



Amtssignaturzertifikate A-Trust (ASZ-ATRUST)

Prozessabläufe für Amtssignaturzertifikate beim Zertifizierungsdiensteanbieter A-Trust

Bezeichnung	Amtssignaturzertifikate A-Trust
Kurzbezeichnung	ASZ-ATRUST
Version	1.0.0
Datum	06.04.2005
Dokumentenklasse	Erläuterung
Dokumentenstadium	Öffentlicher Entwurf
Kurzbeschreibung	Dieses Papier beschreibt die Umsetzung der Allgemeine Richtlinien für Amtssignaturzertifikate in der Verwaltung [ASZ] durch den Zertifizierungsdiensteanbieter A-Trust.
Autoren	Friedrich Hirschbügl (friedrich.hirschbuegl@a-trust.at) Gregor Karlinger (gregor.karlinger@cio.gv.at)
Arbeitsgruppe	A-Trust Ges.für Sicherheitssysteme im elektronischen Datenverkehr GmbH Stabstelle IKT-Strategie des Bundes



Inhaltsverzeichnis

1 Motivation.....	3
2 Zertifikatsverwahrung und Einsatzbereich.....	3
3 Zertifikatsinhalte.....	3
3.1 Bezeichnung des Zertifikatswerbers.....	3
3.2 Schlüsselverwendung.....	3
3.3 Behördeneigenschaft.....	3
3.4 Widerrufsinformation.....	3
3.5 Zertifizierungsrichtlinien.....	3
4 Prozesse.....	4
4.1 Registrierung.....	4
4.1.1 Antragstellung.....	4
4.1.2 Prüfung von Identität und Behördenzugehörigkeit.....	5
4.1.3 Bestätigung durch den Zertifikatswerber.....	5
4.1.4 Übermittlung des erstellten Zertifikats.....	5
4.2 Widerruf.....	6
4.3 Abrechnung.....	6
5 Referenzen.....	8
6 Historie.....	9



1 Motivation

Dieses Papier beschreibt die Umsetzung der Allgemeinen Richtlinien für Amtssignaturzertifikate in der Verwaltung [ASZ] durch den Zertifizierungsdiensteanbieter A-Trust.

2 Zertifikatsverwahrung und Einsatzbereich

Der Zertifikatswerber bewahrt die Signaturerstellungsdaten in einer kennwortgeschützten Datei auf.

Die *Certification Policy* von A-trust muss sowohl den Einsatz für Einzelsignaturen (der Zertifikatswerber stößt jeden Signaturvorgang einzeln an) als auch den Einsatz für Massensignaturen (der Zertifikatswerber konfiguriert einmal ein Signatursystem, das fortan ohne weitere Benutzerinteraktion beliebig oft automatisch einen Signaturvorgang anstößt; organisatorisch ist auf Seiten des Zertifikatswerbers sichergestellt, dass die Signaturerstellungsdaten nicht in die Hände dritter gelangen können) erlauben.

3 Zertifikatsinhalte

3.1 Bezeichnung des Zertifikatswerbers

Das Feld *Subject* des Zertifikats enthält im *CN* den Namen des Zertifikatswerbers sowie in *O* bzw. *OU* die Behörde, für die der Zertifikatswerber als Organwalter tätig ist.

3.2 Schlüsselverwendung

Als Verwendungszwecke für den Schlüssel enthält das Zertifikat in der Zertifikatserweiterung *Key Usage* die Angaben *Digital Signature*, *Key Encipherment* sowie *Data Encipherment*.

3.3 Behördeneigenschaft

Das Zertifikat enthält die Zertifikatserweiterung *Verwaltungseigenschaft* [X509ZE]. Auf Wunsch des Zertifikatswerbers wird in die *Verwaltungseigenschaft* das *Verwaltungskennzeichen* aufgenommen. Dieses Kennzeichen wird vom Zertifikatswerber lediglich behauptet und von A-Trust nicht verifiziert.

3.4 Widerrufsinformation

Das Zertifikat enthält die für eine automatische Bildung der Zertifikatskette sowie für die automatische Widerrufsprüfung nötigen Zertifikatserweiterungen (*Authority Information Access*, *CRL Distribution Point*).

3.5 Zertifizierungsrichtlinien

Das Zertifikat enthält die Zertifikatserweiterung *Certification Policies*, in der auf die angewendete



34 *Policy* und/oder auf das zugehörige *Certification Practice Statement* verwiesen wird.

35 **4 Prozesse**

36 **4.1 Registrierung**

37 Der gesamte Registrierungsprozess wird so gestaltet, dass ein möglichst hoher Grad an Automation er-
38 reicht wird. Die Antragstellung durch den Zertifikatswerber erfolgt online, ebenso die Übermittlung des
39 Zertifikats durch die A-Trust an den Zertifikatswerber.

40 **4.1.1 Antragstellung**

41 Die Antragstellung durch den Zertifikatswerber erfolgt online per HTTPS mittels Web-Formular. Der
42 Zertifikatswerber trägt in dieses Webformular folgende Informationen ein:

- 43 • Angaben zur Person des Zertifikatswerbers:
 - 44 • Vorname, Nachname: Diese Informationen werden im Zertifikat kodiert.
 - 45 • Geburtsdatum, Geburtsort: Diese Informationen dienen zur exakten Benennung der Identität
46 des Zertifikatswerbers.
 - 47 • Emailadresse des Zertifikatswerbers: An diese Emailadresse sendet A-Trust im Rahmen der
48 Registrierung einerseits eine Email, die vom Zertifikatswerber bestätigt werden muss, sowie
49 andererseits das erstellte Zertifikat.
 - 50 • Scan eines Lichtbildausweises des Zertifikatswerbers: An Hand dieses Dokuments verifiziert
51 A-Trust die Identität des Zertifikatswerbers. Als Alternative kann der Zertifikatswerber
52 angeben, dass er eine Kopie des Lichtbildausweises an A-Trust faxen wird. Sollte die Qual-
53 ität des Scans nicht ausreichend für eine klare Identifizierung der Person sein, so kann A-
54 Trust eine Kopie per Fax anfordern, um selbsttätig einen guten Scan zu erstellen.
- 55 • Angaben zur Organisation, für die der Zertifikatswerber als Organwalter tätig ist:
 - 56 • Organisation, Organisationseinheit, ggf. *Verwaltungskennzeichen*: Diese Informationen
57 werden im Zertifikat kodiert.
 - 58 • Postadresse der Organisation für etwaigen Schriftverkehr, z.B. für die Information des Zerti-
59 fikatswerbers sowie der Organisation über eine erfolgte Sperre oder über einen erfolgten
60 Widerruf des Zertifikats.
 - 61 • Scan eines Schreibens einer für die Organisation approbationsbefugten Person, das sowohl
62 deren Unterschrift als auch das Rundsiegel der Organisation trägt, und aus dem hervorgeht,
63 dass der Zertifikatswerber (bezeichnet durch zumindest durch Vorname, Nachname,
64 Geburtsdatum und Emailadresse) für die Organisation als Organwalter tätig ist. Als Alterna-
65 tive kann der Zertifikatswerber angeben, dass er eine Kopie des Schreibens an A-Trust faxen



66 wird. Sollte die Qualität des Scans nicht ausreichend für eine klare Identifizierung der Per-
67 son sein, so kann A-Trust eine Kopie per Fax anfordern, um selbsttätig einen guten Scan zu
68 erstellen.

- 69 • Telefonnummer der Organisation in jener Form, wie sie im öffentlichen Telefonbuch geführt
70 wird (d.h. in der Regel die Vermittlung, keine Angabe einer Nebenstelle); über diese Tele-
71 fonnummer prüft A-Trust die Existenz der Organisation sowie in Ergänzung zum oben erwäh-
72 nten Schreiben die Zugehörigkeit des Zertifikatswerbers zur Organisation.

- 73 • PKCS#10 Request

- 74 • Der Zertifikatswerber erzeugt den privaten Schlüssel selbst; an A-Trust übermittelt er als
75 Beweis des Besitzes des privaten Schlüssels einen PKCS#10 Request.

- 76 • Gültigkeitsdauer des Zertifikats: Die Gültigkeitsdauer beträgt im Standardfall fünf Jahre. Der
77 Zeitraum kann vom Zertifikatswerber im Antrag auf drei Jahre reduziert werden. (*Motivation: Der*
78 *Standardfall beträgt fünf Jahre, um den Verwaltungsaufwand auf Seiten der Organisation sowie*
79 *bei A-Trust möglichst gering zu halten.*)

80 4.1.2 Prüfung von Identität und Behördenzugehörigkeit

81 A-Trust verifiziert an Hand des Scans bzw. der gefaxten Kopie des Lichtbildausweises die Angaben zur
82 behaupteten Identität des Zertifikatswerbers.

83 Weiters prüft A-Trust an Hand des Scans bzw. der gefaxten Kopie des Schreibens der approbations-
84 befugten Person die Zugehörigkeit des Zertifikatswerbers zur von ihm behaupteten Organisation.

85 Die Existenz der Organisation sowie die Zugehörigkeit des Zertifikatswerbers zur Organisationseinheit
86 prüft A-Trust durch einen Anruf bei der vom Zertifikatswerber angegebenen Telefonnummer der Or-
87 ganisation. Vor diesem Anruf verifiziert A-Trust die Zugehörigkeit dieser Telefonnummer zur Organi-
88 sation an Hand eines öffentlichen Telefonbuchs (z.B. Online-Telefonbuch von Herold). An Hand dieses
89 Anrufs prüft A-Trust, ob der Zertifikatswerber für die Organisation tätig ist, und ob die vom Zerti-
90 fikatswerber angegebene Emailadresse eine solche der Organisation ist. (*Motivation: Damit wird aus-*
91 *geschlossen, dass ein Angreifer nur durch Übermittlung von gefälschten Dokumentkopien ein Zer-*
92 *tifikat für einen Organwaller erschleicht*)

93 4.1.3 Bestätigung durch den Zertifikatswerber

94 Nach der erfolgreichen Verifikation von Identität und Behördenzugehörigkeit sendet A-Trust an die im
95 Antrag angegebene Emailadresse des Zertifikatswerbers eine Email, die der Zertifikatswerber bestäti-
96 gen muss, bevor A-Trust mit der Ausstellung des Zertifikats fortfährt. (*Motivation: Dadurch wird aus-*
97 *geschlossen, dass ein Angreifer nur durch Kenntnis des Organwalters sowie durch die Übermit-*
98 *tlung von gefälschten Dokumentkopien ein Zertifikat für einen Organwaller erschleicht; vielmehr*
99 *müsste er nun auch noch im Besitz des Emailkontos des Organwalters sein.*)

100 4.1.4 Übermittlung des erstellten Zertifikats



101 A-Trust übermittelt das erstellte Zertifikat an die im Antrag angegebene Emailadresse des Zerti-
102 fikatswerbers.

103 4.2 Widerruf

104 Der Widerruf des ASZ kann einerseits durch den Zertifikatswerber selbst, andererseits aber auch durch
105 die Organisation, für die der Zertifikatswerber als Organwalter tätig ist, erfolgen.

106 Der Widerruf durch den Zertifikatswerber erfolgt mittels eines eigenhändig vom Zertifikatswerber un-
107 terzeichneten Schreibens, in dem seine Identität zumindest durch Angabe von Vorname, Nachname,
108 Geburtsdatum und Geburtsort, sowie das zu widerrufende Zertifikat bezeichnet ist. Dieses Schreiben
109 sendet der Zertifikatswerber per Fax an A-Trust. *(Motivation: Auf die Vergabe eines Widerrufspass-
110 wortes wird auf Grund der schlechten Erfahrungen von A-Trust mit der Merkbarkeit solcher Pass-
111 wörter verzichtet. Durch die verpflichtende Angabe der im Regelfall nicht öffentlich verfügbaren
112 Identitätsmerkmale Geburtsdatum und Geburtsort wird ein unrechtmäßiger Widerruf durch Dritte
113 trotzdem wesentlich erschwert).*

114 Der Widerruf im Namen der Organisation erfolgt durch ein Schreiben einer für die Organisation appro-
115 bationsbefugten Person, das sowohl deren Unterschrift als auch das Rundsiegel der Organisation trägt,
116 und in dem die Identität des Zertifikatswerbers zumindest durch Angabe von Vorname, Nachname und
117 Geburtsdatum, sowie das zu widerrufende Zertifikat bezeichnet ist. Dieses Schreiben sendet der Appro-
118 bationsbefugte per Fax an A-Trust. *(Motivation: Auf die Vergabe eines Widerrufspasswortes wird
119 auf Grund der schlechten Erfahrungen von A-Trust mit der Merkbarkeit solcher Passwörter
120 verzichtet. Durch die verpflichtende Angabe des im Regelfall nicht öffentlich verfügbaren Iden-
121 titätsmerkmals Geburtsdatum wird ein unrechtmäßiger Widerruf durch Dritte trotzdem wesentlich
122 erschwert; auf die Angabe des Identitätsmerkmals Geburtsort wird im Gegensatz zum Widerruf
123 durch den Zertifikatswerber verzichtet, da dieses Merkmal i.d.R. in der Organisation nicht verfüg-
124 bar ist, und zum Widerruf dann die Mithilfe des Zertifikatswerbers notwendig ist, was u.U. nicht
125 zielführend ist, z.B. nach einer Entlassung).*

126 In beiden Fällen eines möglichen Widerrufs sendet A-Trust eine Verständigung sowohl an die im
127 Antrag angegebene Postadresse des Zertifikatswerbers als auch an die ebendort angegebene Postadresse
128 der Organisation. *(Motivation: Sollte es einem Dritten tatsächlich gelingen, einen unrechtmäßigen
129 Widerruf durchzuführen, erfahren Zertifikatswerber und Organisation rasch davon und können
130 schnell geeignete Schritte zur Behebung des Schadens setzen.)*

131 Für das Zertifikat existiert unter der in der Zertifikatserweiterung *CRL Distribution Point* angegebenen
132 Adresse ein zuverlässiger und hochverfügbarer Widerrufsdienst. Ein Widerruf wird von A-Trust bin-
133 nen 24 Stunden ab Bekanntwerden in ihren Verzeichnissen veröffentlicht.

134 4.3 Abrechnung

135 Folgende Möglichkeiten der Abrechnung zwischen dem Zertifikatswerber und A-Trust werden beste-
136 hen:

137 1. Die Organisation des Zertifikatswerbers ist bei A-Trust als Firmenkunde registriert (derzeit z.B.



138 BKA, BRZ, BMF, BMWAA): Es existiert ein Vertrag zwischen A-Trust und der Organisation, nach
139 dessen Bestimmungen zur Abrechnung dann weiter vorgegangen wird. Der Zertifikatswerber muss
140 in einem solchen Fall im Zertifikatsantrag auf das Bestehen eines Vertragsverhältnisses hinweisen.

141 2. Die Organisation des Zertifikatswerbers ist bei A-Trust nicht als Firmenkunde registriert:

142 a) Wenn davon ausgegangen werden kann, dass die Organisation zukünftig in bedeutendem
143 Ausmaß Zertifikatsprodukte bei A-Trust bestellen wird, kann sie sich als Firmenkunde reg-
144 istrieren lassen. Es gelten dann die Bestimmungen aus 1.

145 b) Die Organisation führt eine Einzelbestellung durch und bezahlt mittels Bankeinzug.
146 Notwendig dazu ist die Erfassung einer Bankverbindung im Zertifikatsantrag durch den Zer-
147 tifikatswerber. In dieser Variante ist die kostenlose Ausstellung eines Ersatzzertifikats
148 möglich, wenn sich Daten im Zertifikat während der Gültigkeitsdauer des Zertifikats verän-
149 dern oder das Zertifikat aus anderen Gründen widerrufen werden muss. Die Bezahlung der
150 Zertifikatsgebühr von €50 exkl. Ust./Jahr erfolgt durch jährlichen Einzug.

151 c) Die Organisation führt eine Einzelbestellung durch und bezahlt mittels Rechnung. Die im
152 Zertifikatsantrag erfasste Postadresse der Organisation gilt in diesem Fall auch als Rech-
153 nungsadresse. In dieser Variante ist die unter b) erwähnte kostenlose Ausstellung eines Er-
154 satzzertifikats nicht möglich. Die Bezahlung der Zertifikatsgebühr von €50 exkl. Ust./Jahr
155 erfolgt für die gesamte Gültigkeitsperiode im voraus.

156 **5 Referenzen**

157 **ASZ**

158 Karlinger, Gregor: Amtssignaturzertifikate (ASZ). Allgemeine Richtlinien für Amtssignaturzerti-
159 fikate in der Verwaltung. Version 1.0.0 vom 06. 04. 2005.
160 <http://www.cio.gv.at/it-infrastructure/pki/Amtssignaturzertifikate.AllgemeineRichtlinien.1-0-0.pdf>

161 **X509ZE**

162 Hollosi, Arno: X509 Zertifikatserweiterungen für die Verwaltung. Version 1.0.3 vom 21. 02.
163 2005.
164 <http://www.cio.gv.at/it-infrastructure/pki/X509ext-1.0.3-20050221.pdf>

6 Historie

Version	Datum	Kommentar
1.0.0	06.04.2005	Erstellt.
Ersteller		
Gregor Karlinger		