKI], um ihre Mitarbeitenden insbesondere mit Zertifikaten für eine sichere und vertrauliche E-Mail-Kommunikation im Unternehmen sowie mit Geschäftspartnern auszustatten. Mitarbeitende erhalten dazu sogenannte X.509v3 Zertifikate und Schlüssel standardmäßig auf Smartcards.

Damit eine gesicherte und vertrauliche Kommunikation auch mit Geschäftskontakten außerhalb der Fraunhofer-Gesellschaft möglich ist, benötigen diese ebenfalls Zertifikate und Schlüssel. Kommunikationspartnern, die noch keine Zertifikate bzw. Schlüssel besitzen, bietet die Fraunhofer-Gesellschaft die in diesem Dokument beschriebene *Public-Key-Infrastruktur für Kontakte – PKI-Contacts* (im Folgenden als *PKI-Contacts* bezeichnet, [PKI-Contacts]) an, aus der sie bei Bedarf ein solches Zertifikat erhalten können.

Mitarbeitende der Fraunhofer-Gesellschaft können für ihre Geschäftskontakte, mit denen sie in Projekten, über Werk- und andere Verträge der Fraunhofer-Gesellschaft oder bei der Anbahnung solcher Vorhaben vertraulich und sicher kommunizieren wollen oder müssen, die Erstellung von Zertifikaten für diese Geschäftskontakte veranlassen. Dies geschieht über den Dienst *PKI-Contacts*, der weltweit im Internet unter https://contacts.pki.fraunhofer.de erreichbar ist. Im Anschluss daran können die Kommunikationspartner den Web-Dienst nutzen, um in ihrem eigenen Browser ein Schlüsselpaar zu erstellen und ein zugehöriges X.509v3 Zertifikat von der *PKI-Contacts* zu erhalten. Das Zertifikat kann dann für (E-Mail-) Verschlüsselung, elektronische Signaturen und Authentifizierung im Rahmen der Kommunikation und Zusammenarbeit mit Mitarbeitenden der Fraunhofer-Gesellschaft genutzt werden.

Im Folgenden werden die Richtlinien für die Beantragung und Nutzung, sowie der Lebenszyklus von digitalen Zertifikaten der *PKI-Contacts* beschrieben.

Die Richtlinien gelten für alle Nutzer der *PKI-Contacts*, also für Mitarbeitende der Fraunhofer-Gesellschaft, die die Zertifikatsausstellung für sich oder Dritte über die *PKI-Contacts* initiieren, sowie insbesondere für die Geschäftskontakte der Fraunhofer-Mitarbeitenden und alle Mitarbeitende selbst, die die Zertifikate der *PKI-Contacts* beantragen und einsetzen (Zertifikatsnehmer).

Diese Richtlinien gilt nicht für die komplett unabhängige interne Fraunhofer-PKI, welche Zertifikate für Mitarbeitende der Fraunhofer-Gesellschaft Smartcard-basiert und auf einem höheren Sicherheitsniveau zur Verfügung stellt.

1 Rahmenbedingungen

1.1 Betreiber der PKI-Contacts

Die *PKI-Contacts* wird betrieben durch das Fraunhofer Competence Center Public Key Infrastructures (CC-PKI), eine Einrichtung der Fraunhofer-Gesellschaft e.V.

1.2 Kontakt

Internet
https://contacts.pki.fraunhofer.de

E-Mail
servicedesk@fraunhofer.de

Postadresse
Fraunhofer Competence Center PKI, Schloss Birlinghoven, 53757 Sankt Augustin

Telefon
01802-FHGPKI bzw. 01802-344754 (6 ct/Anruf aus dem dt. Festnetz)
oder
+49 22 41 / 14 - 14 14 (dt. Festnetz-Rufnummer, i. a. günstiger für Anrufe aus Mobilfunknetzen)

Hinweis
Ein direkter Support für die Geschäftskontakte der Fraunhofer-Gesellschaft ist i. a. nicht vorgesehen. Support-Anfragen sollten durch einen Fraunhofer-Mitarbeitenden an das CC-PKI übermittelt werden.

1.3 Änderungen dieser Policy

Diese Policy kann durch die Fraunhofer-Gesellschaft, vertreten durch das CC-PKI und das Change Advisory Board Identitätsmanagement der Fraunhofer-Gesellschaft, jederzeit abgeändert werden. Die jeweils gültige Fassung wird auf der Website https://contacts.pki.fraunhofer.de veröffentlicht.

1.4 Nutzungsbedingungen und Haftungsausschluss

Die Zertifikate der *PKI-Contacts* dürfen nur zur Absicherung der Kommunikation mit Mitarbeitenden der Fraunhofer-Gesellschaft bzw. zur Absicherung von Kontexten mit Fraunhofer-Beteiligung durch Einsatz von Verschlüsselung, elektronischer Signatur und Authentifizierung genutzt werden.

Da die Fraunhofer-Gesellschaft durch die *PKI-Contacts* ausgestellte Zertifikate nicht bezüglich der Authentizität der Zertifikatsnehmer und deren angegebener E-Mail-Adressen überprüft, wird der Dienst technisch so aufgesetzt und durch rechtliche Regelungen ergänzt, dass eine Haftung der Fraunhofer-Gesellschaft – soweit möglich – ausgeschlossen ist. Weiterhin wird eine Haftung der Mitarbeitenden der Fraunhofer-Gesellschaft ausgeschlossen.

Die nachfolgenden Bedingungen regeln die Haftungsausschlüsse in den verschiedenen Beziehungen der Fraunhofer-Gesellschaft zu

1. ihren Geschäftspartnern, mit denen sie eine vertragliche Beziehung hat oder anbahnt (nachfolgend "Vertragspartner" genannt),

2. sonstigen Dritten und

3. ihren Angestellten und externen Mitarbeitenden

1.4.1 Nutzungsbedingungen und Haftungsausschluss gegenüber Vertragspartnern

Der Zertifikatsnehmer bestätigt durch Anklicken eines Feldes auf der Zielseite des Bestätigungslinks, dass er rechtlich befugt ist, nachfolgende Nutzungsbedingungen und Haftungsausschlüsse für 1) sich und 2) aufgrund vorheriger ausdrücklicher Erlaubnis seiner Organisation, d. h. den Vertragspartner der Fraunhofer-Gesellschaft, für diese zu vereinbaren.

Das Klicken gilt als Annahme der nachfolgenden Bedingungen und Haftungsausschlüsse und verpflichtet sowohl den Zertifikatsnehmer persönlich als auch dessen Organisation (Zertifikatsnehmer persönlich und Organisation nachfolgend ohne Differenzierung "ZERTIFIKATSNEHMER" genannt):

– Nachfolgende Nutzungsbedingungen und Haftungsregelungen (nachfolgend NUTZUNGSBEDINGUNGEN) gelten zwischen der Fraunhofer-Gesellschaft e. V., Hansastraße 27c, 80686 München (FRAUNHOFER-GESELLSCHAFT) und dem ZERTIFIKATSNEHMER.

- Der ZERTIFIKATSNEHMER kann eine natürliche Person sein, die das Zertifikat für sich selbst nutzt, als auch eine Organisation, für die der Antragsteller das Zertifikat als Vertreter beantragt und als Angestellter oder freier Mitarbeiter nutzt (in beiden Fällen ohne Unterscheidung ZERTIFIKATSNEHMER genannt).

- Zwischen der FRAUNHOFER-GESELLSCHAFT und dem ZERTIFIKATSNEHMER gelten ausschließlich nachfolgende NUTZUNGSBEDINGUNGEN. Davon abweichende Allgemeine Geschäftsbedingungen des ZERTIFIKATSNEHMERS werden nicht Vertragsbestandteil.

- Der ZERTIFIKATSNEHMER bestätigt, Verfügungsberechtigter der E-Mail-Adresse zu sein, die zur Aktivierung des Zertifikats verwendet wird.

- Der ZERTIFIKATSNEHMER bestätigt, dass alle Angaben für die Erzeugung des Zertifikats der Wahrheit entsprechen.

- Der ZERTIFIKATSNEHMER ist selbst verantwortlich, dass die von ihm angegebenen Daten, insbesondere seine E-Mail-Adresse, bei Antragstellung und während der Zertifikatslaufzeit gültig sind und bleiben.

- Der ZERTIFIKATSNEHMER ist verpflichtet, Zertifikate auf nicht mehr gültige E-Mail-Adressen selbst sperren zu lassen; gleiches gilt bei Beendigung der Geschäftsbeziehungen zur FRAUNHOFER-GESELLSCHAFT.

- Der ZERTIFIKATSNEHMER ist verpflichtet, Missbrauchsfälle und konkrete Missbrauchsverdachte des Zertifikats oder des zugehörigen Schlüssels umgehend der FRAUNHOFER-GESELLSCHAFT zu melden.

- Die FRAUNHOFER-GESELLSCHAFT ist zur Sperrung von Zertifikaten nur innerhalb von 7 Tagen ab Anzeige eines Missbrauchsfalls oder konkreten -verdachts verpflichtet. Der ZERTIFIKATSNEHMER trägt während dieser Zeit selbst die Verantwortung und ergreift alle erforderlichen Maßnahmen, dass das Zertifikat nicht mehr weiter verwendet wird.

- Der ZERTIFIKATSNEHMER verpflichtet sich, Zertifikate nur im Zusammenhang mit Fraunhofer-Projekten bzw. in der betrieblichen Kommunikation mit Angestellten oder externen Mitarbeitern der FRAUNHOFER-GESELLSCHAFT zu verwenden.

- Die FRAUNHOFER-GESELLSCHAFT bietet den Dienst freiwillig und kostenlos an, schließt dafür aber jegliche Haftung für Schäden aus, die im Zusammenhang mit der Verwendung des Zertifikats und Schlüssels entstehen können. Dies gilt auch zugunsten ihrer Angestellten und sonstigen Mitarbeiter.

- Der ZERTIFIKATSNEHMER stellt die FRAUNHOFER-GESELLSCHAFT von allen Ansprüchen frei, die Dritte im Zusammenhang mit einer entgegen diesen NUTZUNGSBEDINGUNGEN erfolgten Nutzung des auf die E-Mail-Adresse der Person des ZERTIFKATSNEHMERS ausgestellten Zertifikats gegen die FRAUNHOFER-GESELLSCHAFT oder deren Angestellte oder sonstigen Mitarbeiter erheben.

- Die FRAUNHOFER-GESELLSCHAFT hat jederzeit das Recht, ein Zertifikat zu sperren.

- Der ZERTIFIKATSNEHMER verpflichtet sich, private Schlüssel nicht an Dritte weiterzugeben.

- Die FRAUNHOFER-GESELLSCHAFT bietet keine Key-Recovery an. Der ZERTIFIKATSNEHMER ist daher selbst verantwortlich, eine Sicherungskopie von Schlüsseln und Zertifikat anzulegen. Der ZERTIFIKATSNEHMER wird darauf hingewiesen, dass ohne seinen privaten Schlüssel an ihn versendete und verschlüsselte E-Mails nicht mehr entschlüsselt und gelesen werden können. Er ist verpflichtet, seine Organisation auf diesen Umstand hinzuweisen und selbst entsprechende Maßnahmen zur Key-Recovery abzustimmen, etwa durch Hinterlegung einer Kopie seiner Schlüssel bei seiner Organisation.

- Sollte eine Bestimmung dieser NUTZUNGSBEDINGUNGEN ganz oder teilweise unwirksam, undurchführbar oder lückenhaft sein oder werden, berührt dies nicht die Wirksamkeit der anderen Bestimmungen. Bei Vorliegen einer unwirksamen, undurchführbaren oder lückenhaften Bestimmung einigen sich die Parteien nach billigem Ermessen auf eine Bestimmung, die die Interessen beider Parteien und den angestrebten Vertragszweck angemessen berücksichtigt.

1.4.2 Haftungsbegrenzung gegenüber sonstigen Dritten

Die Haftung gegenüber Dritten kann mangels Vertrags mit diesen nicht vertraglich eingeschränkt werden. Möglich sind jedoch Hinweise an Dritte, die diesen zumindest den guten Glauben nehmen.

Die Fraunhofer-Gesellschaft weißt sonstige Dritte durch Angaben im Zertifikat auf folgende Beschränkungen hin:

- Die Fraunhofer-Gesellschaft hat im Zuge der Zertifikatserstellung die Person bzw. Organisation, der die E-Mail-Adresse gehört, auf die das Zertifikat ausgestellt ist, nicht verifiziert. Jedermann, der über die im Zertifikat angegebene E-Mail-Adresse verfügt oder Zugang zum entsprechenden E-Mail-Postfach hatte, konnte das Zertifikat beantragen und den zugehörigen Schlüssel erzeugen und kann ihn aktuell besitzen. Jede solche Person

und auch jeder, der später Zugang zum Postfach erhält, kann mit dem Zertifikat verschlüsselte Nachrichten entschlüsseln und Nachrichten auch elektronisch signieren.

- Die Erstellung der den Zertifikaten zu Grunde liegenden Schlüsselpaare erfolgt durch die externen Kommunikationspartner auf deren Computer-Systemen und nicht durch die Fraunhofer-Gesellschaft. Die Fraunhofer-Gesellschaft hat keinerlei Einfluss auf die Qualität des Schlüsselpaares bzw. auf die Verwaltung und Verwendung des Schlüsselmaterials. Daher kann auch keinerlei Gewähr für ein bestimmtes Sicherheitsniveau beim Einsatz der Zertifikate der *PKI-Contacts* gegeben werden.

- Die Tatsache, dass einer E-Mail-Adresse ein PKI-Contacts-Zertifikat zugeordnet wurde und dass dies angewendet wird, bedeutet nicht notwendig, dass die das Postfach nutzende Person aktuell ein Geschäftspartner der Fraunhofer-Gesellschaft oder in einer bestimmten Weise mit der Fraunhofer-Gesellschaft verbunden ist oder war.

- Das Zertifikat darf nur im Verhältnis der Fraunhofer-Gesellschaft zum Zertifikatsnehmer oder von Zertifikatsnehmern untereinander verwendet werden, und ist nur in diesem Verhältnis gültig.

- Die Fraunhofer-Gesellschaft übernimmt keine Gewähr und hat auch keine Kontrolle für die Verwendung und den Schutz des Zertifikats bzw. des zugehörigen Schlüsselpaares durch den Nutzer.

1.4.3 Haftungsausschluss zugunsten von Angestellten und externen Mitarbeitern

Mitarbeitende der Fraunhofer-Gesellschaft haften gegenüber der Gesellschaft nicht für Schäden jeglicher Art, die im Zusammenhang mit der ordnungsgemäßen Veranlassung der Beantragungsmöglichkeit von Zertifikaten und/oder Schlüsseln für Geschäftskontakte der Gesellschaft und Nutzung durch diese entstehen.

Die Fraunhofer-Gesellschaft stellt Angestellte und externe Mitarbeiter von jeglichen Ansprüchen Dritter frei, die im Zusammenhang mit der Verwendung von Zertifikaten und / oder Schlüsseln durch Geschäftskontakte der Gesellschaft erhoben werden.

Vorstehende Regelungen gelten auch, soweit ausnahmsweise *PKI-Contacts*-Zertifikate von Fraunhofer Mitarbeitenden für sich selbst genutzt werden dürfen (vgl. Abschnitt 3.1).

Vorstehende Regelungen gelten nicht in Fällen vorsätzlichen Handelns oder Unterlassens durch Mitarbeitende der Fraunhofer-Gesellschaft.

1.5 Zertifikatslaufzeit und Beendigung der Zertifikatsnutzung

Die Zertifikatsnutzungszeit ist auf die Dauer der Kooperation des Zertifikatsnehmers mit der Fraunhofer-Gesellschaft begrenzt. Diese wird bei Beantragung des Zertifikats durch den beantragenden Mitarbeitenden der Fraunhofer-Gesellschaft festgelegt. Die maximale Laufzeit der Zertifikate beträgt drei Jahre.

Zertifikate können jederzeit gesperrt werden. Sie werden nach Ablauf des Gültigkeitszeitraums ungültig.

Eine Beendigung der Zertifikatsnutzung erfolgt daher entweder durch eine Sperrung des Zertifikats, oder indem nach Ablauf des Gültigkeitszeitraums kein neues Zertifikat beantragt wird.

2 Root-Key und Root-Zertifikat

Der Root-Key der *PKI-Contacts* wurde im Trustcenter der Fraunhofer-Gesellschaft generiert und wird in speziell gesicherten Räumen und auf gesicherten Computersystemen eingesetzt.

Das zugehörige selbst-signierte Root-Zertifikat (Root-Certificate, Wurzelzertifikat) wurde ebenfalls im Trustcenter der Fraunhofer-Gesellschaft erstellt.

Zur Absicherung der Kommunikation müssen Mitarbeitende der Fraunhofer-Gesellschaft und Nutzer der *PKI-Contacts* einmalig das Root-Zertifikat der *PKI-Contacts* in ihren Browser bzw. E-Mail-Client importieren. Das Root-Zertifikat steht unter https://contacts.pki.fraunhofer.de zum Download zur Verfügung.

Bezeichnung

CN = Fraunhofer Contacts Root CA 2011, OU = PKI for Fraunhofer Contacts, O = Fraunhofer, C = DE

Fingerprint

Bei der Installation des Root-Zertifikates der *PKI-Contacts* ist die Überprüfung des SHA1- bzw. SHA2-Fingerprints des Zertifikats erforderlich. Der SHA-1 Fingerprint lautet:

D7 8E 87 3C 30 24 08 C9 6C B9 D7 1D D9 19 F7 79 B2 E3 F3 51

und der SHA-2 Fingerprint:

E7 9A A2 B5 5B F2 7A 32 1E A1 5A EB 0A A2 0E 1A
81 B0 F8 07 5F 5F 25 C7 0F A4 84 BB 90 79 F2 C7

Gültigkeit

Das Root-Zertifikat ist gültig bis Donnerstag, 18. Mai 2023 um 14:28:04 GMT.

Zertifikate der *PKI-Contacts* werden nur so ausgestellt, dass sie vor dem Root-Zertifikat ungültig werden.

Kompromittierung und Sperrung des Root-Keys

Der Root-Key ist besonders geschützt. Sollte der private Root-Key kompromittiert werden, so werden das Root-Zertifikat der *PKI-Contacts* und alle damit ausgestellten Zertifikate gesperrt werden. Außerdem werden – soweit möglich – alle betroffenen Zertifikatsnehmer von zum Zeitpunkt der Sperrung gültigen Zertifikaten informiert.

3 Beantragung von Zertifikaten

3.1 Mögliche Zertifikatsinhaber

Die Zertifikate sind für Geschäftspartner der Fraunhofer-Gesellschaft bzw. deren Mitarbeiter vorgesehen. Geschäftspartner sind Mitarbeiter von Organisationen, die mit der Fraunhofer-Gesellschaft bzw. einem ihrer Institute und Einrichtungen, in Projekten, über Werk- und sonstige Verträge oder im Zuge von deren Anbahnung oder Nachbereitung sicher kommunizieren sollen. Geschäftspartner sind beispielsweise universitäre oder industrielle Partner in Kooperationsprojekten, Kunden oder Lieferanten. Auch Angestellte und externe Mitarbeiter, sowie ehemalige Angestellte und externe Mitarbeiter der Fraunhofer-Gesellschaft können für die geschäftliche Kommunikation mit der Fraunhofer-Gesellschaft ausnahmsweise *PKI-Contacts*-Zertifikate erhalten.

Die Zertifikatsnehmer müssen aus dem geschäftlichen Kontakt dem die Zertifikatsaustellung initiierenden Mitarbeitenden von Fraunhofer bekannt sein, der im Antragsprozess auch die E-Mail-Adresse, den Namen, die Firma und die Geschäftsbeziehung bestätigen muss.

Zertifikate werden nur auf Initiative eines Angestellten oder externen Mitarbeiters der Fraunhofer-Gesellschaft ausgestellt, ein Anspruch darauf besteht nicht.

Der Mitarbeitende der Fraunhofer-Gesellschaft muss sich zur Beantragung eines Zertifikats mit einem gültigen Zertifikat aus der PKI für Fraunhofer-Mitarbeitende ausweisen. Akzeptiert werden ausschließlich Benutzerzertifikate, die von der *Fraunhofer User CA – G01* bzw. der *Fraunhofer User CA – G02*, die Fraunhofer beim DFN-Verein betreibt, ausgestellt wurden.

3.2 Initiierung der Antragstellung durch Mitarbeitende der Fraunhofer-Gesellschaft

Zertifikate der *PKI-Contacts* werden durch die Zertifikatsnehmer selbst beantragt. Dies ist jedoch nur dann möglich, sofern zunächst eine individuelle Freischaltung der Beantragungsmöglichkeit seitens eines Fraunhofer-Mitarbeitenden für dessen Kommunikations- oder Projektpartner bzw. Kontakt vorgenommen wird. Die Freischaltung sowie die Beantragung erfolgen über die Website der *PKI-Contacts* (https://contacts.pki.fraunhofer.de).

Login für Fraunhofer-Mitarbeitende

Um die Zertifikatbeantragungsmöglichkeit für einen Kommunikationspartner freizuschalten, muss sich der Fraunhofer-Mitarbeitende mit seinem persönlichen Zertifikat der Fraunhofer-PKI anmelden. Der Login und eine Anleitung finden sich im Internet unter https://contacts.pki.fraunhofer.de. Zur Anmeldung werden ausschließlich Zertifikate der Fraunhofer-PKI akzeptiert, d. h. Zertifikate der *Fraunhofer User CA – G01* bzw. der *Fraunhofer User CA – G02* (Fraunhofer-Smartcard).

Nach dem Login besteht für den Mitarbeitenden der Fraunhofer-Gesellschaft die Möglichkeit, alle Zertifikate aufzulisten, deren Beantragung er selbst bereits in der Vergangenheit bei der *PKI-Contacts* unter diesem Anmeldenamen für Kommunikationspartner initiiert hat. Bei Bedarf kann er diese auch revozieren.

Weiterhin kann er nach bereits ausgestellten Zertifikaten für Fraunhofer Kommunikationspartner suchen, die von anderen Fraunhofer-Mitarbeitenden initiiert wurden sowie die Beantragungsmöglichkeit für ein neues Zertifikat eines Kontakts freischalten.

Freischaltung der Zertifikatsbeantragung

Der Fraunhofer-Mitarbeitende muss zur Freischaltung der Zertifikatbeantragungsmöglichkeit für seinen Kontakt folgende Daten angeben:

1. E-Mail-Adresse des Kontakts, die geschäftlich genutzt wird
2. Vor- und Nachname des Kontakts
3. Firma bzw. Organisation des Kontakts
4. Nutzungszweck

Die Angaben 2. bis 4. erscheinen nicht im Zertifikat, sondern dienen der internen Dokumentation und Unterscheidbarkeit der Zertifikate. 2. und 3. werden bei Suche nach Zertifikaten ausschließlich Fraunhofer-Mitarbeitenden angezeigt. Die Angabe zu 4. wird vor allem im Falle einer Zertifikatssperrung zur Vermeidung unabsichtlicher Sperrungen benötigt. Sie wird ausschließlich demjenigen Fraunhofer-Mitarbeitenden angezeigt, der berechtigt ist, die Sperrung durchzuführen.

Der Fraunhofer-Mitarbeitende, der eine Zertifikatbeantragungsmöglichkeit für einen Kontakt freischaltet, muss bestätigen, dass die vorliegenden Richtlinien eingehalten werden (insbesondere Kapitel 4) und dass die Kommunikation mit der angegebenen E-Mail-Adresse des Kontakts im dienstlichen Kontext erfolgt. Diese Bestätigung wird protokolliert. Es wird darauf hingewiesen, dass der Fraunhofer-Mitarbeitende verpflichtet ist, das Zertifikat zu sperren oder sperren zu lassen, wenn ihm bekannt ist, dass einer der in Abschnitt 7.1 genannten Sperrgründe zutrifft.

Im Anschluss an die o. a. Datenerfassung erhält der externe Kontakt eine E-Mail mit einem Aktivierungslink, die auch die Nutzungsbedingungen und Haftungsausschlüsse gemäß Abschnitt 1.4.1 sowie Hinweise zum Datenschutz enthält. Mit dem in der E-Mail enthaltenen Aktivierungslink kann der Empfänger einmalig ein Zertifikat für die vom Fraunhofer-Mitarbeitenden angegebene E-Mail-Adresse des Kontakts beantragen. Dieser Link besitzt eine Gültigkeit von acht Tagen. Nach Ablauf dieser Frist muss eine erneute Freischaltung der Beantragungsmöglichkeit durch einen Fraunhofer-Mitarbeitenden erfolgen.

4 Identifizierung und Authentisierung

Im Rahmen der Freischaltung der Zertifikatsbeantragung für den externen Kontakt durch den Fraunhofer-Mitarbeitenden erfolgt durch ihn oder das CC-PKI keine spezielle Prüfung der Identität des Antragstellers.

Fraunhofer-Mitarbeitende sind vor der Freischaltung der Beantragungsmöglichkeit von Zertifikaten der *PKI-Contacts* jedoch angehalten, im Rahmen ihrer Möglichkeiten abzuwägen, ob die angegebene E-Mail-Adresse tatsächlich durch die bei der Freischaltung anzugebende Kontakt-Person genutzt wird, bzw. ob die übrigen Daten korrekt angegeben sind, und nur wenn sie davon ausgehen, dass alle Antragsdaten zutreffend sind, die Freischaltung durchzuführen.

Die eigentliche Identifizierung und Authentisierung für ein beantragtes Zertifikat durch die Zertifizierungsstelle *PKI Contacts* erfolgt anhand der E-Mail-Adresse des potentiellen Zertifikatsinhabers:

An die vom Fraunhofer-Mitarbeitenden angegebene E-Mail-Adresse wird eine E-Mail mit Erläuterungen, Nutzungsbedingungen inkl. Haftungsausschluss und Hinweisen zum Datenschutz sowie ein Aktivierungslink versendet. Wer den Aktivierungslink per E-Mail erhält und benutzen kann, ist in der Lage, ein Zertifikat für die E-Mail-Adresse zu erhalten.

Der Aktivierungslink ist lediglich für eine begrenzte Zeit gültig. Die Gültigkeitsdauer beträgt 8 Tage. Danach verfällt der Link und es muss eine neue Freischaltung der Zertifikatsbeantragungsmöglichkeit durch einen Fraunhofer-Mitarbeitenden für den externen Kontakt erfolgen.

Der zukünftige Zertifikatsnehmer wird über den Link auf eine Webseite geleitet, auf welcher er bestätigen muss, dass die angegebenen Daten, welche die Basis für die Zertifikatsbeantragung bilden, tatsächlich korrekt sind. Dies sind Vorname, Name, E-Mail-Adresse und organisatorische Zugehörigkeit (Firma). Er muss weiterhin bestätigen, dass er für sich und für seine Organisation befugt ist, die Nutzungsbedingungen und Haftungsausschlüsse sowie die Hinweise zum Datenschutz zu akzeptieren. Er klickt dazu drei Schaltflächen an.

Im Folgenden werden seine Angaben nochmals in einer Zusammenfassung aufgelistet. Falls die Angaben falsch sind oder diese Richtlinien nicht erfüllt sind oder er kein Zertifikat erhalten möchte, kann der Vorgang abgebrochen werden.

Falls alle Angaben korrekt und diese Richtlinien erfüllt sind, beginnt nach Auswahl der entsprechenden Schaltfläche die Schlüssel- und Zertifikatsgenerierung.

5 Schlüssel- und Zertifikatsgenerierung

5.1 Schlüsselgenerierung

Die Schlüsselgenerierung erfolgt auf dem Rechner des Zertifikatsnehmers. Die Schlüssellänge beträgt 2048 Bit (RSA-Verfahren). Die Fraunhofer-Gesellschaft kann keinerlei Haftung, Gewähr oder Garantie für die Qualität des generierten Schlüsselpaares übernehmen, da diese durch die Systeme der Zertifikatsnehmer erzeugt werden.

Im Anschluss an die Schlüsselgenerierung wird das zugehörige Zertifikat durch die *PKI-Contacts* generiert und unmittelbar anschließend zum Download bereitgestellt. Abschließend wird durch den Zertifikatsnehmer das Zertifikat im Zertifikatspeicher des Browsers abgelegt, der zur Schlüsselgenerierung und Antragstellung genutzt wurde.

Es wird dringend empfohlen eine Sicherungskopie von Schlüsseln und Zertifikat anzulegen, da die Fraunhofer-Gesellschaft keine Ablage bzw. Wiederherstellung von Schlüsselmaterial anbietet.

5.2 Zertifikatsinhalte

Die von der *PKI-Contacts* erstellten X.509v3 Zertifikate weisen u. a. folgende Inhalte auf:

- Subject / Distinguished Name: CN = E-Mail-Adresse
- Subject Alternative Name: E-Mail-Adresse (nicht kritische Erweiterung)
- Öffentlicher Schlüssel (RSA 2048-Bit)
- Schlüsselverwendung (kritisch): Digitale Signatur, Schlüsselverschlüsselung, Datenverschlüsselung

  Hinweis: Es wird nur ein einziges Schlüsselpaar für alle Verwendungszwecke erstellt. Codesigning ist nicht möglich, jedoch aber Dokumentensignatur.
- Erweiterte Schlüsselverwendung (nicht kritisch): Client-Authentifizierung (1.3.6.1.5.5.7.3.2), Sichere E-Mail (1.3.6.1.5.5.7.3.4), Verschlüsselndes Dateisystem (1.3.6.1.4.1.311.10.3.4), Dokumentensignatur (1.3.6.1.4.1.311.10.3.12)
- Austeller: PKI-Contacts Root (vgl. Kapitel 2)

- Gültigkeitszeitraum: drei Jahre
- Zertifikatsrichtlinien (Austellererklärung): Richtlinien-Identifier: 1.3.6.1.4.1.778.80.4.1.1; URL: http://contacts.pki.fraunhofer.de/general/showCertPolicy.asp
- Hinweis zur Haftung in Form eines „Netscape-Comments" (2.16.840.1.113730.1.13) in deutscher und englischer Sprache:

  „Jede Haftung fuer das Zertifikat, die Vertraulichkeit und Integritaet der Schluesssel wird ausgeschlossen. Der Inhaber der E-Mail-Adresse wurde nicht verifiziert. Fuer Einzelheiten siehe http://contacts.pki.fraunhofer.de/general/showCertPolicy.asp?language=DE - Any liability for the certificate, the confidentiality and integrity of the keys is excluded. The owner of the email address has not been verified. For details see http://contacts.pki.fraunhofer.de/general/showCertPolicy.asp?language=EN."

6 Verteilung von Zertifikaten

Um eine verschlüsselte Nachricht zu versenden, benötigt der Absender das Verschlüsselungszertifikat des Empfängers. Es gibt prinzipiell drei Möglichkeiten das entsprechende Zertifikat des Empfängers zu erhalten:

- Über eine signierte E-Mail, die er vom Empfänger erhalten hat. Gängige E-Mail-Tools können hieraus das Verschlüsselungszertifikat extrahieren und später zur Verschlüsselung nutzen (z. B. mittels Antworten-Funktion auf die signierte E-Mail).

- Das Verschlüsselungszertifikat des Empfängers wird dem Absender explizit zur Verfügung gestellt, beispielsweise über einen E-Mail-Anhang.

- Über einen Suchdienst/Verzeichnisdienst, der die Zertifikate zum Herunterladen zur Verfügung stellt.

Wenn externe Kommunikationspartner untereinander verschlüsselt kommunizieren möchten (z. B. in Projekten mit Beteiligung der Fraunhofer-Gesellschaft), dann müssen sie anhand von signierten E-Mails bzw. mittels Dateiaustausch die Zertifikate austauschen.

Auf den Webseiten der *PKI-Contacts* stehen für Mitarbeitende der Fraunhofer-Gesellschaft und für deren Kommunikationspartner zwei unterschiedliche Suchdienste / Verzeichnisdienste für Zertifikate zur Verfügung.

6.1 Suche nach Zertifikaten von Mitarbeitenden der Fraunhofer-Gesellschaft

Kommunikationspartner der Fraunhofer-Gesellschaft können über eine Suchmaske nach Zertifikaten von Fraunhofer-Mitarbeitenden suchen, deren E-Mail-Adresse oder Namen sie kennen. Nach Download und Installation der jeweiligen Zertifikate können dann verschlüsselte Nachrichten an Fraunhofer-Mitarbeitende versendet werden.

6.2 Suche nach Zertifikaten der PKI-Contacts

Zertifikate der *PKI-Contacts* können nur von Mitarbeitenden der Fraunhofer-Gesellschaft nach einem erfolgreichen Login mit ihrer Fraunhofer-Smartcard gesucht

werden. Dabei wird dem Fraunhofer-Mitarbeitenden nach Eingabe der E-Mail-Adresse eines Kontakts oder eines Teils davon (Wildcard-Suche) das entsprechende Zertifikat zum Download zur Verfügung gestellt.

Weitere Informationen und Anleitungen stehen unter https://contacts.pki.fraunhofer.de/ zur Verfügung.

7 Sperrung von Zertifikaten

7.1 Sperrgründe

Die Sperrung von Zertifikaten kann durch einen Fraunhofer-Mitarbeitenden oder durch den Zertifikatsinhaber selbst verlangt werden. Hierzu ist ein Sperrantrag zu stellen, woraufhin das betroffene Zertifikat auf die Sperrliste gesetzt wird.

Die Sperrung eines Zertifikates muss in jedem Fall veranlasst werden, falls

- Missbrauch oder Kompromittierung des privaten Schlüssels befürchtet wird oder bekannt ist,
- die E-Mail-Adresse des Zertifikatsinhabers sich geändert hat,
- der Zertifikatsinhaber nicht weiter in einer Geschäftsbeziehung mit der Fraunhofer-Gesellschaft steht.

Darüber hinaus sind Mitarbeitende der Fraunhofer-Gesellschaft oder Zertifikatsinhaber bzw. berechtigte Nutzer der im Zertifikat genannten E-Mail-Adresse jederzeit berechtigt, von ihnen selbst beantragte bzw. ihnen selbst zugeordnete Zertifikate aus anderen Gründen zu sperren.

Eine Sperrung durch das Trustcenter kann ebenfalls bei Bedarf aus anderen Gründen erfolgen.

7.2 Sperrung durch Mitarbeitende der Fraunhofer-Gesellschaft

Jeder Mitarbeitende der Fraunhofer-Gesellschaft kann genau die Zertifikate sperren, deren Beantragungsmöglichkeit er freigeschaltet hat und die noch nicht gesperrt sind. Der Sperrdienst wird über die Webseiten https://contacts.pki.fraunhofer.de zur Verfügung gestellt.

Ein Mitarbeitender der Fraunhofer-Gesellschaft authentifiziert sich gegenüber dem Sperrdienst durch ein Zertifikats-basiertes Login, das ihn als Fraunhofer-Mitarbeitenden ausweist, z. B. mit seiner Fraunhofer-Smartcard.

Im Anschluss werden ihm diejenigen Zertifikate der *PKI-Contacts* angezeigt, deren Beantragungsmöglichkeit er freischaltet hat und er kann eines zur Sperrung auswählen.

Vor der Durchführung der eigentlichen Sperrung werden dann nochmals die relevanten Daten des ausgewählten Zertifikats zur Kontrolle angezeigt und es muss einer der folgenden Sperrgründe ausgewählt werden:

- Kompromittierung des zugehörigen Schlüsselpaares wird befürchtet (z. B. Verlust oder Diebstahl)
- E-Mail-Adresse oder deren Nutzer hat sich geändert
- Zertifikat wird nicht länger benötigt oder sonstiger Grund

Schließlich wird ein Sperrantrag generiert und an die Zertifizierungsstelle der *PKI-Contacts* weitergeleitet. Der Fraunhofer-Mitarbeitende erhält eine Rückmeldung, dass die Sperrung in Auftrag gegeben wurde.

Der Zertifikatsinhaber wird per E-Mail an die im Zertifikat genannte E-Mail-Adresse darüber informiert, dass sein Zertifikat gesperrt wurde. Diese E-Mail kann auch Informationen darüber enthalten, von wem und aus welchem Grund das Zertifikat gesperrt wurde.

Die Zertifikatssperrung führt zur Erstellung einer aktualisierten Sperrliste.

7.3 Sperrung durch Zertifikatsinhaber

Der Zertifikatsinhaber kann unter https://contacts.pki.fraunhofer.de eine E-Mail zur Sperrung seines Zertifikats anfordern. Er muss dazu die E-Mail-Adresse angeben, auf die das zu sperrende Zertifikat ausgestellt ist. Um missbräuchliche Sperrungen zu vermeiden bzw. aufklären zu können, werden dabei Datum, Uhrzeit und die Client-IP-Adresse protokolliert und es wird darauf hingewiesen, dass ein Missbrauch Sperrantragformulars rechtliche Konsequenzen nach sich ziehen können.

Nach Absenden des Sperrantrags wird eine E-Mail mit einer Liste aller für die E-Mail-Adresse gültigen Zertifikate und zugehörigen Revozierungs-Links versendet. Durch Aufruf eines solchen Links wird der Zertifikatsnehmer auf eine spezielle Webseite der *PKI-Contacts* geführt und er kann dort nach einer expliziten Bestätigung des Sperrwunschs das Zertifikat sperren lassen.

Die Zertifikatssperrung führt zur Erstellung einer aktualisierten Sperrliste.

7.4 Sperrliste

Die Sperrliste (Certificate Revocation List, CRL) der *PKI-Contacts* kann unter https://contacts.pki.fraunhofer.de heruntergeladen werden.

Die Sperrliste wird mindestens einmal pro Woche erstellt und veröffentlicht.

Eine neue Sperrliste wird weiterhin jeweils nach einer Sperrung automatisch generiert und zeitnah unter https://contacts.pki.fraunhofer.de veröffentlicht, im Allgemeinen spätestens innerhalb von 30 Minuten nach Eingang der Sperrung.

8 Kosten

Für die Bereitstellung der Infrastruktur und des Dienstes *PKI-Contacts*, sowie für die Erstellung, Nutzung, Sperrung von Zertifikaten und Sperrlisten und die Zertifikatssuche fallen derzeit keine Kosten an.

Der in Kapitel 9 beschriebene allgemeine Support ist ebenfalls kostenlos.

9 Support

Allgemeiner Support wird von der Fraunhofer-Gesellschaft durch das CC-PKI zur Verfügung gestellt, erfolgt jedoch nur in geringem Umfang und ohne garantierte Service-Zeiten oder Service-Levels.

Support-Anfragen sind für Mitarbeitende der Fraunhofer-Gesellschaft möglich, die ihre Anfragen an die unter auf der Webseite der *PKI-Contacts* (https://contacts.pki.fraunhofer.de) genannte Kontaktadresse richten können.

Kommunikationspartner der Fraunhofer-Gesellschaft sollen sich bei Fragen mit demjenigen Ansprechpartner bei Fraunhofer in Verbindung setzen, der für sie die Freischaltung der Zertifikatbeantragungsmöglichkeit durchgeführt hat.

10 Verzeichnis der Quellen

[FhG-PKI] Die Fraunhofer-PKI, eine Fraunhofer-interne Public Key Infrastructure für interne und externe Mitarbeitende der Fraunhofer-Gesellschaft, http://www.pki.fraunhofer.de

[PKI-Contacts] Zertifizierungsstelle für Kontakte der Fraunhofer-Gesellschaft – PKI-Contacts, https://contacts.pki.fraunhofer.de

Abkürzungen / Begriffe

CC-PKI	Competence Center Public Key Infrastructures, eine Einrichtung der Fraunhofer-Gesellschaft
CRL	Certificate Revocation List, Sperrliste
PKI	Public Key Infrastruktur