

mobilkom austria AG & Co KG
Obere Donaustrasse 29
1020 Wien
Tel.: +43 1 33161 – 0
Fax: 0800 664 601
www.mobilkomaustria.com

Hotline A1 SIGNATUR: 0800 664 680
Fax A1 SIGNATUR: 0800 664 681

A1 SIGNATUR

Certificate Policy für A1 SIGNATUR Zertifikate für Verwaltungssignaturen nach E-Government-Gesetz (E-GovG)

Version 1.3
23. April 2004

Inhaltsverzeichnis

Certificate Policy	3
Certification Practice Statement	5
Erstellung von Zertifikaten	6
Bedingungen für die Erstellung eines Zertifikats für die A1 SIGNATUR	7
Sicherheitsmanagement	10
Versionsgeschichte	14

A1 SIGNATUR

Certificate Policy

Mit dieser Certificate Policy wird der Einsatzbereich der von mobilkom austria AG & CoKG angebotenen A1 SIGNATUR geregelt.

Name der Policy:

Certificate Policy für A1 SIGNATUR Zertifikate für Verwaltungssignaturen nach E-Government-Gesetz (BGBl. I Nr. 10/2004)

Version 1.2 vom 16. April 2004

Die Certificate Policy für A1 SIGNATUR Zertifikate gilt für Endkundenzertifikate die im Rahmen der A1 SIGNATUR ausgestellt werden. Diese Zertifikate werden auf begutachteten Signaturerstellungseinheiten erstellt und sind entsprechend den Bestimmungen des E-Government-Gesetzes (E-GovG, BGBl. I Nr. 10/2004) für die Erstellung von Verwaltungssignaturen geeignet.

Die A1 SIGNATUR ist eine fortgeschrittene Signatur im Sinne der Signaturrechtlinie (Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates vom 13. Dezember 1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen) und entspricht der Verordnung des Bundesministeriums für Finanzen, mit der die Anforderungen an eine auf elektronischem Weg übermittelte Rechnung bestimmt werden (BGBl. II 583/2003).

Entsprechend den Bestimmungen des E-GovG und der Verwaltungssignaturverordnung (VerwSigV) werden die geheimen Schlüssel in einem durch zusätzliche, ergänzende Maßnahmen verstärkten gesicherten Kryptomodul verwahrt. Eine Verwaltungssignatur im Sinne des E-GovG kann nur unter Verwendung dieser Schlüssel erzeugt werden.

Die eingesetzten Komponenten und die angewandten Prozesse wurden auf ihre Konformität entsprechend den Bestimmungen des E-GovG (BGBl. I Nr. 10/2004), der VerwSigV (BGBl. II Nr. 159/2004) und der Verordnung des Bundesministeriums für Finanzen, mit der die Anforderungen an eine auf elektronischem Weg übermittelte Rechnung bestimmt werden (BGBl. II Nr. 583/2003), evaluiert.

Berechtigte für eine A1 SIGNATUR

Jeder Bürger für den eine positive Personenbindung erstellt werden kann, kann Kunde der A1 SIGNATUR werden, sofern nicht Ablehnungsgründe gemäß § 5 AGB Mobil vorliegen.

Zertifizierungskonzept:

mobilkom stellt im Rahmen der A1 SIGNATUR für ihre Kunden des Produkts A1 SIGNATUR individuelle X 509 Version 3 Zertifikate aus. Jedes Zertifikat ist einzigartig, trägt eine individuelle Seriennummer und ist ausschließlich dem Signator zugeordnet.

Der Aufbau der Zertifikatskette ist dreistufig.

Basis für die Zertifizierungskette ist ein trusted root Zertifikat von A-Trust. Dieses Zertifikat erfüllt die Voraussetzungen des Signaturgesetzes und der Signaturverordnung. A-Trust mißt der Sicherheit höchste Priorität bei und erfüllt durch umfangreiche Sicherheitsvorkehrungen sowie der Begutachtung ihre Zertifizierungseinheiten durch eine notifizierte Bestätigungsstelle alle Anforderungen für die Erstellung sicherer Signaturen im Sinne des SigG.

Detaillierte Informationen über die Sicherheitsstandards von A-Trust können unter www.a-trust.at eingesehen werden.

Mit diesem trusted Rootzertifikat von A-Trust wird das mobilkom Zwischeninstanzzertifikat signiert.

Dieses Zwischeninstanzzertifikat ist das Zertifikat, mit dem wieder die individuellen Zertifikate der Kunden der A1 SIGNATUR signiert werden.

Auf diese Weise wird eine lückenlose chain of trust geschaffen.

Die ausgestellten Endkundenzertifikate haben eine Laufzeit von 3 Jahren. Das Zwischeninstanzzertifikat hat eine Laufzeit von 10 Jahren.

Certification Practice Statement

Mit der Certificate Policy und dem Certification Practice Statement stellt mobilkom auf die Erbringung von Verwaltungssignaturen gem. § 25 E-GovG ab.

Um die erforderliche Sicherheit und Verlässlichkeit bei der Erbringung eines Zertifizierungsdienstes unter dem Aspekt der Erstellung von Verwaltungssignaturen zu gewährleisten hat mobilkom unter anderem eine Reihe von Maßnahmen ergriffen:

- mobilkom hat potentielle Risiken evaluiert und entsprechende Sicherheits- und Durchführungsmaßnahmen zur Vermeidung dieser Risiken vorgenommen
- Ein Sicherheitskonzept, das den gesetzlichen Anforderungen an eine Umsetzung der A1 SIGNATUR entspricht wurde erstellt und von einer unabhängigen Stelle begutachtet und bestätigt
- Diese Certificate Policy steht ergänzend zu den Informationen zur A1 SIGNATUR online auf www.a1.net zur Verfügung
- Die laufende Überprüfung der Vorgangsweisen und Prozesse im Rahmen der A1 SIGNATUR ist durch einen definierten, regelmäßigen Auditierungsprozeß gewährleistet.
- mobilkom hat mit physischen und organisatorischen Sicherheitsmaßnahmen für eine weitgehende Ausfallsicherheit des Systems vorgesorgt

mobilkom verpflichtet sich im Rahmen der A1 SIGNATUR alle gesetzlichen und behördlichen Auflagen für die sichere Erbringung des Verwaltungssignaturdienstes nach E-Government Gesetz zu erfüllen und alle in dieser Policy angeführten Verhaltensweisen einzuhalten.

Verpflichtungen des Signators

Der Signator verpflichtet sich mit der Bestellung der A1 SIGNATUR alle in den Allgemeinen Geschäftsbedingungen zur A1 SIGNATUR festgelegten Bestimmungen und Vorsichtsmaßnahmen einzuhalten, insbesondere seinen Mobilfunkanschluß mit der ihm zugeordneten SIM Karte nicht an Dritte weiterzugeben bzw. seine Signaturerstellungsdaten, insbesondere das frei wählbare Paßwort des abrechenbaren A1.Net Benutzernamens und den persönlich gewählten Signaturcode (Secure-PIN) nicht einer dritten Person mitzuteilen. Dieser persönlich gewählte Secure PIN muß mindestens acht Zeichen umfassen. Paßwort und Secure-PIN dürfen nicht schriftlich aufgezeichnet oder im Gerät gespeichert werden. Der Signator verpflichtet sich auch bei Verlust oder Diebstahl seines Mobilfunkanschlusses mobilkom unmittelbar unter der rund um die Uhr zur Verfügung stehenden Hotline (0800 664 664 bzw. 0800 664 680) zu verständigen.

Erstellung von Zertifikaten

Umgang mit den Schlüsseln zur Erstellung von Zertifikaten

Die für die Erbringung des Zertifizierungsdienstes und die Erstellung von Verwaltungssignaturen erforderliche Generierung von CA Schlüsseln erfolgt entsprechend den gesetzlichen Bestimmungen.

Autorisiertes, speziell geschultes Personal erzeugt im 4 Augenprinzip in physisch abgesicherter Umgebung die für die Durchführung der A1 SIGNATUR erforderlichen CA Schlüssel.

Die CA Schlüssel werden in einem speziellen Security Server erstellt, der auch für die Erzeugung fortgeschrittener Signaturen geeignet ist. Die Länge der CA Schlüssel beträgt 2048 bit.

Der für die Schlüsselgenerierung eingesetzte Algorithmus entspricht hinsichtlich Schlüssellänge und Signaturerstellungsdaten den Anforderungen an eine sichere Signatur und ist für qualifizierte Zertifikate geeignet.

Der Client Private Key des Kunden bleibt geheim und kann nur durch diesen selbst für Ver- und Entschlüsselungstransaktionen genutzt werden.

Security Server

Zur Durchführung der A1 SIGNATUR werden spezielle Security Server eingesetzt, die in gesicherter Umgebung im 4 Augenprinzip in Betrieb genommen werden. Im Zuge der Inbetriebnahme erfolgte eine Funktionsprüfung durch qualifizierte Mitarbeiter von mobilkom. Die Betriebsabläufe in Zusammenhang mit dem Security Server wurden von unabhängiger Stelle begutachtet.

Bedingungen für die Erstellung eines Zertifikats für die A1 SIGNATUR

Nutzung der A1 SIGNATUR

Informationen sowie Geschäftsbedingungen für die Nutzung der A1 SIGNATUR werden von mobilkom unter www.a1.net öffentlich zur Verfügung gestellt.

Personenbindung

Um das Produkt A1 SIGNATUR nutzen zu können, ist eine erfolgreiche Identifikation des Teilnehmers durch mobilkom erforderlich. Eine Überprüfung der Identität wird anhand eines amtlichen Lichtbildausweises (Reisepaß, Personalausweis) vorgenommen. Eine Kopie des Lichtbildausweises wird elektronisch archiviert. Die Anmeldung zur A1 SIGNATUR erfolgt online, die persönliche Identifikation wird in den A1 Shops und im ausgewählten Fachhandel durchgeführt. mobilkom kann für die Identifikation auch die im Zusammenhang mit einem früheren Geschäftsfall durchgeführte Identitätsfeststellung, sofern diese auf den o.a. Dokumenten beruht heranziehen.

Im Antrag für die A1 SIGNATUR werden gem. § 11/2 SigVO folgende Angaben erhoben: Namen, Datum und Ort der Geburt sowie Adresse des A1 SIGNATUR Kunden, Datum der Ausstellung und Nummer des vorgelegten Lichtbildausweises sowie die Behörde von der der Lichtbildausweis ausgestellt wurde. Die vom Kunden angegebenen Daten werden von mobilkom auf Übereinstimmung mit den Ausweisdaten des Kunden überprüft.

Erstellung des Zertifikats

Nach Überprüfung der erhobenen Daten wird seitens mobilkom die Personenbindung erstellt. Kann eine Personenbindung nicht erfolgreich erstellt werden, so wird kein Zertifikat ausgestellt. Bei erfolgreicher Personenbindung wird seitens mobilkom dem Kunden das Zertifikat für die A1 SIGNATUR ausgestellt. Die Gültigkeit des Zertifikats ist mit 3 Jahren beschränkt. Bei der A1 SIGNATUR werden X.509 Version 3 Zertifikate ausgestellt.

Jedes Zertifikat beinhaltet:

- Seriennummer des Zertifikats

- Bezeichnung des Zertifikatsausstellers:

CN = A1 SIGNATUR
OU = A1.net
O = mobilkom austria AG & Co KG
C = AT

- Beginn und Ende der Gültigkeit des Zertifikats
- Bezeichnung des Zertifikatsinhabers

givenName / G First name of the subject
Surname / sn Surname
CommonName / cn Name of the owning person or entity

- Den öffentlichen Schlüssel des Zertifikatsinhabers (RSA 2048 Bit)
- Angabe des Algorithmus für die Signatur des Zertifikats
(mobilkom verwendet für die Signatur der Zertifikate den RSA Algorithmus mit 2048 Bit)

Eine Verlängerung eines ausgestellten Zertifikats ist nicht möglich. Vor dessen Ablauf wird der Kunde verständigt und – nachdem er die A1-SIGNATUR erneut beantragt hat – für ihn ein neues Zertifikat ausgestellt.

Widerruf

Unter Widerruf ist eine nicht rückgängig machbare Beendigung der Gültigkeit eines Zertifikates zu verstehen, ein einmal widerrufenes Zertifikat kann nicht wieder Gültigkeit erlangen. Ein Widerruf kann jederzeit vom Kunden der A1 SIGNATUR beantragt werden. Der Widerruf wird via Internet und unter Einsatz der A1 SIGNATUR beantragt. In Falle der Störung der Internetverbindung ist ein telefonischer Widerruf unter der Hotline 0800 664 680 mit den im Geschäftsverkehr mit mobilkom etablierten Authentifizierungsmechanismen möglich. Widerrufene Zertifikate werden seitens mobilkom in einer im a1.net einsehbaren Widerrufsliste veröffentlicht.

Widerrufsliste (CRL)

Die von mobilkom geführte Widerrufsliste wird mindestens einmal täglich aktualisiert. Das Datum und die Zeit der letzten Aktualisierung sind aus der Widerrufsliste ersichtlich. Widerrufslisten sind täglich 24 Stunden im a1.net unter <http://www.a1.net/signatur/crl/currentcrl.crl> abrufbar. In der CRL werden die Seriennummer und der Zeitpunkt der Eintragung veröffentlicht.

Verzeichnisdienst

Der Status der A1 SIGNATUR Zertifikate kann über einen eigenen Verzeichnisdienst abgerufen werden. Der Empfänger eines mit A1 SIGNATUR signierten Dokumentes kann den Status des dafür benutzten Zertifikats einzeln abfragen.

Zu diesem Zweck ist eine e-mail mit der Nummer des Zertifikats an folgende Adresse zu richten:

Verzeichnisdienst_A1_SIGNATUR@mobilkom.at

Sicherheitsmanagement

Sicherheitsmaßnahmen und sicherheitsrelevante Funktionen im Bereich der A1 SIGNATUR werden von mobilkom dokumentiert und regelmäßigen Reviews unterzogen. Eine Anpassung an sich ändernde Anforderungen wird durchgeführt und dokumentiert.

Zum Schutz der Daten und Informationen werden von mobilkom geeignete, dem Stand der Technik entsprechende Maßnahmen getroffen.

Personal

mobilkom setzt im Bereich der A1 SIGNATUR nur Personal ein, das das entsprechende Fachwissen, die Qualifikation und die Erfahrung für eine solche Tätigkeit aufweist. Sämtliche eingesetzten Mitarbeiter müssen den durch mobilkom festgelegten Rekrutierungs- und Identifikationsprozeß durchlaufen haben sowie die mobilkominternen Schulungen zur Datensicherheit besucht haben.

Funktionen und Verantwortlichkeiten im Rahmen der A1 SIGNATUR werden formell festgelegt und den Mitarbeitern zur Kenntnis gebracht. Die Zuteilung der Verantwortlichkeiten erfolgt direkt durch das zugeordnete Management.

Die Einhaltung der Sicherheitsrichtlinien im Zusammenhang mit der A1 SIGNATUR unterliegt einem wiederkehrenden, regelmäßigen Audit.

Physikalische und organisatorische Sicherheitsmaßnahmen

Sicherheitskritische Operationen finden unter besonderen räumlichen Schutzvorkehrungen statt. Der Zutritt zu diesen speziell abgesicherten Räumlichkeiten ist nur für von mobilkom autorisiertes Personal möglich.

Der Betrieb der Systeme für die Zertifikatsgenerierung und –erstellung erfolgt in einer technischen Umgebung die soweit abgeschirmt ist, daß eine Kompromittierung durch nicht autorisierte Zugriffe nicht möglich ist.

Sicherheitsmaßnahmen im Bereich der A1 SIGNATUR umfassen den Gebäude und Zutrittsschutz, den Schutz der eingesetzten EDV Systeme sowie Schutzmaßnahmen zur Abwendung von Elementargefahren und Stromausfällen.

Betriebsführung

mobilkom betreibt das Zertifizierungssystem in sicherer und korrekter Weise um das Risiko des Versagens oder eines Ausfalls zu minimieren, dazu wurden folgende Maßnahmen ergriffen:

- Die Integrität der Computersysteme wird durch verschiedenste technische und organisatorische Maßnahmen vor Virenangriffen oder böswilliger, nicht autorisierter Software geschützt.
- Das interne Netzwerk wird durch Firewalls und Intrusion Detection Systeme vor Zugriffen von außen geschützt. Regelmäßige Kontrollen betreffend nicht autorisierter Zugriffsversuche werden durchgeführt.
- Die eingesetzten Systeme entsprechen dem Stand der Technik.
- Datenträger werden vor Beschädigung, Diebstahl und nicht autorisiertem Zugriff geschützt. Datenträger werden entsprechend aufbewahrt und wenn nicht mehr benötigt, in sicherer Art und Weise vernichtet.
- Für die Administration und Ausführung sämtlicher sicherheitskritischer Prozesse die im Rahmen der A1 SIGNATUR ablaufen sind seitens mobilkom genau definierte Verfahrensweisen festgelegt, die einem regelmäßigen Review unterzogen werden.
- Der Einsatz der Mitarbeiter erfolgt entsprechend den ihnen zugewiesenen und in der Benutzerverwaltung abgebildeten Rollen.
- Ein Systemzugriff ohne vorhergehende Authentifizierung des Personals ist nicht möglich.
- Jeder Systemzugriff wird mitgeloggt. Eine Kontrolle der Logfiles in wiederkehrenden Abständen wird durchgeführt.

Kundendienst

Um Fragen und Reklamationen in Zusammenhang mit der A1 SIGNATUR beauskunften und bearbeiten zu können, wird seitens mobilkom ein entgeltfreier, telephonisch rund um die Uhr erreichbarer Kundendienst zur Verfügung gestellt.

Hotline A1 SIGNATUR: 0800 664 680
Kundenfax A1 SIGNATUR 0800 664 681

Die Bestimmungen des § 30 der AGB Mobil (Einwendungen) gelten für die A1-SIGNATUR sinngemäß.

Aufrechterhaltung des Betriebs / Behandlung von Zwischenfällen

mobilkom trachtet danach durch interne Sicherheits- und Vorsorgemaßnahmen das Risiko eines Ausfalls in Folge von Katastrophen oder Kompromittierung eines Zertifikats so gering wie möglich zu halten.

Notfalls- und Ausfallspläne wurden erstellt um für eine etwaige Beeinträchtigung des Dienstes vorbereitet zu sein und eine kurzfristige Wiederaufnahme des Dienstes zu gewährleisten.

Einstellung der Tätigkeit

Entsprechend den gesetzlichen Vorschriften wird mobilkom im Falle der Einstellung des Dienstes dies unverzüglich der Aufsichtsstelle anzeigen und ihre Kunden durch Veröffentlichung von der Einstellung informieren.

Übereinstimmung mit den gesetzlichen Bestimmungen

Die A1 SIGNATUR wird unter Einhaltung aller gesetzlicher Regelungen und Auflagen des E-GovG und der VerwSigV durchgeführt. Die Verpflichtungen des Datenschutzgesetzes werden umgesetzt und damit persönliche Daten vor Beschädigung, Manipulation sowie nicht autorisierter und ungesetzlicher Verarbeitung geschützt. Die im Zuge einer Signatur an mobilkom übermittelten Daten werden nur mit Einverständnis des Signators oder aufgrund gerichtlichen Beschlusses auf Basis gesetzlicher Regelungen offengelegt.

Aufbewahrung der Informationen

Datensätze zur A1 SIGNATUR werden vollständig und vertraulich für die Dauer von 7 Jahren bei mobilkom aufbewahrt. Die Aufbewahrung erfolgt manipulations- und zerstörungssicher und umfaßt den genauen Zeitpunkt des Eintretens des Ereignisses. Die Aufbewahrung umfaßt auch alle Informationen die in Zusammenhang mit der Registrierung stehen.

Dies umfaßt insbesondere:

- Die Art des Identifikationsdokuments, daß bei der Registrierung vorgelegt wurde
- Die Daten und die eindeutige Nummer des Identifikationsdokuments
- Die Akzeptanz der Vertragsbestimmungen und –vereinbarungen
- Die Angaben über die Registrierung

Ereignisse die den Lebenszyklus der Zertifikate und Schlüssel betreffen werden aufgezeichnet und gespeichert.
Anträge auf Sperre, deren Aufhebung bzw. Kündigung der A1 SIGNATUR werden aufgezeichnet.

Versionsgeschichte

Version	Datum	Titel	Anlaß für Neuversion
1.0	24.02.2004	CP A1 SIGNATUR	mobilkominterne Erstfassung
1.1	02.03.2004	CP A1 SIGNATUR	mobilkominterne Fassung Einarbeitung E-GovG
1.2	16.04.2004	CP A1 SIGNATUR	Veröffentlichung CP/ Produktlaunch A1 SIGNATUR
1.3	23.04.2004	CP A1 SIGNATUR	Aufnahme Verzeichnisdienst