DFN – PCA
Medium – Level Policy

Zertifizierungsrichtlinien für die DFN-PCA
Stand: 28. Dezember 2001
Version: 1.4

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

Inhaltsverzeichnis

DFN – PCA: Medium-Level Policy

Vorbemerkung zu dieser Version

Dies ist die Version 1.4 der Policies der DFN-PCA. Diese Version ist gültig bis zum 31. Dezember 2003 oder bis eine neue Version dieser Policy veröffentlicht wird (je nachdem, welches dieser Ereignisse zuerst eintritt) und unterscheidet sich inhaltlich von der Vorgängerversion 1.3, die bis zum 31. Dezember 2001 gültig war, lediglich in der geänderten Gültigkeitsdauer.

1 Einleitung

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

Der Sinn dieses Dokumentes ist es, Benutzern im Netzwerk eine Einschätzung der durch diese Medium-Level-PCA ausgestellten Zertifikate zu ermöglichen sowie Hinweise und Informationen für den Betrieb einer eigenen Zertifizierungsinstanz (CA) – zertifiziert durch die DFN-PCA – zu geben. Die Policy der ebenfalls betriebenen Low-Level-PCA ist in einem separaten Dokument enthalten.

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 Medium-Level-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)

Allgemeine Informationsdienste der DFN-PCA

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

Auf diesen Informationsdiensten erhalten Sie die Wurzelzertifikate der DFN-PCA, die Schlüssel zur vertraulichen Kommunikation mit den PCA-Mitarbeitern, sowie sämtliche weiteren Informationen zur DFN-PCA.

Gültigkeit dieses Dokumentes

1. Januar 2002 bis 31. Dezember 2003 oder bis eine neue Version dieser Policy veröffentlicht wird (je nachdem, welches dieser Ereignisse zuerst eintritt)

Version dieses Dokumentes

1.4

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 können auf Anfrage zertifiziert werden. Das vorrangige Ziel der DFN-PCA besteht in dem Aufbau einer DFN-weiten Public Key-Zertifizierungs-Infrastruktur mit CAs in den einzelnen Mitgliedseinrichtungen, welche von der DFN-PCA zertifiziert werden. Die lokalen CAs operieren ihrerseits im Namen der jeweiligen Einrichtung, beispielsweise einer Hochschule oder eines Forschungsinstitutes. Eine solche Infrastruktur ist die Voraussetzung für die vertrauenswürdige Kommunikation im Wissenschaftsnetz (WiN), unterstützt durch Sicherheitsdienste wie Integrität, Authentizität und Vertraulichkeit.

Ferner wird für die Zwecke der internationalen Kommunikation eine Anbindung der DFN-Zertifizierungshierarchie an andere Infrastrukturen nach Maßgabe der Möglichkeiten bereitgestellt.

Die DFN-PCA wird ausschließlich Zertifikate für Zertifizierungsinstanzen, nicht aber für Benutzer erteilen.

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 Mitarbeitern nach bestem Wissen und Gewissen durchgeführt.

3.2 Die DFN-Zertifizierungshierarchie

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

- Zertifizierungsinstanzen (CAs)
- Registrierungsinstanzen (RAs) (s. 3.3)
- Benutzern

Die internationale Anbindung der kompletten DFN-Zertifizierungshierarchie an andere Hierarchien kann durch eine gegenseitige Zertifizierung (Cross-Zertifizierung) der DFN-PCA mit anderen PCAs erfolgen. Die Eingliederung der DFN-Hierarchie in eine Internet-weite Infrastruktur kann erfolgen, sobald eine entsprechende Instanz (genannt IPRA: Internet PCA Registration Authority) verfügbar ist. In jedem Fall werden die Teilnehmer der DFN-Hierarchie über internationale Anbindungen und Cross-Zertifizierungen informiert.

Das Ziel der DFN-Zertifizierungshierarchie ist es, pro wissenschaftlicher Einrichtung eine CA zu betreiben, welche direkt von der DFN-PCA zertifiziert wird. Diese CAs haben die Möglichkeit, ihrerseits Zertifikate für Benutzer und untergeordnete Sub-CAs zu erteilen; das genaue Konzept zum Aufbau und Betrieb solcher CAs ist in RFC 1422 (s. Literaturverzeichnis) erläutert.

Unterhalb der DFN-PCA operierende CAs haben weiterhin die Möglichkeit – durch den Vorgang der 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 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 werden von keiner Zertifizierungsinstanz innerhalb der Medium-Level DFN-Hierarchie erteilt.

3.3 Registrierungsinstanzen (RA)

Innerhalb großer Organisationen kann es vorkommen, daß die zuständige CA weit entfernt von den zu zertifizierenden Benutzern lokalisiert ist. In diesem Fall besteht die Möglichkeit, vertrauenswürdige Registrierungsinstanzen (RAs) für die lokale Überprüfung von Identität und Authentizität der einzelnen Benutzer einzusetzen. Durch den Einsatz solcher RAs läßt sich die Zahl organisations-eigener CAs überschaubar halten. RAs dürfen lediglich zur Registrierung und Überprüfung von Benutzern, nicht jedoch von CAs, eingesetzt werden.

Bei einer Registrierungsinstanz handelt es sich um einen in der üblichen Weise durch eine CA zertifizierten Teilnehmer, der im Auftrag seiner CA die Überprüfung anderer Benutzer vor deren Zertifizierung durch die CA übernimmt. Dabei ist für diesen Teilnehmer kein separates RA-Schlüsselpaar notwendig. Benutzer, die zertifiziert werden möchten, übermitteln ihr selbst-signiertes Zertifikat an die entsprechende RA, welche sich anschließend noch von der Identität des Benutzers – beispielsweise durch Vorlage eines Personalausweises – überzeugen muß, um unzulässige Zertifizierungswünsche auszuschließen.

Eine RA darf weder das asymmetrische Schlüsselpaar für Benutzer erzeugen, noch kann sie Benutzer-Zertifikate erteilen oder widerrufen. Die RA leitet, nachdem die Identität des Benutzers in geeigneter Weise überprüft wurde, das selbst-signierte Zertifikat eines Benutzers elektronisch an die CA weiter. 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 Benutzer selbst vorgenommen wird, leitet die RA nur die Identitätsinformationen des Benutzers digital signiert an die CA weiter. Empfängt eine CA den Zertifizierungswunsch eines Benutzers durch eine vertrauenswürdige RA, hat sie zunächst die Gültigkeit der RA-Signatur zu verifizieren. Darüber hinaus ist ein persönlicher Kontakt (z.B. durch telefonischen Rückruf) zwischen CA und RA notwendig, um unzulässige Zertifizierungswünsche auszuschließen. Nach diesem Kontakt wird das von der CA neu ausgestellte Zertifikat sowohl an die RA als auch an den Benutzer übermittelt.

Jede CA kann beliebig viele Benutzer zu Registrierungsinstanzen ernennen. Ein Benutzer, welcher als RA fungiert, muß mit der zertifizierenden CA eine Vereinbarung unterzeichnen, welche ihn an bestimmte Prozeduren, festgelegt durch die CA, bindet. Jede CA veröffentlicht diese Prozeduren, zusammen mit einer mindestens halbjährlich erneuerten Liste aller von ihr benannten RAs.

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 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 Passworte bzw. PINs geschützt, welche nur den PCA-Mitarbeitern bekannt sind und niemals im Klartext abgelegt werden. Die Peripherie darf nicht auf anderen Rechnern eingesetzt werden.
- Mit geheimen Signatur-Schlüsseln der PCA dürfen ausschließlich CA-Schlüssel bzw. Widerrufslisten (CRLs) unterschrieben oder Cross-Zertifikate erstellt werden. Für jegliche Standard-Kommunikation dürfen geheime Signatur-Schlüssel nicht verwendet werden;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 Bits.
- 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.

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

4.2 Sicherheitsanforderungen an CAs

Folgende Anforderungen werden an die von der DFN-PCA zertifizierten CAs gestellt:

- Für die Dienste der CA muß ein dedizierter Rechner eingesetzt werden, der über keinerlei Verbindung zu einem Rechnernetz verfügt. Der unbefugte Zugriff auf den CA-Rechner ist durch den Einsatz geeigneter Hard- und Software zu unterbinden.

- Jeglicher Datenaustausch mit vernetzten Rechnern muß von Mitarbeitern der CA mittels eines elektronischen Datenträgers vorgenommen werden; es findet keine automatisierte Bearbeitung der Daten statt.

- Jede CA muß unterschiedliche asymmetrische Schlüsselpaare zum Signieren und Entschlüsseln verwenden.

- 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 Schlüssel einzusetzen, soweit dies technisch möglich ist. Der Zugriff auf diese geheimen CA-Schlüssel ist in jedem Fall durch Passworte bzw. PINs zu schützen, welche nur den CA-Administratoren bekannt sein und niemals im Klartext abgelegt werden dürfen. Die Peripherie darf nicht auf anderen Rechnern eingesetzt werden.

- Mit dem geheimen Signatur-Schlüssel der CA dürfen ausschließlich CA- oder Benutzer-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 Bits aufweisen; es werden jedoch deutlich größere Schlüssellängen empfohlen.

- In solchen Fällen, in denen eine CA asymmetrische Schlüsselpaare für die Benutzer erzeugt, muß sichergestellt werden, daß nach der Zertifizierung und Schlüsselübergabe an den Benutzer alle Kopien des geheimen Schlüssels des Benutzers auf Seiten der CA endgültig gelöscht werden. 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.

4.3 Sicherheitsanforderungen an RAs

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

- Eine RA muß auf einem in geeigneter Weise abgesicherten Rechner betrieben werden. Insbesondere muß die Möglichkeit bestehen, den Zugriff von externen Rechnern auf den RA-Rechner zu kontrollieren und zu beschränken. Kritisch für den Betrieb einer RA sind dabei u.a. die im Internet gebräuchlichen Kommunikations-Protokolle bzw. Programme:

  - `rlogin / rsh`
  - `Network File System (NFS)`
  - `Network Information Service (NIS/NIS+)`
  - alle Dienste, deren Authentisierung auf IP-Adressen bzw. Hostnamen beruht
  - sowie ähnliche Protokolle (evtl. vorgegeben durch die CA).

  Wird die RA auf einem PC betrieben, sind ausreichende Sicherheitsmaßnahmen zu ergreifen, die den unbefugten Zugriff auf den PC 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 der RA durch Passworte bzw. PINs zu schützen. Weder die optionale Peripherie noch Passwort bzw. PIN dürfen an andere Benutzer oder CA-Administratoren weitergegeben werden.

- Asymmetrische Schlüsselpaare der RA zur Erzeugung von Signaturen müssen eine Mindestlänge von 1024 Bits aufweisen; es werden jedoch deutlich größere Schlüssellängen empfohlen.

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

4.4 Sicherheitsanforderungen an Benutzer

Benutzer im Sinne dieser Policy sind einzelne Personen. Folgende Anforderungen werden an die von einer CA zertifizierten Benutzer gestellt:

- Der geheime Schlüssel des Benutzers muß ausreichend vor Mißbrauch durch Unbefugte geschützt und darf nicht weitergegeben werden; hierfür ist jeder Benutzer selbst verantwortlich. Werden keine SmartCards zum Speichern des geheimen Schlüssels eingesetzt, ist der Zugriff auf den geheimen Schlüssel des Benutzers durch ein Passwort bzw. eine PIN zu schützen. Weder die optionale SmartCard noch das Passwort bzw. die PIN dürfen an andere Benutzer oder CA-Administratoren weitergegeben werden.
- Das asymmetrische Schlüsselpaar des Benutzers muß eine minimale Länge von 1024 Bits aufweisen.

5 Zertifizierungsregeln

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

Sowohl Zertifizierungsinstanzen als auch Benutzer werden innerhalb einer X.509-Hierarchie mit eindeutigen Namen – sog. Distinguished Names (DNs) – bezeichnet, deren korrekte 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 (Benutzer bzw. CA-Administrator) zu überzeugen, welcher eine Zertifizierung wünscht. Dieser Vorgang muß in jedem Fall durch persönlichen Kontakt vor der Zertifizierung erfolgen. Setzt eine CA Registrierungsinstanzen ein, liegt die Verantwortung der Identitätsprüfung bei der RA, kann aber auch von der CA übernommen werden. In keinem Fall dürfen jedoch Zertifizierungswünsche automatisiert bearbeitet werden.

Das selbst-signierte Zertifikat eines Zertifikatnehmers im Sinne dieser Policy muß mindestens den DN des Teilnehmers sowie dessen Public Key enthalten. Wahlweise kann dieses Zertifikat auch eine Gültigkeitsdauer enthalten, die jedoch endgültig von der zertifizierenden Instanz festgelegt wird.

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.

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

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 die Sicherheitsanforderungen nach Abschnitt 4.2 eingehalten werden. Berechtigt zu der Unterzeichnung dieser Vereinbarung ist eine für den Betrieb der CA verantwortliche Person.

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 sowie ein selbst-signiertes Zertifikat und übermittelt dieses an die DFN-PCA. Dies 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 sowie die Zugehörigkeit des CA-Administrators zu der jeweiligen Einrichtung. 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.

Zertifikate für CAs haben eine Gültigkeitsdauer von maximal 3 Jahren.

Die Einrichtung organisationsweiter Sub-Hierarchien obliegt der Verantwortung der obersten CA einer jeweiligen Organisation. Ziel ist es, eine CA je Organisation (gemäß Abschnitt 3.2) durch die DFN-PCA zertifizieren zu lassen; jede dieser CAs sollte dabei eine eigene Policy - die auf der Medium-Level Policy der DFN-PCA basiert - definieren und öffentlich verfügbar machen.

5.2 Regeln für die Zertifizierung von RAs

Jede Organisation mit eigener CA kann Benutzer bestimmen, die im Auftrag der CA als Registrierungsinstanz (RA) fungieren. RAs, die von einer CA zertifiziert werden möchten, unterzeichnen vor der Zertifizierung eine Vereinbarung mit der CA. Diese Vereinbarung enthält eine Erklärung darüber, daß die Richtlinien dieser Policy akzeptiert werden und deren Einhaltung beim Betrieb der RA zugestimmt wird. Insbesondere müssen die Sicherheitsanforderungen nach Abschnitt 4.3 eingehalten werden. Weitere Anforderungen können von der verantwortlichen CA gestellt werden. Die CA muß ferner sicherstellen, daß der Benutzer die technischen Voraussetzungen zum sicheren Betrieb einer RA erfüllt.

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

5.3 Regeln für die Zertifizierung von Benutzern

Ein Benutzer, welcher zertifiziert werden möchte, generiert zunächst sein persönliches asymmetrisches Schlüsselpaar und übermittelt anschließend ein selbst-signiertes Zertifikat per Email oder mittels eines Datenträgers an die zuständige RA bzw. CA. Gegebenenfalls wird das asymmetrische Schlüsselpaar des Benutzers auch von der CA erzeugt; wobei von der CA die in Abschnitt 4.2 beschriebenen Sicherheitsanforderungen einzuhalten sind.

Unabhängig vom Einsatz einer RA hat sich der Benutzer persönlich vorzustellen, um der CA (bzw. RA) die Verifikation der Identität 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 das vom Benutzer vorgelegte selbstunterschriebene Zertifikat in einer durch die RA signierten Nachricht an die zuständige CA weiter.

Zertifikate für Benutzer haben eine Gültigkeitsdauer von maximal einem Jahr.

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 Zertifizierungsinstanzen. Die Cross-Zertifizierung bietet einen Mechanismus, einen direkten Vertrauenspfad zwischen zwei Instanzen herzustellen, welcher von der strikten Zertifizierungshierarchie abweicht und so eine größere Flexibilität bietet. Dadurch wird auch den Teilnehmern zweier Hierarchien die sichere Kommunikation untereinander ermöglicht. 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 geändert, ist eine erneute Cross-Zertifizierung erforderlich.

Es sei darauf hingewiesen, daß der Prozeß der Cross-Zertifizierung nicht notwendigerweise die gegenseitige Zertifizierung zweier Instanzen bedeuten muß. Denkbar ist eine Zertifizierung in lediglich eine Richtung beispielsweise dann, wenn eine universitäre CA ihren Benutzern die

Zertifikate einer kommerziellen CA verfügbar machen möchte, diese CA jedoch aus Policy-Gründen kein Zertifikat für die universitäre CA erteilen kann.

Die Cross-Zertifizierung einer CA unterscheidet sich grundsätzlich nicht von der Zertifizierung eines Benutzers. Der Public Key einer CA wird in einem selbst-signierten Zertifikat 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 sowie eine Kopie der Policy der anderen CA, signiert mit dem Secret Key eines CA-Administrators. Es steht den Administratoren einer CA frei, auch die von der cross-zertifizierten CA erteilten Zertifikate den eigenen Benutzern zur Verfügung zu stellen. Jede CA sollte jedoch ihren Benutzern zumindest Hinweise auf die Informationsdienste der anderen CAs bereitstellen.

Ein Cross-Zertifikat sollte keine längere Gültigkeitsdauer als das reguläre Zertifikat der cross-zertifizierten CA besitzen.

6 Management von Zertifikaten

Jede zertifizierende Instanz der DFN-Hierarchie ist für die Bereitstellung der Zertifikate zuständig. Die Zertifikate einer CA werden dabei zunächst in einer lokalen Datenbank gespeichert und gepflegt.

Alle Zertifikate der DFN-Hierarchie sollen über ein DFN-weites X.500-Verzeichnis veröffentlicht werden. Die DFN-PCA wird hierfür die von ihr erteilten Zertifikate an einen entsprechenden X.500-Server zur Verteilung weiterleiten. Auch alle untergeordneten CAs sind aufgefordert, Zertifikate direkt im X.500-Verzeichnis zur Verfügung zu stellen.

Nur in solchen Fällen, in denen eine CA keine Möglichkeit hat, Zertifikate im X.500-Verzeichnis abzulegen, kann sie auf Anfrage die von ihr ausgestellten Zertifikate per Email an die DFN-PCA senden, welche die entsprechenden X.500-Einträge vornehmen wird. Zu diesem Zweck wird von der DFN-PCA eine entsprechende Email-Adresse eingerichtet.

Als alternative, zusätzliche Verteilungsformen zu X.500 werden von der DFN-PCA diverse Informationsdienste eingerichtet, deren Aufgabe die Verteilung von Zertifikaten und CRLs (s. Abschnitt 7) ist. Zu diesen Diensten gehören vorrangig ein Email-basierter Server, FTP- und WWW-Server sowie bei Bedarf die Einrichtung von Mailinglisten oder UNIX-basierten “finger”-Servern. Diese Dienste können auch von den einzelnen CAs angeboten werden, um ihren Benutzern das Auffinden von Zertifikaten zu erleichtern.

Zertifikate der DFN-Hierarchie können dann entweder durch direkten Zugriff auf das DFN-weite

X.500-Verzeichnis oder durch Verwendung der Informationsdienste der DFN-PCA abgefragt werden.

Details zu den von der DFN-PCA zur Verteilung von Zertifikaten und CRLs angebotenen Informationsdiensten werden, der höheren Flexibilität wegen, in einem separaten Dokument und in den Anhängen zu dieser Policy veröffentlicht. Diese Hinweise finden sich außerdem auf dem WWW-Server der DFN-PCA (URL s. Abschnitt 2).

Alle Teilnehmer der DFN-Zertifizierungshierarchie erklären sich grundsätzlich mit der Veröffentlichung ihres Zertifikates einverstanden. Es besteht jedoch die Möglichkeit, bei der Beantragung eines Zertifikates gegen eine Veröffentlichung Widerspruch einzulegen.

7 Widerruf von Zertifikaten

Die PCA behält sich vor, von ihr erteilte Zertifikate jederzeit vor Ablauf der Gültigkeitsdauer ohne Angabe expliziter Gründe zu 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.

Jede CA kann von ihr erteilte Zertifikate für CAs oder Benutzer jederzeit vor Ablauf der Gültigkeitsdauer widerrufen.

Jeder Teilnehmer der DFN-Hierarchie kann von der Instanz, die seinen Schlüssel zertifiziert hat, ohne Angabe von Gründen verlangen, daß diese das entsprechende Zertifikat widerruft. Die betreffende CA (gegebenenfalls auch eine für die CA tätige RA) hat diesem Verlangen nachzukommen, sobald sie sich durch geeignete Schritte davon überzeugt hat, daß der Antrag vom Zertifikatnehmer selbst stammt bzw. von ihm autorisiert ist. Wird der Mißbrauch des eigenen geheimen Schlüssels bekannt, hat jeder Teilnehmer unmittelbar die zertifizierende Instanz zu benachrichtigen und den Widerruf des eigenen Zertifikates zu veranlassen.

Zertifikate können nur von der ausstellenden Instanz widerrufen werden. Sämtliche widerrufenen Zertifikate werden von der zuständigen CA auf einer sog. Certificate Revocation List (CRL) veröffentlicht, welche allen Teilnehmern zur Verfügung gestellt werden muß, um widerrufene Zertifikate nicht irrtümlicherweise zu benutzen. Widerrufene Zertifikate bleiben solange auf der CRL, bis die ursprüngliche Gültigkeitsdauer überschritten wurde. Ein rückwirkender Widerruf ist nicht möglich.

Einmal widerrufene Zertifikate können nicht erneuert werden. Jedoch hat jeder Teilnehmer der DFN-Hierarchie die Möglichkeit, ein neues Zertifikat zu beantragen.

Jede Zertifizierungsinstanz innerhalb der DFN-Hierarchie muß unmittelbar nach ihrer Zertifizierung durch eine übergeordnete Instanz und danach mindestens einmal monatlich eine neue CRL herausgeben, auch wenn keine weiteren Zertifikate widerrufen wurden. Die Herausgabe der CRL hat an einem bestimmten, vorher festgelegten Tag eines jeden Monats zu erfolgen, welches auch dann eingehalten werden muß, wenn zwischenzeitlich zusätzliche CRLs herausgegeben wurden. Diese Regelung gilt auch für die DFN-PCA.

Alle CRLs der DFN-Zertifizierungshierarchie sollen über ein DFN-weites X.500-Verzeichnis veröffentlicht werden. Die DFN-PCA wird hierfür ihre CRLs an einen entsprechenden X.500-Server zur Verteilung weiterleiten. Auch alle untergeordneten CAs sind aufgefordert, CRLs im X.500-Verzeichnis zur Verfügung zu stellen.

Nur in solchen Fällen, in denen eine CA keine Möglichkeit hat, CRLs im X.500-Verzeichnis abzulegen, kann sie auf Anfrage die von ihr ausgestellten CRLs per Email an die DFN-PCA senden, welche die entsprechenden X.500-Einträge vornehmen wird. Zu diesem Zweck wird von der DFN-PCA eine entsprechende Email-Adresse eingerichtet.

Als alternative Verteilungsformen zu X.500 werden von der DFN-PCA diverse Informationsdienste eingerichtet, deren Aufgabe die Verteilung von Zertifikaten (s. Abschnitt 6) und CRLs ist. Zu diesen Diensten gehören vorrangig ein Email-basierter Server, FTP- und WWW-Server sowie bei Bedarf die Einrichtung von Mailinglisten oder UNIX-basierten “finger”-Servern.

Jeder zertifizierenden Instanz steht es frei, CRLs cross-zertifizierter Instanzen zu veröffentlichen.

8 Regeln für die Namensgebung

Allen Zertifikatnehmern der DFN-Zertifizierungshierarchie wird ein eindeutiger Distinguished Name (DN) nach X.500 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. Die korrekte Wahl von DNs ermöglicht daher die effiziente Speicherung und Suche von Zertifikaten innerhalb eines X.500-Verzeichnisses.

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

8.1 Wahl eines Namens für CAs

Jede von der DFN-PCA unmittelbar zertifizierte CA wählt ihren eigenen DN. Dieser sollte die Zugehörigkeit zu einer Organisation direkt widerspiegeln. Vor der Zertifizierung wird die Korrektheit des DNs von der DFN-PCA in Abstimmung mit dem DFN-X.500 Verzeichnis überprüft; es wird kein DN mehrfach vergeben.

Der DN jeder CA soll folgendem Schema folgen:

```
C=DE, [L=DFN,] O=<Organisation> [,OU=<Abteilung>]
```

Der Organisationsname enthält den Namen der Einrichtung, welche durch die CA repräsentiert wird; optional können eine oder mehrere Organisationsbereiche (Abteilungen) angegeben werden. Dies ist insbesondere für große Organisationen sinnvoll, in denen mehrere CAs betrieben werden sollen.

Jede CA ist verantwortlich für die korrekte Namenswahl der durch sie zertifizierten CAs und Benutzer. Bei der Vergabe von Zertifikaten gilt die in RFC 1422 definierte Regel der Namensunterordnung, wonach die DNs sämtlicher Zertifikatnehmer alle DN-Attribute ihrer zertifizierenden Instanz beinhalten müssen.

8.2 Wahl eines Namens für RAs und Benutzer

Da Registrierungsinstanzen innerhalb der Zertifizierungshierarchie den gleichen Status besitzen wie Benutzer, unterscheidet sich auch die Wahl der zugehörigen DNs nicht.

Die Wahl von Benutzer-DNs wird in erster Linie durch die Richtlinien der Organisations-CAs bestimmt, es gilt jedoch auch für Benutzer die Regel der Namensunterordnung. Alle DN-Attribute der zertifizierenden Instanz müssen Teil des Benutzer-DNs sein, so daß aus dem DN eines Benutzers auf dessen zertifizierende Instanz geschlossen werden kann.

Der DN eines Benutzers soll folgendem Schema folgen:

```
C=DE, [L=DFN,] O=<Organisation>, [OU=<Abteilung>,] CN=<Vorname Name>
```

Das Attribut “CN” kommt pro Benutzer genau einmal vor und enthält üblicherweise den vollständigen Namen des Benutzers. Kommt ein Name innerhalb einer Organisation mehrmals vor, ist es die Aufgabe der CA, durch geeignete Namenszusätze eindeutige DNs 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 DNs verfügen.

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 Administratoren und Benutzern.

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 Zertifizierungs- und Registrierungsinstanzen 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

Ein Benutzer, welcher für eine CA als RA fungieren will, hat handschriftlich eine Vereinbarung mit der CA zu unterzeichnen, in welcher die Einhaltung dieser Policy sowie eventuell weiterer, durch die CA festgelegte Richtlinien, erklärt wird. Diese Vereinbarung 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 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.

Eingesetzte Software

Die eingesetzten Implementationen sind im Rahmen der technischen und organisatorischen Möglichkeiten auf Sicherheitsmechanismen und Funktionalität zu überprüfen.

Die von der DFN-PCA in erster Linie eingesetzten Softwarepakete zum Betrieb einer Zertifizierungsinfrastruktur sollen auf entsprechenden Informations-Servern zum Abruf bereitgestellt werden, sofern es sich um frei verfügbare Implementationen handelt.

Bestimmte kryptographische Algorithmen unterliegen in einigen Ländern export- oder lizenzrechtlichen Bestimmungen, die bei der Verwendung zu beachten sind.

Neue Protokolle bzw. Standards (z.B. S/MIME, SSL, S-HTTP, X.509v3) zur sicheren Kommunikation sowie weitere Algorithmen und Neuerungen im Bereich der Kryptographie (z.B. DSA, SHA-1) sollen durch die DFN-PCA untersucht und unterstützt werden, sobald entsprechende Applikationen zur Verfügung stehen.

Anwendungsabhängige Richtlinien, die Besonderheiten im Umgang mit bestimmten Protokollen bzw. Implementationen beschreiben, werden bei Bedarf in separaten Dokumenten als Anhänge zu dieser Policy veröffentlicht.

Literaturverzeichnis

IN-CH: Individual Network e.V.: Certification Policy, 10. März 1997

RFC 1421: J. Linn: Privacy Enhancement for Internet Electronic Mail: Part I: Message Encryption and Authentication Procedures, Februar 1993

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

RFC 1423: D. Balenson: Privacy Enhancement for Internet Electronic Mail: Part III: Algorithms, Modes, and Identifiers, Februar 1993

RFC 1424: B. Kaliski: Privacy Enhancement for Internet Electronic Mail: Part IV: Key Certification and Related Services, Februar 1993

RFC 1875: N. Berge: UNINETT PCA Policy Statements, Dezember 1995

X.509: ITU-T: Recommendation X.509: The Directory – Authentication Framework, 1988