Mobile Pools – Policy

(Letzte Änderung dieser Policy: 25. April 2004)

Vorbemerkung zu dieser Version

Dies ist die Version 2.0 der Policy des Projekts Mobile Pools der Fakultät für Angewandte Wissenschaften der Universität Freiburg. Diese Version ist gültig bis zum 30. Oktober 2004 und beruht auf der Low-Level-Policy der DFN-PCA, Version 1.6. Sie soll den Anforderungen der Low-Level DFN-Policy an eine CA gerecht werden.

1 Einleitung

Dieses Dokument enthält die Zertifizierungsrichtlinien (die sog. *Policy*) der Zertifizierungsstelle des Projekts Mobile Pools der Fakultät für Angewandte Wissenschaften der Universität Freiburg – nachfolgend MoPo-CA genannt. Dabei handelt es sich um Zertifizierung mit niedrigen Sicherheitsanforderungen an die Zertifizierungsstelle, bei der Ausstellung der Zertifikate und an die Zertifikatnehmer.

Der Sinn dieses Dokuments ist es, Benutzern die Einschätzung der durch die MoPo-CA ausgestellten Zertifikate zu ermöglichen.

Die in diesem Dokument getroffenen Aussagen sind für die Arbeit der MoPo-CA bindend. (Dies gilt nicht für diejenigen Teile, die gesetzlichen Vorschriften widersprechen. Derartige Widersprüche sind nicht beabsichtigt; sollten sie aber dennoch auftreten, so verlieren dadurch die übrigen Vorgaben dieser Policy nicht ihre Gültigkeit.) Die MoPo-CA zertifiziert ausschließlich nach den Richtlinien dieser Policy.

2 Identität der MoPo-CA

Adresse
MoPo Projekt
Fakultät für Angewandte Wissenschaften, Universität Freiburg
Gebäude 051, Zimmer 02-031
Georges-Köhler-Allee
D-79110 Freiburg
Telefon: (+49) 0761 203 8187

E-Mail-Adresse
`mopomgr@informatik.uni-freiburg.de`

Allgemeine Informationsdienste der MoPo-CA
WWW-Server: `http://mopoinfo.informatik.uni-freiburg.de/`
Auf diesen Servern finden Sie die Wurzelzertifikate der MoPo-CA sowie weitere Informationen zur MoPo-CA und zum Projekt Mobile Pools.

Gültigkeit dieses Dokuments
1. April 2004 bis 30. Oktober 2004

3 Zuständigkeitsbereich der MoPo-CA

Der Zuständigkeitsbereich der MoPo-CA umfaßt die Einrichtungen des Projekts Mobile Pools und desen Mitarbeiter sowie desen Projektteilnehmer. Das Ziel der MoPo-CA besteht darin, den Projektteilnehmern des Projekts Mobile Pools einen Rahmen zur Verfügung zu stellen, der es ihnen erlaubt, sich im Funknetz des Projekts Mobile Pools auszuweisen und eine sichere Verbindung zum universitären Computernetzwerk aufzubauen.

Die MoPo-CA wird nur Zertifikate für Teilnehmer des Projekts Mobile Pools und Server des Projekts Mobile Pools ausstellen, keine CA-Zertifikate.

3.1 Die MoPo-Zertifizierungshierarchie

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

3.2 Rechtliche Bedeutung

Eine Zertifizierung durch die MoPo-CA ist keine Zertifizierung *im Sinne des Signaturgesetzes* [SigG]. Die MoPo-CA erhebt nicht den Anspruch, eine Zertifizierungsstelle *im Sinne von §2 Abs. 2 des Signaturgesetzes* zu sein.

Ein *Anspruch* auf die Erteilung eines Zertifikats durch die MoPo-CA besteht nicht.

Insbesondere die Fakultät für Angewandte Wissenschaften der Universität Freiburg, das Projekt Mobile Pools sowie die Mitarbeiter des Projekts Mobile Pools übernehmen keine Form der Gewährleistung. Alle Aufgaben werden von den Mitarbeitern des Projekts Mobile Pools nach besten Wissen und Gewissen durchgeführt.

4 Sicherheitsanforderungen

Durch die Teilnahme an einer Public-Key-Infrastruktur entstehen für alle Beteiligten bestimme Anforderungen hinsichtlich der Sicherheit der eingesetzten Hard- und Software einerseits sowie des verantwortungsvollen Umgangs mit kryptographischen Schlüsseln andererseits. Die Anforderungen an die MoPo-CA sind dabei höher als die an Nutzer gestellten, da der Mißbrauch eines CA-Schlüssels allen untergeordneten Zertifikaten die Vertrauenswürdigkeit entziehen würde und insofern viel gravierendere Auswirkungen hätte.

4.1 Sicherheitsanforderungen an die MoPo-CA

Die MoPo-CA arbeitet nach folgenden Maßgaben:

- Für die Dienste der MoPo-CA wird ein Rechner eingesetzt, der in geeigneter Weise vor mißbräuchlicher Benutzung geschützt ist. Der unbefugte Zugriff auf den CA-Rechner und eventuell gespeicherte Schlüsseldaten wird durch den Einsatz geeigneter Hard- und Software unterbunden (Zugangs-/Zugriffskontrolle).

- Geheime Schlüssel der MoPo-CA zum Erzeugen digitaler Signaturen müssen vor Mißbrauch geschützt werden und dürfen nicht wiedergegeben werden.
- Es werden mit dem geheimen Signatur-Schlüssel der MoPo-CA ausschließlich Benutzer-Schlüssel, Zertifikatwiderrufe oder die Policy der MoPo-CA unterschrieben. Der geheime Signatur-Schlüssel wird nicht für Kommunikationszwecke verwendet.
- Asymmetrische Schlüsselpaare der MoPo-CA zur Erzeugung von Signaturen weisen eine Mindestlänge von 1024 Bits auf.
- Sämtliche persönlichen Daten der Zertifikatnehmer, die den MoPo-CA-Mitarbeitern bei der Zertifizierung über die Schlüssel- und Zertifikatdaten hinaus bekannt werden (z.B. Personalausweisnummer), werden von den MoPo-CA-Mitarbeitern vertraulich behandelt und ausschließlich zu internen Dokumentationszwecken erhoben; sie werden nicht veröffentlicht.
- Von dem Datenbestand der Rechner der MoPo-CA sind regelmäßige Sicherungen anzufertigen. Diese Sicherungskopieen sind genauso wie der Rechner zu schützen.

4.2 Sicherheitsanforderungen an Benutzer

Benutzer im Sinne dieser Policy sind natürliche Personen oder Server des Projekts Mobile Pools, die die Zertifizierungsdienste der MoPo-CA in Anspruch nehmen (Zertifikatnehmer). Folgende Anforderungen werden an die Zertifikatnehmer der MoPo-CA 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. Der Benutzer wird hierauf bei der Zertifizierung ausdrücklich hingewiesen.
- Der zu zertifizierende Schlüssel des Benutzers muß eine Länge von 1024 Bits aufweisen.
- Natürliche Personen müssen die während der gesammten Gültigkeitsdauer, für die sie ein Zertifikat der MoPo-CA beantragen, Mitglieder der Universität Freiburg sein und über einen gültigen Rechneraccount an der Fakultät für Angewandte Wissenschaften verfügen.

5 Zertifizierungsregeln

Die MoPo-CA führt keine Cross-Zertifizierung mit anderen Zertifizierungsstellen durch. Sie zertifiziert keine nachgeordneten CAs und auch keine Registrierungsstellen (RAs), sondern ausschliesslich Nutzer, genauer: deren öffentliche Schlüssel. Die einzige Ausnahme von dieser Regel bilden der Wurzel-Schlüssel der MoPo-CA selbst: Der Wurzel-Schlüssel wird mit einem Selbst-Zertifikat versehen.

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

Anonyme oder pseudonyme Zertifikate werden von der MoPo-CA *nicht* ausgestellt. Ebenso werden keine Zertifikate für Gruppenschlüssel ausgestellt.

5.1 Unterstützte Schlüsselformate

Die MoPo-CA zertifiziert ausschließlich *RSA*-Schlüssel in Form von PEM oder DER kodierten x.509v3 Zertifikat Anfragen [x.509].

5.2 Schlüsselgenerierung

Die Schlüsselgenerierung erfolgt automatisch durch eine entsprechende Software auf den geschützten Rechnern der MoPo-CA.

5.3 Namenswahl

Jedes x.509v3 Zertifikat enthält einen x.500 *distinguished name* (DN), der den Eigentümer (*subject*) des Zertifikats bezeichnet, und einen DN der die Zertifizierungsstelle (*issuer*) bezeichnet. Um eine eindeutige Zuordnung zwischen Benutzer und DN zu gewährleisten, werden folgende Anforderungen an den DN gestellt:

Der DN muß folgende *relative distinguished names* (RDN) enthalten:

```
C=DE, O=MoPo WLAN Uni Freiburg
```

Außerdem müssen der RDN CN (*common name*) vorhanden sein. Der RDN CN enthält den vollständigen Namen des Benutzers, so, wie er in der Benutzerdatenbank der Fakultät für Angewandte Wissenschaften erfaßt ist. Handelt es sich bei dem Benutzer um einen Server des Projekts Mobile Pools, so enthält der RDN CN einen Eintrag der Form `root@hostname.domainname`.

Der DN des Wurzel-Zertifikats der MoPo-CA ist

```
C=DE, O=MoPo WLAN Uni Freiburg, CN=MoPo Root-CA
```

Alle Zertifiakte außer das Wurzel-Zertifikat enthalten die x.509v3 Erweiterung *subjectAlternativeName* mit einem Wert der Form

```
email:account@informatik.uni-freiburg.de
```

bzw. `email:root@hostname.domainname` für Server des Projekts Mobile Pools.

5.4 Identitätsprüfung

Um unerlaubte Zertifizierungswünsche zu erkennen, hat sich die MoPo-CA vor jeder Zertifizierung in geeigneter Weise von der Identität desjenigen Schlüsselinhabers zu überzeugen, welcher eine Zertifizierung wünscht.

Dazu muß der Benutzer sich gegenüber der geschützen Rechner der MoPo-CA durch seinen Account an der Fakultät für angewandte Wissenschaften ausweisen. Dies geschieht durch Angabe des *login* und des *Passworts*.

5.5 Anforderungen an den Schlüssel

Zertifikate werden ausschließlich dann erteilt, wenn der zu zertifizierende Public-Key über die in Abschnitt 4 festgelegte Länge verfügt, die zu zertifizierende Benutzerkennung die Anforderungen in Abschnitt 8 erfüllt und sich die MoPo-CA in geeigneter Weise von der Identität des Antragstellers überzeugt hat.

5.6 Gültigkeitsdauer

Ein x.509v3 Zertifikat enthält grundsätzlich den Public-Key sowie den DN des Benutzers oder der Zertifizierungsstelle, die das Zertifikat ausgestellt hat, und einen Gültigkeitsbereich.

Die Zertifikate der MoPo-CA haben eine Gültigkeitsdauer von maximal einem Semester für Studenten, bzw. bis maximal zum Ende des Accounts an der Fakultät für angewandte Wissenschaften für Mitarbeiter. Der Beginn des Gültigkeitszeitraumes ist der auf die Zertifizierung folgende Tag, das Ende der Tag vor Beginn des nächsten Semesters.

5.7 Verlängerung von Zertifikaten

Zertifikate werden nicht automatisch durch die MoPo-CA erneuert oder verlängert. Eine Re-Zertifizierung erfolgt nicht, es ist stattdessen ein neuer normaler Zertifizierungsantrag (wie bei der erstmaligen Zertifizierung) bei der MoPo-CA zu stellen.

6 Management von Zertifikaten

Die MoPo-CA behält sich das Recht vor, die von ihr ausgestellten Zertifikate in geeigneter Form zu veröffentlichen, wenn sie dies für nötig befindet, um die Arbeit der MoPo-CA im Sinne dieser Policy zu ermöglichen.

Alle Zertifikatnehmer der MoPo-CA erklären sich mit der Veröffentlichung ihres Zertifikats einverstanden. Sie werden auf die Publikation der Daten auf den Zertifizierungsanträgen ausdrücklich hingewiesen. Ohne diese Einwilligung kann keine Zertifizierung erfolgen.

7 Widerruf von Zertifikaten

Die MoPo-CA behält sich vor, von ihr erteilte Zertifikate vor Ablauf der Gültigkeitsdauer ohne öffentliche Nennung expliziter Gründe zu widerrufen. Dem Schlüsselinhaber wird die MoPo-CA auf Anfrage die Gründe mitteilen, die sie dazu veranlaßt haben.

Jeder Zertifikatnehmer der MoPo-CA kann von ihr ohne Angabe von Gründen verlangen, daß sie das entsprechende Zertifikat für seinen Schlüssel widerruft. Die MoPo-CA 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 eigene geheime Schlüssel Dritten bekannt, so hat der betroffene Nutzer unverzüglich die MoPo-CA zu benachrichtigen und den Widerruf des eigenen Zertifikats veranlassen, sobald er Kenntnis von diesem Umstand hat.

Die MoPo-CA wird mindestens einmal monatlich eine *certificate revocation list* (CRL) auf dem WWW Server des Projekts Mobile Pools veröffentlichen, die alle widerrufenen Zertifikate enthält. Diese CRL wird als DER kodierte Datei zur Verfügung gestellt.

8 Verschiedenes

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 MoPo-CA oder die Nutzung eines oder mehrerer von ihr ausgestellter Zertifikate, übernommen werden. Die Verantwortung für die Verwendung der oben beschriebenen Verfahren und Programme liegt allein bei den die Installation durchführenden Administratoren und Benutzern.

Die MoPo-CA behält sich vor, Zertifizierungswünschen nicht nachzukommen. Ferner kann keine Garantie für die Verfügbarkeit des MoPo-CA-Dienste übernommen werden.

Die MoPo-CA fragt *niemals* Nutzer nach ihrer geheimen *Passphrase*, dem Code-Wort oder -satz, mit dem der geheime Nutzerschlüssel (*private key*) vor unbefugtem Zugriff geschützt ist!

Datenschutz

Alle Zertifikatnehmer stimmen mit dem Antrag auf Zertifizierung der Speicherung und Verarbeitung ihrer bei der Zertifizierung anfallenden Daten, die auch maschinell erfolgen wird, durch die zertifizierende Instanz zu.

Erklärung der Teilnehmer

Durch das Beantragen eines Benutzeraccounts an der Fakultät für angewandte Wissenschaften erkennen Teilnehmer gleichzeitig die Richtlinien der MoPo-CA Policy an.

Maßgebliche Fassung dieser Policy

Eventuell werden Übersetzungen dieser Policy in andere Sprachen verfügbar gemacht, um beispielsweise die internationale Zusammenarbeit mit anderen CAs zu ermöglichen und Anwendern von Public-Key-Verfahren weltweit die Möglichkeit zu geben, die Arbeitsweise der MoPo-CA nachzuvollziehen und so die Verläßlichkeit ihrer Zertifikate einschätzen zu können. Maßgeblich ist jedoch in jedem Fall die deutschsprachige Version in ihrer jeweils aktuellsten Fassung.

Gebühren

Für die Leistungen der MoPo-CA werden keine Gebühren erhoben.

„Dienstaufsicht“

Nutzer, die mit der Arbeit der MoPo-CA unzufrieden sind, weil sie *konkretes* Fehlverhalten festgestellt haben, werden gebeten, ihr Anliegen den MoPo-CA-Mitarbeitern persönlich mitzuteilen.

Darüber hinaus steht den Betroffenen die Möglichkeit offen, sich bei Policy-Verstößen der MoPo-CA an den Lehrstuhl für Rechnerarchitektur der Fakultät für Angewandte Wissenschaften der Universität Freiburg als übergeordnete Kontrollinstanz zu wenden.

Literaturverzeichnis

[**SigG**] *Gesetz zur digitalen Signatur (Signaturgesetzt – SigG)* vom 22. Juli 1997, BGBl. I,S. 1870 ff.

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

Abkürzungsverzeichnis

CA:	Certification Authority (Zertifizierungsinstanz)
CRL:	Certificate Revocation List (Widerrufsliste)
DER:	Distignuished Encoding Rules (Datenformat)
DFN:	Verein zur Förderung eines Deutschen Forschungsnetzes e.V.
DN:	Distinguished Name (X.500-Name)
ID:	Identifier
ITU:	International Telecommunication Union
MoPo:	Mobile Pools
PCA:	Policy Certification Authority
PEM:	Privacy Enhanced Mail (Datenformat)
PIN:	Personal Identification Number
RA:	Registration Authority (Registrierungsinstanz)
RDN:	Relative Distinguished Name (X.500-Name)
RSA:	Rivest-Shamir-Adleman (Public-Key-Kryptographie Verfahren)
SigG:	Signaturgesetz