DFN – PCA
Die World Wide Web Policy

Zertifizierungsrichtlinien für die DFN-PCA
Stand: 28. Dezember 2001
Version: 1.2

DFN-CERT GmbH “Zentrum für sichere Netzdienste”
DFN-PCA
Oberstraße 14 b
D - 20144 Hamburg
Germany

Inhaltsverzeichnis

1 Einleitung **3**

2 Identität der PCA **3**

3 Zuständigkeitsbereich der PCA **4**

3.1 Rechtliche Bedeutung 4

3.2 Die DFN-Zertifizierungshierarchie 5

3.3 Registrierungsinstanzen (RA) 6

4 Sicherheit der PCA-Ausstattung **6**

4.1 Sicherheitsanforderungen an die DFN-PCA 7

4.2 Sicherheitsanforderungen an CAs 8

4.3 Sicherheitsanforderungen an RAs 9

4.4 Sicherheitsanforderungen an Endteilnehmer 9

5 Zertifizierungsregeln **10**

5.1 Regeln für die Zertifizierung von CAs 12

5.2 Regeln für die Zertifizierung von RAs 12

5.3 Regeln für die Zertifizierung von Endteilnehmern 12

5.4 Regeln für die Cross-Zertifizierung zweier PCAs / CAs 13

6 Management von Zertifikaten **14**

7 Widerruf von Zertifikaten **14**

8 Regeln für die Namensgebung **15**

8.1 Wahl eines Namens für CAs 16

8.2 Wahl eines Namens für RAs und Endteilnehmer 16

9 Verschiedenes **17**

DFN – PCA: Die World Wide Web Policy

Vorbemerkung

Dies ist die Version 1.2 der World Wide Web Policy der DFN-PCA. Diese Version ist gültig bis zum 31. Januar 2010 oder bis eine neue Version dieser Policy veröffentlicht wird (je nachdem, welches dieser Ereignisse zuerst eintritt) und ist angelehnt an die Low-Level Policy Version 1.4 der DFN-PCA. Sie ist identisch mit der WWW-Policy Version 1.0 der DFN-PCA bis auf die neue Anschrift und die Änderungen, die durch den Wegfall des Status' als Forschungsprojekt erforderlich wurden.

1 Einleitung

Dieses Dokument enthält die Zertifizierungsrichtlinien (die sog. "Policy" bzw. "Certification Practice Statement", CPS) der obersten Zertifizierungsinstanz des *Vereins zur Förderung eines Deutschen Forschungsnetzes e.V.* (DFN-PCA).

Die in diesem Dokument getroffenen Aussagen sind für die Arbeit der DFN-PCA und der durch die DFN-PCA zertifizierten CAs bindend, soweit sie nicht gesetzlichen Regelungen widersprechen. Die DFN-PCA zertifiziert ausschließlich nach den Richtlinien dieser Policy. Um die internationale Zusammenarbeit mit anderen CAs zu ermöglichen, wird ferner eine englische Übersetzung dieses Dokumentes veröffentlicht werden; maßgeblich ist in jedem Fall die hier vorliegende deutsche Version in seiner aktuellen Fassung.

2 Identität der PCA

Adresse

DFN-CERT GmbH "Zentrum für sichere Netzdienste"
DFN-PCA
Oberstraße 14 b
D - 20144 Hamburg
Germany

Telefon: 040 - 80 80 77 - 555
Telefax: 040 - 80 80 77 - 556

Email-Adressen

`certify@pca.dfn.de`	(für Fragen bzgl. der Zertifizierung)
`dfnpca@pca.dfn.de`	(für allgemeine Anfragen an die DFN-PCA)
`s=dfnpca;ou=pca;p=dfn;a=d400;c=de`	(X.400)

Informationsdienste der DFN-PCA

FTP-Server:	`ftp://ftp.pca.dfn.de/pub/pca/`
WWW-Server:	`http://www.pca.dfn.de/dfnpca/`

Gültigkeit dieses Dokumentes

01. Dezember 2001 bis 31. Januar 2010 oder bis eine neue Version dieser Policy veröffentlicht wird (je nachdem, welches dieser Ereignisse zuerst eintritt)

Version dieses Dokumentes

1.2

3 Zuständigkeitsbereich der PCA

Der Zuständigkeitsbereich der DFN-PCA umfaßt alle Mitgliedseinrichtungen des DFN-Vereins, in erster Linie also natürliche sowie juristische Personen des öffentlichen oder privaten Rechts aus Wissenschaft und Forschung. Weitere Organisationen und Teilnehmer können auf Anfrage zertifiziert werden.

Die DFN-PCA wird ausschließlich Zertifikate für CAs, nicht aber für Endteilnehmer erteilen. Die DFN-PCA wird zusätzlich die Dienste einer oder mehrerer untergeordneter CAs anbieten, um Zertifikate für Endteilnehmer ausstellen zu können, deren Einrichtung noch keine eigene CA betreibt.

Diese Policy unterstützt insbesondere das Zertifikat-Format X.509v3, das in aktuellen Standard-Browsern für unterschiedliche Anwendungen (SSL und S/MIME bzw. “Code Signing”) eingesetzt wird.

3.1 Rechtliche Bedeutung

Eine Zertifizierung durch die DFN-PCA (oder untergeordnete CAs) zieht keinerlei rechtliche Bedeutung nach sich; ein gesetzlicher Anspruch auf die Erteilung eines Zertifikates durch die DFN-PCA oder untergeordnete CAs besteht nicht. Insbesondere ist die allgemeine rechtliche Relevanz *digitaler Signaturen derzeit unklar. Der Sinn einer DFN-weiten Public Key-Infrastruktur liegt in der Schaffung der technischen Voraussetzungen für eine gesicherte elektronische Kommunikation. Insbesondere der DFN-Verein sowie die Mitarbeiter der DFN-PCA übernehmen keine Form der Gewährleistung. Alle Aufgaben werden von den PCA-Mitarbeitern nach bestem Wissen und Gewissen durchgeführt.*

Die dieser Policy zugrundeliegenden Anforderungen an technische Komponenten und Verfahren zur Zertifizierung sind derzeit nicht Signaturgesetz-konform.

3.2 Die DFN-Zertifizierungshierarchie

Die Zertifizierungshierarchie unterhalb der DFN-PCA besteht aus drei verschiedenen Einheiten (Zertifikatnehmern):

- Zertifizierungsinstanzen (CAs)
- Registrierungsinstanzen (RAs, s. 3.3)
- Endteilnehmer:
  - WWW-Server
  - Benutzer (Client-Zertifikate für SSL, S/MIME, "Code Signing")

Die internationale Anbindung der DFN-Zertifizierungshierarchie an andere Hierarchien kann durch eine gegenseitige Zertifizierung (Cross-Zertifizierung, s. Abschnitt 5.4) der DFN-PCA mit anderen PCAs, oder die Einbindung der DFN-PCA in europäische Zertifizierungshierarchien erfolgen.

Unterhalb der DFN-PCA operierende CAs haben ihrerseits die Möglichkeit, durch eine Cross-Zertifizierung mit anderen CAs eigene Verbindungen zu Zertifizierungsinstanzen bzw. -infrastrukturen von Einrichtungen herzustellen, welche nicht dem DFN-Verein angehören (s. Abschnitt 5.4).

Der öffentliche Schlüssel (Public Key) der DFN-PCA ist in einem selbst-signierten Zertifikat (Wurzel-Zertifikat), ausgestellt durch die DFN-PCA, enthalten. Alle Teilnehmer der Infrastruktur erhalten dieses Wurzel-Zertifikat im Zuge der eigenen Zertifizierung und können somit die Authentizität und Gültigkeit aller unterhalb der DFN-PCA erteilten Zertifikate überprüfen.

Anonyme oder pseudonyme Zertifikate können für Benutzer, nicht aber für CAs erstellt werden, wenn sie als solche erkennbar sind.

3.3 Registrierungsinstanzen (RA)

Alle CAs haben die Möglichkeit, vertrauenswürdige Registrierungsinstanzen (RAs) für die lokale Überprüfung (Registrierung) von Identität und Authentizität einzelner Endteilnehmer zu benennen. RAs dürfen lediglich zur Registrierung und Überprüfung von Endteilnehmern, nicht jedoch von CAs, eingesetzt werden.

Bei einer RA handelt es sich um einen in der üblichen Weise durch eine CA zertifizierten Benutzer, der im Auftrag seiner CA die Überprüfung anderer Endteilnehmer vor deren Zertifizierung durch die CA übernimmt.

Eine RA darf weder asymmetrische Schlüsselpaare für andere Teilnehmer erzeugen, noch kann sie selbst Zertifikate erteilen oder widerrufen. Die RA leitet, nachdem die Identität des Endteilnehmers in geeigneter Weise überprüft wurde (s. Kapitel 5), den Zertifizierungswunsch ("Certificate Signing Request", CSR) eines Endteilnehmers an die CA weiter. Die Übermittlung der registrierten Daten kann dabei durch persönliche Übergabe an die CA oder durch elektronische Übermittlung geschehen. Um einen Mißbrauch auszuschließen, muß jede elektronische Übermittlung an die CA durch die RA digital signiert werden.

In solchen Fällen, in denen die Schlüsselerzeugung nicht vom Endteilnehmer selbst vorgenommen wird, leitet die RA nur die Identitätsinformationen des Endteilnehmers an die CA weiter. Empfängt eine CA den Zertifizierungswunsch eines Endteilnehmers durch eine vertrauenswürdige RA, hat sie grundsätzlich die Gültigkeit der RA-Signatur zu verifizieren, falls die registrierten Daten elektronisch übermittelt wurden. Das von der CA neu ausgestellte Zertifikat wird anschließend sowohl an die RA als auch an den Endteilnehmer übermittelt.

Jede CA kann beliebig viele Personen zu RAs ernennen. Die CA kann die Unterzeichnung einer Vereinbarung verlangen, welche die RA an bestimmte Richtlinien, festgelegt durch die CA, bindet. Insbesondere sollen von der RA die Sicherheitsanforderungen nach Abschnitt 4.3 eingehalten werden. Jede CA sollte diese Richtlinien, zusammen mit einer Liste aller von ihr benannten RAs veröffentlichen.

4 Sicherheit der PCA-Ausstattung

Durch die Teilnahme an einer Public Key-Infrastruktur entstehen für alle Teilnehmer bestimmte Anforderungen hinsichtlich der Sicherheit der eingesetzten Hard- und Software einerseits, sowie dem verantwortungsvollen Umgang mit kryptographischen Schlüsseln andererseits. Die Anforderungen an die DFN-PCA und die CAs sind dabei naturgemäß höher, da der Mißbrauch eines PCA-/CA-Schlüssels allen untergeordneten Zertifikaten die Vertrauenswürdigkeit entziehen würde.

4.1 Sicherheitsanforderungen an die DFN-PCA

Folgende Anforderungen werden an die DFN-PCA gestellt:

- Für die Dienste der DFN-PCA wird ein dedizierter Rechner eingesetzt, der über keinerlei Verbindung zu einem Rechnernetz verfügt. Zertifikate werden ausschließlich off-line auf dem dedizierten Rechner erzeugt.

- Jeglicher Datenaustausch mit vernetzten Rechnern wird von Mitarbeitern der DFN-PCA per externem Datenträger (z.B. Diskette oder Magnetband) vorgenommen; es findet keine automatisierte Bearbeitung der Daten statt. Sämtliche schlüsseltragenden Datenträger werden in unbenutztem Zustand an einem sicheren Ort verwahrt.

- Geheime Schlüssel der DFN-PCA zur Erzeugung digitaler Signaturen werden von den Mitarbeitern ausschließlich auf dem dedizierten Rechner erzeugt und verwendet sowie auf externer Peripherie (z.B. SmartCard, Wechsel-Festplatte, Diskette) gespeichert, soweit dies von Hard- und Software unterstützt wird. Der Zugriff auf diese Peripherie wird durch nicht-triviale Passworte (Mindestlänge: 8 Zeichen) bzw. PINs geschützt, welche nur den PCA-Mitarbeitern bekannt sind und niemals im Klartext abgelegt bzw. über ungeschützte Netzwerkverbindungen gesendet werden. Die Peripherie wird nicht auf anderen Rechnern eingesetzt.

- Mit geheimen Signatur-Schlüsseln der PCA werden ausschließlich CA-Schlüssel bzw. Widerrufslisten (CRLs) unterschrieben oder Cross-Zertifikate erstellt. Für jegliche Standard-Kommunikation werden geheime Signatur-Schlüssel nicht verwendet; von der DFN-PCA werden daher unterschiedliche asymmetrische Schlüsselpaare zum Signieren und Entschlüsseln verwendet.

- Asymmetrische Schlüsselpaare der DFN-PCA zur Erzeugung von Signaturen haben eine Länge von mindestens 2048 Bit RSA (oder vergleichbares Niveau).

- Die Integrität aller relevanten Daten und Programme auf Rechnern der DFN-PCA wird unter Zuhilfenahme kryptographischer Applikationen regelmäßig verifiziert. Ferner werden sämtliche Daten von den PCA-Mitarbeitern vertraulich behandelt; alle geltenden gesetzlichen Datenschutzbestimmungen werden eingehalten.

- Von allen relevanten (elektronischen) Daten der DFN-PCA wird in regelmäßigen, kurzen Abständen eine Datensicherung durchgeführt, deren Datenträger an einem externen Standort aufbewahrt werden. Ein geeignetes Backup-Konzept für die DFN-PCA liegt dieser Datensicherung zugrunde; dieses soll insbesondere lange Aufbewahrungszeiten von Zertifikaten und CRLs ermöglichen.

4.2 Sicherheitsanforderungen an CAs

Folgende Anforderungen werden an alle zertifizierten CAs unterhalb der DFN-PCA gestellt:

- Für die Dienste der CA muß ein Rechner eingesetzt werden, der in geeigneter Weise vor mißbräuchlicher Benutzung geschützt ist. Der unbefugte Zugriff auf den CA-Rechner und eventuell gespeicherte Schlüsseldaten ist durch den Einsatz geeigneter Hard- und Software zu unterbinden. Insbesondere wird empfohlen, einen Rechner ohne jeglichen Netzwerkanschluß einzusetzen und diesen physikalisch zu schützen.

- Geheime Schlüssel der CA zum Erzeugen digitaler Signaturen müssen ausreichend vor Mißbrauch durch Unbefugte geschützt und dürfen nicht weitergegeben werden. Die Verantwortung hierfür liegt bei den Administratoren der CA, die daher angehalten sind, externe Peripherie (z.B. SmartCard, Wechsel-Festplatte, Diskette) zum Schutz der geheimen CA-Schlüssel einzusetzen. Der Zugriff auf diese geheimen CA-Schlüssel ist in jedem Fall durch nicht-triviale Passworte (Mindestlänge: 8 Zeichen) bzw. PINs zu schützen, welche nur den CA-Administratoren bekannt sein und niemals im Klartext abgelegt bzw. über ungeschützte Netzwerkverbindungen gesendet werden dürfen. Die externe Peripherie darf nicht auf anderen Rechnern eingesetzt werden.

- Mit dem geheimen Signatur-Schlüssel der CA dürfen ausschließlich CA- oder Endteilnehmer-Schlüssel bzw. Widerrufslisten (CRLs) unterschrieben oder Cross-Zertifikate erstellt werden. Für jegliche Standard-Kommunikation darf der geheime Signatur-Schlüssel nicht verwendet werden.

- Jede CA muß asymmetrische Schlüsselpaare grundsätzlich selbst erzeugen; es findet keine Schlüsselerzeugung durch die DFN-PCA oder andere CAs statt.

- Asymmetrische Schlüsselpaare der CA zur Erzeugung von Signaturen müssen eine Mindestlänge von 1024 Bit RSA (oder vergleichbares Niveau) aufweisen; es werden jedoch deutlich größere Schlüssellängen empfohlen.

- In solchen Fällen, in denen eine CA asymmetrische Schlüsselpaare für die Endteilnehmer erzeugt, hat die CA dies auf dem dedizierten CA-Rechner durchzuführen. Ferner muß sichergestellt werden, daß nach der Zertifizierung und Schlüsselübergabe an den Endteilnehmer alle Kopien des geheimen Schlüssels des Endteilnehmers auf Seiten der CA endgültig gelöscht werden. Die CA darf in keinem Fall nach der Schlüsselübergabe geheime Schlüssel oder Teile des geheimen Schlüssels des Endteilnehmers aufbewahren, hinterlegen, oder an Dritte weitergeben. Der Prozeß der Löschung des geheimen Schlüssels ist in geeigneter Weise zu dokumentieren.

- Sämtliche bei der Zertifizierung anfallenden Daten müssen von den CA-Mitarbeitern vertraulich behandelt werden. Die für die CA geltenden gesetzlichen Datenschutzbestimmungen sind einzuhalten.

Die in diesem Abschnitt beschriebenen Sicherheitsanforderungen an CAs gelten in gleicher Weise auch für die von den Mitarbeitern der DFN-PCA direkt betriebenen CAs, welche durch die DFN-PCA zertifiziert werden. Diese CAs erzeugen jedoch niemals asymmetrische Schlüsselpaare für andere Endteilnehmer.

4.3 Sicherheitsanforderungen an RAs

Folgende Anforderungen werden an die von einer CA eingesetzten RAs gestellt:

- Für die Dienste der RA muß ein Rechner eingesetzt werden, der in geeigneter Weise vor mißbräuchlicher Benutzung geschützt ist. Der unbefugte Zugriff auf den RA-Rechner und eventuell gespeicherte Schlüsseldaten ist zu unterbinden.

- Geheime Schlüssel der RA zum Erzeugen digitaler Signaturen müssen ausreichend vor Mißbrauch durch Unbefugte geschützt und dürfen nicht weitergegeben werden. Werden keine SmartCards oder andere Peripherie zum Speichern geheimer Schlüssel eingesetzt, ist der Zugriff auf die geheimen Schlüssel durch nicht-triviale Passworte (Mindestlänge: 8 Zeichen) bzw. PINs zu schützen. Weder die optionale Peripherie noch Passwort bzw. PIN dürfen an andere Personen weitergegeben werden. Passwort bzw. PIN dürfen niemals im Klartext abgelegt bzw. über ungeschützte Netzwerkverbindungen gesendet werden.

- Asymmetrische Schlüsselpaare der RA zur Erzeugung von Signaturen müssen eine Mindestlänge von 1024 Bit RSA (oder vergleichbares Niveau) aufweisen.

- Weitere Anforderungen können von der für die RA zuständigen CA festgelegt werden.

4.4 Sicherheitsanforderungen an Endteilnehmer

Der geheime Schlüssel des Endteilnehmers muß ausreichend vor Mißbrauch durch Unbefugte geschützt und darf nicht weitergegeben werden; hierfür ist jeder Endteilnehmer selbst verantwortlich.

Wird keine externe Peripherie (z.B. Diskette) zum Speichern des geheimen Schlüssels eingesetzt, sollte der Zugriff auf den geheimen Schlüssel des Endteilnehmers durch das Setzen eines nicht-trivialen Passworts (Mindestlänge: 8 Zeichen) bzw. einer PIN geschützt werden. Weder die optionale Peripherie noch Passwort bzw. PIN dürfen an andere Personen weitergegeben werden. Passwort bzw. PIN dürfen niemals im Klartext abgelegt bzw. über ungeschützte Netzwerkverbindungen gesendet werden.

Sicherheitsanforderungen an Benutzer (SSL, S/MIME, "Code Signing")

Benutzer im Sinne dieser Policy sind einzelne Personen.

- Das asymmetrische Schlüsselpaar des Benutzers muß eine minimale Länge von 512 Bit RSA (oder vergleichbares Niveau) aufweisen. Die Wahl größerer Schlüssellängen wird dringend empfohlen und richtet sich nach der technischen Verfügbarkeit.
- Der Benutzer hat den Zugriff auf seinen geheimen Schlüssel durch das Setzen eines nicht-trivialen Passworts zu schützen, sofern die eingesetzte Applikation dies unterstützt.
- Das Verzeichnis bzw. die Dateien, in dem die kryptographischen Schlüssel von der Applikation gespeichert werden, sind vom Benutzer nach Maßgabe der Möglichkeiten vor unbefugtem Mißbrauch zu schützen. Dies kann z.B. durch das Setzen bestimmter Zugriffsrechte geschehen, sofern das eingesetzte Betriebssystem dies unterstützt. Die Speicherung der kryptographischen Schlüssel auf externen Datenträgern (z.B. Diskette) wird dringend empfohlen.

Sicherheitsanforderungen an WWW-Server

- Das asymmetrische Schlüsselpaar für WWW-Server muß eine minimale Länge von 1024 Bit RSA (oder vergleichbares Niveau) aufweisen.
- Da der geheime Schlüssel üblicherweise einmalig beim Starten des WWW-Servers (z.B. durch die Eingabe eines nicht-trivialen Passworts) entsperrt wird, ist der Server-Rechner samt entsprechender Dateien und Verzeichnisse durch geeignete (auch physikalische) Maßnahmen vor mißbräuchlicher Benutzung zu schützen. Dies sollte insbesondere durch das Setzen entsprechender Zugriffsrechte geschehen. Die Speicherung der kryptographischen Schlüssel auf externen Datenträgern (z.B. Diskette) wird dringend empfohlen.

5 Zertifizierungsregeln

Dieser Abschnitt beschreibt technische und organisatorische Richtlinien und Prozeduren, die vor einer Zertifizierung von CAs oder Endteilnehmern zu beachten sind.

Sowohl CAs als auch Endteilnehmer werden mit eindeutigen Namen bezeichnet, deren korrekter Wahl eine besondere Bedeutung zukommt. Die Wahl dieser Namen wird in Abschnitt 8 beschrieben.

Um unerlaubte Zertifizierungswünsche zu erkennen, hat sich die zertifizierende Instanz (CA bzw. PCA) vor jeder Zertifizierung in geeigneter Weise durch technische und organisatorische Maßnahmen von der Identität desjenigen Schlüsselinhabers zu überzeugen, welcher eine Zertifizierung wünscht. In diesem Zusammenhang kann die CA auch verlangen, daß der Schlüsselinhaber vor einer Zertifizierung den Besitz des entsprechenden geheimen Schlüssels nachweist ("proof of possession"). Dies kann beispielsweise durch den Austausch digital signierter Nachrichten geschehen.

Der Vorgang der Registrierung kann nur durch persönlichen Kontakt – oder in einzelnen Ausnahmefällen durch telefonischen Rückruf zu persönlich gut bekannten Personen – vor der Zertifizierung erfolgen. Setzt eine CA RAs ein, liegt die Verantwortung der Identitätsprüfung bei der RA, kann aber dennoch von der CA übernommen werden. In keinem Fall dürfen jedoch Zertifizierungswünsche automatisiert bearbeitet werden.

Zertifikate werden ausschließlich dann erteilt, wenn der zu zertifizierende Public Key über die in Abschnitt 4 festgelegten Mindestlängen verfügt und sich die zertifizierende Instanz in geeigneter Weise von der Identität des Schlüsselinhabers und dem Besitz des korrekten asymmetrischen Schlüsselpaares überzeugt hat. Das neu ausgestellte Zertifikat wird dem Zertifikatnehmer unmittelbar nach der Zertifizierung beispielsweise per Email oder über eine URL übermittelt. Der Zertifikatnehmer ist angehalten, die Korrektheit des eigenen Zertifikates sowie der übergeordneten CA-Zertifikate sofort zu verifizieren.

Jedes Zertifikat muß eine Seriennummer beinhalten, die von der zertifizierenden CA vergeben wird. Dabei hat jede CA bei der Zertifizierung zu gewährleisten, daß von ihr keine Seriennummer mehrfach vergeben wird.

Zertifikate werden in der Regel nicht automatisch durch die ausstellende CA erneuert; Anträge auf Re-Zertifizierung sind gegebenenfalls bei der entsprechenden CA zu stellen.

Zertifikat-Erweiterungen

X.509v3-Zertifikate zeichnen sich dadurch aus, daß jedes Zertifikat beliebige Erweiterungen ("certificate extensions") enthalten kann. Jede Erweiterung kann darüber hinaus durch das Setzen eines bestimmten Bits ("critical flag") als besonders signifikant gekennzeichnet werden.

Zertifikat-Erweiterungen werden von der jeweiligen CA bei der Zertifizierung in das Zertifikat aufgenommen; Erweiterungen können jedoch auch schon im Zertifizierungswunsch ("Certificate Signing Request", CSR) vorgeschlagen werden.

Jede CA sollte alle von ihr unterstützten Erweiterungen bekanntgeben. Insbesondere kann eine CA durch solche Erweiterungen die Anwendung eines ausgestellten Zertifikates auf bestimmte Funktionen (z.B. das Signieren von Objekten wie Java Applets) beschränken. CAs wird dringend empfohlen, nur Zertifikate nach X.509v3 zu erzeugen und verbreitete Standard-Erweiterungen (vgl. X.509v3, PKIX, Netscape) zu unterstützen.

Empfängt eine CA einen Zertifizierungswunsch mit unbekannten Zertifikat-Erweiterungen, sollte sie kein Zertifikat erteilen.

5.1 Regeln für die Zertifizierung von CAs

CAs, die von der DFN-PCA zertifiziert werden möchten, unterzeichnen vor der Zertifizierung eine Vereinbarung mit der DFN-PCA. Diese Vereinbarung enthält eine Erklärung darüber, daß die Richtlinien dieser Policy akzeptiert werden und deren Einhaltung beim Betrieb der eigenen CA zugestimmt wird. Insbesondere müssen von den CA-Administratoren die Sicherheitsanforderungen nach Abschnitt 4.2 eingehalten werden.

Berechtigt zu der Unterzeichnung dieser Vereinbarung ist eine für den Betrieb der CA verantwortliche Person. Diese Berechtigung kann von der DFN-PCA vor der Ausstellung eines Zertifikates überprüft werden.

Die DFN-PCA behält sich vor, CAs auf deren Eignung sowie das Vorhandensein der technischen Voraussetzungen vor Ort zu überprüfen.

Eine CA generiert ihr eigenes asymmetrisches Schlüsselpaar und übermittelt anschließend den Zertifizierungswunsch (CSR) an die DFN-PCA. Dieser Zertifizierungswunsch sollte zum Schutz digital signiert werden; die zertifizierende CA hat vor der Zertifizierung die digitale Signatur zu verifizieren. Die Übermittlung des CSR an die CA kann per Email oder durch den Austausch eines Datenträgers geschehen.

Vor der Zertifizierung einer CA verifiziert ein Mitarbeiter der DFN-PCA die Identität des CA-Administrators, die Zugehörigkeit des CA-Administrators zu der jeweiligen Einrichtung, sowie gegebenenfalls deren Existenz. Diese Überprüfung erfordert in jedem Fall ein persönliches Treffen zwischen einem CA-Administrator und einem Mitarbeiter der DFN-PCA. Für den Prozeß der Verifikation ist die Vorlage eines Personalausweises/Reisepasses bzw. eines vergleichbaren Dokumentes erforderlich.

Die Einrichtung organisationsweiter Sub-CA-Hierarchien obliegt der Verantwortung der obersten CA einer jeweiligen Organisation. Für untergeordnete Sub-CAs gelten die Regeln dieses Abschnitts entsprechend; über diese Policy hinausgehende Richtlinien können bei Bedarf von dieser CA in einer eigenen Policy festgelegt werden.

Zertifikate für CAs haben eine Gültigkeitsdauer von maximal 2 Jahren.

5.2 Regeln für die Zertifizierung von RAs

Ein RA-Zertifikat unterscheidet sich nicht von einem üblichen Benutzer-Zertifikat. Für die Zertifizierung von RAs siehe daher den folgenden Abschnitt.

5.3 Regeln für die Zertifizierung von Endteilnehmern

Endteilnehmer, welche zertifiziert werden möchten, generieren zunächst ein persönliches asymmetrisches Schlüsselpaar und übermitteln anschließend den Zertifizierungswunsch (CSR) an die zuständige RA bzw. CA. Dieser Zertifizierungswunsch sollte zum Schutz digital signiert werden; die zertifizierende CA hat vor der Zertifizierung die digitale Signatur zu verifizieren. Gegebenenfalls wird das asymmetrische Schlüsselpaar des Endteilnehmers auch von der CA erzeugt; wobei von der CA unbedingt die in Abschnitt 4.2 beschriebenen Sicherheitsanforderungen einzuhalten sind.

Unabhängig vom Einsatz einer RA hat sich der Endteilnehmer persönlich vorzustellen, um der CA (bzw. RA) die Verifikation dessen Identität und die korrekte Zuordnung der im Zertifikat angegebenen Informationen zu diesem Endteilnehmer (sowie gegebenenfalls die Zuordnung der Identität zu einem Pseudonym) zu ermöglichen. Für den Prozeß der Verifikation ist die Vorlage eines Personalausweises/Reisepasses bzw. eines vergleichbaren Dokumentes erforderlich. Erfolgt die Verifikation durch eine RA, leitet diese den vom Endteilnehmer vorgelegten Zertifizierungswunsch (CSR) an die zuständige CA weiter (vgl. Abschnitt 3.3).

Zertifikate für Endteilnehmer haben eine Gültigkeitsdauer von maximal einem Jahr.

Zusätzliche Regeln für die Zertifizierung von WWW-Servern

Zusätzlich zu den oben beschriebenen Zertifizierungsregeln für Endteilnehmer gelten besondere Richtlinien bei der Zertifizierung von WWW-Servern, welche nicht einer einzelnen Person, sondern einem Rechner (-namen) zugeordnet sind.

Sollen WWW-Server zertifiziert werden, hat ein Administrator dieses Servers den Zertifizierungswunsch (CSR) an die zertifizierende Instanz zu übermitteln. Diese hat vor der Zertifizierung in geeigneter Weise die Eindeutigkeit folgender Informationen zu überprüfen:

- Zugehörigkeit des Servers zu einer bestimmten Organisation
- Identität der Organisation
- Identität des Server-Administrators

5.4 Regeln für die Cross-Zertifizierung zweier PCAs / CAs

Um die Anbindung an andere Zertifizierungshierarchien zu erlauben, besteht sowohl für CAs als auch für die PCA die Möglichkeit der Cross-Zertifizierung mit anderen CAs. Der Vorgang unterscheidet sich dabei für PCAs und CAs nicht.

Vor einer Cross-Zertifizierung haben sich die verantwortlichen CA-Administratoren mit den Zertifizierungsrichtlinien der jeweils anderen CA vertraut zu machen. Der Vorgang der Cross-Zertifizierung besagt, daß die Policy der anderen CA bei der Zertifizierung bekannt war und deren aktuelle Richtlinien akzeptiert werden, nicht jedoch, daß diese Richtlinien mit der eigenen Policy übereinstimmen müssen. Die Cross-Zertifizierung bezieht sich also immer auf die momentan gültige Policy einer CA; wird diese grundlegend geändert, ist eine erneute Cross-Zertifizierung erforderlich.

Die Cross-Zertifizierung einer CA unterscheidet sich organisatorisch nicht von der Zertifizierung eines Endteilnehmers. Der Public Key bzw. das Zertifikat einer CA wird per Email oder durch den Austausch eines Datenträgers an die andere CA übermittelt. Daran anschließend hat eine gegenseitige Verifikation der Identitäten zu erfolgen, um unerlaubte Zertifizierungswünsche auszuschließen. Dieser Vorgang muß bei einem persönlichen Treffen der CA-Administratoren stattfinden.

Nach der Zertifizierung veröffentlicht die CA das erteilte Cross-Zertifikat, welches den Public Key der anderen CA enthält. Ein Cross-Zertifikat sollte keine längere Gültigkeitsdauer als das reguläre Zertifikat der cross-zertifizierten CA besitzen.

6 Management von Zertifikaten

Alle Teilnehmer der DFN-Zertifizierungshierarchie erklären sich grundsätzlich mit der Veröffentlichung ihres Zertifikates einverstanden. Es besteht jedoch die Möglichkeit, bei der Beantragung eines Zertifikates individuell einer Veröffentlichung zu widersprechen.

Jede CA (inkl. der DFN-PCA) ist für die Bereitstellung aller selbst ausgestellten Zertifikate verantwortlich. Hierzu gehören sowohl das eigene als auch die übergeordneten CA-Zertifikate. Von einer CA neu ausgestellte Zertifikate und CRLs (s. Abschnitt 7) müssen innerhalb einer angemessenen Zeitspanne (üblicherweise innerhalb eines Werktages) veröffentlicht werden.

Für die Bereitstellung von Zertifikaten sind von jeder CA Informationsdienste (Verzeichnisse) einzurichten, deren Aufgabe die Verteilung von Zertifikaten und CRLs ist. Geeignet hierfür sind insbesondere WWW-, FTP-, Mail-, LDAP- und X.500-Server, deren Daten ausreichend vor Mißbrauch geschützt werden müssen. Der Betrieb solcher Informationsdienste kann von Partner-Einrichtungen der CA übernommen werden; in Ausnahmefällen übernimmt die DFN-PCA auf Anfrage die Veröffentlichung von Zertifikaten und CRLs einer CA.

7 Widerruf von Zertifikaten

Jede CA (inkl. der DFN-PCA) kann von ihr erteilte Zertifikate jederzeit vor Ablauf der Gültigkeitsdauer ohne Angabe expliziter Gründe widerrufen. Ursachen für den Widerruf eines Zertifikates können beispielsweise das Bekanntwerden mißbräuchlicher Handlungen eines CA-Administrators oder das Nichtbefolgen auch einzelner Richtlinien dieser Policy sein. Andere Gründe sind beispielsweise das Ausscheiden eines Mitarbeiters aus einer Einrichtung oder die Änderung des Namens.

Jeder Zertifikatnehmer kann von der Instanz, die seinen Public Key zertifiziert hat, ohne Angabe von Gründen verlangen, daß diese ein für ihn ausgestelltes Zertifikat widerruft. Die betreffende CA hat diesem Verlangen innerhalb einer angemessenen Zeitspanne nachzukommen, sobald sie sich durch geeignete Schritte davon überzeugt hat, daß der Antrag vom Zertifikatnehmer selbst stammt bzw. von ihm autorisiert ist. Werden der Mißbrauch oder die Kompromittierung des eigenen geheimen Schlüssels bekannt, sollte jeder Teilnehmer unverzüglich die zertifizierende Instanz benachrichtigen und den Widerruf des eigenen Zertifikates veranlassen.

Zertifikate können nur von der ausstellenden Instanz widerrufen werden. Alle widerrufenen Zertifikate werden von der zuständigen CA auf einer Widerrufsliste ("Certificate Revocation List", CRL) veröffentlicht, welche allen Teilnehmern zur Verfügung gestellt werden muß. Diese CRL enthält u.a. das Datum der CRL-Herausgabe (z.B. in Form eines Zeitstempels) und wird von der CA digital signiert. Widerrufene Zertifikate bleiben solange auf der CRL, bis die ursprüngliche Gültigkeitsdauer überschritten wurde. Dabei werden auch solche Zertifikate auf einer CRL veröffentlicht, gegen deren Veröffentlichung bei der Zertifizierung widersprochen wurde.

Einmal widerrufene Zertifikate können nicht erneuert oder verlängert werden. Jedoch hat jeder Teilnehmer grundsätzlich die Möglichkeit, ein neues Zertifikat zu beantragen.

Unmittelbar nach der Aufnahme des eigenen Betriebs hat jede CA eine neue (leere) CRL herauszugeben. Daran anschließend müssen in regelmäßigen Abständen (z.B. monatlich) neue CRLs herausgeben werden, auch wenn in der Zwischenzeit keine weiteren Zertifikate durch die CA widerrufen wurden. Es wird empfohlen, alte CRLs zu archivieren, um die Gültigkeit von Zertifikaten auch zu einem späteren Zeitpunkt verifizieren zu können.

Die DFN-PCA wird mindestens einmal pro Monat eine CRL veröffentlichen.

Für die Bereitstellung von CRLs sind von der CA Informationsdienste (Verzeichnisse) einzurichten, deren Aufgabe die Verteilung von Zertifikaten und CRLs (vgl. Abschnitt 6) ist. Da viele Softwareprodukte die Bearbeitung von CRLs derzeit nur unzureichend unterstützen, ist jede CA angehalten, ihre Zertifikatnehmer hierüber zu informieren und gegebenenfalls eigene Lösungen für die CRL-Verteilung zu implementieren.

8 Regeln für die Namensgebung

Allen Zertifikatnehmern wird ein eindeutiger Name (Distinguished Name, DN) zugeordnet, welcher bei der Ausstellung eines Zertifikates für einen Teilnehmer als dessen Subjektname zu verwenden ist. Ein DN enthält eine Folge von eindeutig kennzeichnenden Namensattributen, durch die alle Teilnehmer einer Hierarchie referenziert werden können; auf unübliche Sonderzeichen (z.B. Umlaute) innerhalb dieses Namens sollte aus Gründen der Interoperabilität verzichtet werden.

Die DNs aller Zertifikatnehmer unterhalb der DFN-PCA enthalten das Attribut `C=DE`. Vor der

Zertifizierung wird die Korrektheit und Eindeutigkeit des angegebenen Namens von der CA überprüft; es darf kein Name mehrfach vergeben geben.

Der Name jedes Zertifikatnehmers soll folgendem Schema folgen:

```
C=DE,
O=<Organisation>,
[OU=<Abteilung>,]
[CN=<Eindeutiger Name>,]
[EMAIL=<Email-Adresse>]
```

Abweichungen von diesem Schema sind nur nach vorheriger Absprache mit der DFN-PCA möglich.

Alternative Namen können bei Bedarf über Zertifikat-Erweiterungen im Zertifikat aufgenommen werden. Die zertifizierende CA hat in diesem Fall vor der Zertifizierung den Inhalt dieser Erweiterungen auf Korrektheit zu überprüfen.

8.1 Wahl eines Namens für CAs

Jede von der DFN-PCA unmittelbar zertifizierte CA wählt ihren eigenen Namen. Dieser sollte die Zugehörigkeit zu einer Organisation direkt widerspiegeln.

Der Organisationsname (“`O=`”) enthält den Namen der Einrichtung, welche durch die CA repräsentiert wird. Es können ein oder mehrere Organisationsbereiche (Abteilungen, “`OU=`”) angegeben werden; optional können weitere Attribute (z.B. “`L=`”) in den Namen aufgenommen werden.

Es sollte eine gültige Email-Adresse der CA angegeben werden; das Attribut “`CN=`” ist für CAs optional, sollte jedoch aus Interoperabilitätsgründen verwendet werden.

Jede CA ist verantwortlich für die korrekte Namenswahl der von ihr zertifizierten CAs und Endteilnehmer.

8.2 Wahl eines Namens für RAs und Endteilnehmer

Die Wahl von eindeutigen Endteilnehmer-Namen wird in erster Linie durch die Richtlinien der zertifizierenden CA bestimmt. RAs unterliegen denselben Regeln für die Namensgebung wie Benutzer.

Das Attribut “`CN=`” ist für alle Endteilnehmer obligatorisch und kommt genau einmal vor. Es enthält den vollständigen Namen des Benutzers.

Es wird empfohlen, über das Attribut "`EMAIL=`" eine gültige Emailadresse in den Namen aufzunehmen; optional können weitere Attribute (z.B. "`L=`") in den Namen aufgenommen werden.

Kommt ein Name innerhalb einer Organisation mehrmals vor, ist es die Aufgabe der CA, durch geeignete Namenszusätze eindeutige Namen zu wählen. Die zuständige CA ist ferner dafür verantwortlich, die Zugehörigkeit des Benutzers zu der betreffenden Einrichtung zu überprüfen und sicherzustellen, daß alle zertifizierten Benutzer über unterschiedliche Namen verfügen.

Zusätzliche Regeln für WWW-Server

Zertifikate für WWW-Server müssen im Attribut "`CN=`" einen eindeutigen Hostnamen enthalten. Dieses Attribut darf keine Platzhalter ("Wildcards") und keine numerischen IP-Adressen enthalten.

Das optionale Attribut "`EMAIL=`" sollte eine gültige Emailadresse, beispielsweise die des Server-Administrators, enthalten.

9 Verschiedenes

Dieses Dokument entstand in einem DFN-Projekt an der Universität Hamburg. Es wird keine Haftung für die Korrektheit, Vollständigkeit oder Anwendbarkeit der enthaltenen Informationen und der vorgeschlagenen Maßnahmen übernommen. Ferner kann keine Haftung für eventuelle Schäden, entstanden durch die Inanspruchnahme der Dienste der DFN-PCA, übernommen werden. Die Verantwortung für die Verwendung der oben beschriebenen Verfahren und Programme liegt allein bei den die Installation durchführenden Personen.

Die DFN-PCA behält sich vor, Zertifizierungswünschen nicht nachzukommen. Ferner kann keine Garantie für die Verfügbarkeit der PCA-Dienste übernommen werden. Es besteht derzeit keine Möglichkeit, die Dienste der DFN-PCA auf einer 24-Stunden-Basis anzubieten.

Dokumentation und Datenschutz

Alle Arbeiten im Rahmen dieser Policy werden, soweit technisch durchführbar, dokumentiert. Alle CAs und RAs müssen die bei der Zertifizierung anfallenden Daten vertraulich behandeln und die für sie geltenden Datenschutzrichtlinien einhalten.

Sämtliche Zertifikatnehmer stimmen der Speicherung und Verarbeitung ihrer bei der Zertifizierung anfallenden Daten durch die zertifizierende Instanz zu.

Vereinbarungen zwischen PCA und CA

Ein CA-Administrator, welcher eine Zertifizierung durch die DFN-PCA wünscht, hat handschriftlich eine Vereinbarung mit der DFN-PCA zu unterzeichnen. Diese Vereinbarung enthält in erster Linie eine Erklärung über die Einhaltung der Richtlinien dieser Policy und kann bei der DFN-PCA angefordert werden.

Vereinbarungen zwischen CA und RA

Eine CA kann die Unterzeichnung einer Vereinbarung verlangen, welche die RA an bestimmte Richtlinien bindet. Diese Vereinbarung ist von der als RA tätigen Person handschriftlich zu unterzeichnen; sie kann bei der zuständigen CA angefordert werden.

Erklärung der Teilnehmer

Alle Teilnehmer der DFN-Hierarchie haben vor ihrer Zertifizierung handschriftlich eine Erklärung zu unterzeichnen, in der sie über ihre Rechte und Pflichten sowie über die Risiken und Gefahren beim Einsatz von Public Key-Systemen aufgeklärt wurden. Diese Erklärung, die im Einzelfall auch vom Teilnehmer an die zertifizierende CA gefaxt werden kann, wird von der zertifizierenden Instanz verwahrt und beinhaltet in erster Linie die Zustimmung zu den Richtlinien dieser Policy sowie gegebenenfalls eine Erklärung darüber, von welcher Partei das zu zertifizierende asymmetrische Schlüsselpaar erzeugt wurde.

Gebühren

Die DFN-PCA behält sich vor, für bestimmte Leistungen Gebühren zu erheben. Jede zertifizierte CA hat ihrerseits die Möglichkeit, für bestimmte Leistungen Gebühren zu erheben.

Literaturverzeichnis

DFN-PCA: DFN-PCA: Low-Level Policy, Version 1.4, 28. Dezember 2001

RFC 1422: S. Kent: Privacy Enhancement for Internet Electronic Mail: Part II: Certificate-Based Key Management, Februar 1993

X.509: ITU-T Recommendation X.509 (1997 E): Information Technology - Open Systems Interconnection - The Directory: Authentication Framework, Juni 1997

PKIX: Public Key Infrastructure (X.509), Arbeitsgruppe der *Internet Engineering Task Force* (IETF), 1999

Abkürzungsverzeichnis

CA: Certification Authority (Zertifizierungsinstanz)

CPS Certification Practice Statement

CRL: Certificate Revocation List (Widerrufsliste)

CSR: Certificate Signing Request (Zertifizierungswunsch)

DFN: Verein zur Förderung eines Deutschen Forschungsnetzes e.V.

DN: Distinguished Name (X.500-Name)

FTP: File Transfer Protocol

ID: Identifier

ITU: International Telecommunication Union

LDAP: Lightweight Directory Access Protocol

PCA: Policy Certification Authority (Wurzelinstanz)

PIN: Personal Identification Number

RA: Registration Authority (Registrierungsinstanz)

RFC: Request for Comment

RSA: Rivest, Shamir, Adleman (Entwickler des RSA-Algorithmus)

S/MIME: Secure/Multipurpose Internet Mail Extensions

SSL: Secure Sockets Layer

WiN: Wissenschaftsnetz