



Amtssignaturzertifikate (ASZ)

Allgemeine Richtlinien für Amtssignaturzertifikate in der Verwaltung

Bezeichnung	Amtssignaturzertifikate
Kurzbezeichnung	ASZ
Version	1.0.0
Datum	06.04.2005
Dokumentenklasse	Konvention
Dokumentenstadium	Öffentlicher Entwurf
Kurzbeschreibung	§ 19 des österreichischen E-Government Gesetzes (E-GovG, vergleiche [E-GovG]) normiert den Begriff der Amtssignatur für die digitale Signatur auf Erledigungen der Behörde. Dieses Papier skizziert die daraus abzuleitenden Anforderungen an ein Zertifikat für eine solche Amtssignatur.
Autoren	Gregor Karlinger (gregor.karlinger@cio.gv.at)
Arbeitsgruppe	Stabstelle IKT-Strategie des Bundes



Inhaltsverzeichnis

1 Motivation.....	3
2 Direkt ableitbare Anforderungen.....	3
3 Konkretisierung der Anforderungen.....	3
3.1 Zertifikatsverwahrung.....	3
3.2 Einsatzgebiet der Signatur.....	3
3.3 Zertifikatsaufbau.....	4
3.4 Registrierungsprozess.....	4
3.4.1 Fax/Telefonrückruf.....	4
3.4.2 Persönliche Registrierung in einer Registrierungsstelle des ZDA.....	4
3.4.3 Registrierung durch eine Behörde.....	5
3.5 Widerruf.....	5
4 Referenzen.....	6
5 Historie.....	7



1 Motivation

§ 19 des österreichischen E-Government Gesetzes (E-GovG, vergleiche [E-GovG]) normiert den Begriff der Amtssignatur für die digitale Signatur auf Erledigungen der Behörde. Dieses Papier skizziert die daraus abzuleitenden Anforderungen an ein Zertifikat für eine solche Amtssignatur.

2 Direkt ableitbare Anforderungen

Direkt aus § 19 E-GovG lassen sich folgende Anforderungen an das Zertifikat für die Amtssignatur ableiten:

1. Signatur nach dem österreichischen Signaturgesetz: Damit ist das Zertifikat jedenfalls auf eine natürliche Person auszustellen.
2. Zertifikatserweiterung Verwaltungseigenschaft: Diese einfache X509-Zertifikatserweiterung statuiert, dass das Zertifikat auf eine Person ausgestellt ist, die als Organwalter für eine Behörde tätig sein kann. Vergleiche [SpecVE].

Aus den einschlägigen Bestimmungen des Allgemeinen Verwaltungsverfahrensgesetzes (AGV, vergleiche [AVG]) lassen sich darüber hinaus folgende weitere Anforderungen ableiten:

3. Bezeichnung der Behörde: Aus dem Zertifikat muss neben dem Namen des Signators auch der Name der Behörde ablesbar sein.

3 Konkretisierung der Anforderungen

Aus den oben angeführten Anforderungen sowie den Anforderungen an eine praxistaugliche Public Key Infrastruktur lassen sich folgende, konkretisierte Anforderungen an ein Zertifikat für die Amtssignatur ableiten:

3.1 Zertifikatsverwahrung

Aus Anforderung 1 ergibt sich keine Notwendigkeit der Aufbewahrung der Signaturerstellungsdaten (privater Schlüssel) auf einer Krypto-Hardware (HSM oder Smartcard). Vielmehr ist es auch ausreichend, dass der Zertifikatswerber die Signaturerstellungsdaten in einer kennwortgeschützten Datei aufbewahrt.

3.2 Einsatzgebiet der Signatur

Die Certification Policy des Zertifizierungsdiensteanbieters 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 sichergestellt, dass die Signaturerstellungsdaten nicht in die Hände unbefugter Dritter gelangen kön-



37 nen) erlauben.

38 3.3 Zertifikatsaufbau

39 Das Feld Subject des Zertifikats benennt zumindest in CN den Namen des Zertifikatswerbers sowie in
40 O bzw. OU die Behörde, für die der Zertifikatswerber als Organwalter tätig ist.

41 Das Zertifikat trägt die Zertifikatserweiterung Verwaltungseigenschaft (Anforderung 2).

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

45 Das Zertifikat enthält die Zertifikatserweiterung Certification Policies, in der auf die angewendete Poli-
46 cy und/oder auf das zugehörige Certification Practice Statement verwiesen wird.

47 3.4 Registrierungsprozess

48 Direkt aus Anforderung 1 ist sind zwar keine besonderen Anforderungen an die Qualität der Reg-
49 istrierung des Zertifikatswerbers abzuleiten, dennoch ist durch das hohe Vertrauen, das vermutlich vom
50 Bürger in ein vorliegendes, amtsigniertes Dokument gelegt wird, eine gewisse Mindestqualität betref-
51 fend die Identifikation und Authentisierung des Zertifikatswerbers zu fordern.

52 Folgende drei Varianten kommen dafür in Frage. Den ersten beiden Varianten ist gemein, dass der Zer-
53 tifizierungsdiensteanbieter bei einem Zweifel, ob es sich bei der Organisation, welcher der Zerti-
54 fikatswerber angehört, überhaupt um eine Behörde handelt, eine (z. B. telefonische) Rückfrage bei der
55 Stabsstelle IKT-Strategie des Bundes durchführt.

56 3.4.1 Fax/Telefonrückruf

57 Der Zertifikatswerber schickt eine Kopie eines amtlichen Lichtbildausweises zusammen mit Unterla-
58 gen, die die Zugehörigkeit seiner Person zur im Zertifikat zu benennenden Behörde bestätigen (z. B. ein
59 mit Rundsiegel und Unterschrift eines Approbationsbefugten versehenes Schreiben oder der Dien-
60 stausweis des Zertifikatswerbers), an den Zertifizierungsdiensteanbieter.

61 Weiters übermittelt der Zertifikatswerber dem Zertifizierungsdiensteanbieter die Telefonnummer der
62 Behörde (Vermittlung) für einen Rückruf. Der Zertifizierungsdiensteanbieter prüft, ob diese Telefon-
63 nummer im öffentlichen Telefonbuch der Behörde zugeordnet ist. Falls ja, ruft der Zertifizierungsdien-
64 steanbieter diese Telefonnummer an und überprüft durch Anfrage, ob der Zertifikatswerber für die Or-
65 ganisation tätig ist, und ob vom Zertifikatswerber tatsächlich ein Amtssignaturzertifikat beantragt
66 wurde.

67 3.4.2 Persönliche Registrierung in einer Registrierungsstelle des ZDA

68 Der Zertifikatswerber erscheint persönlich zur Prüfung seiner Identität an Hand eines amtlichen Licht-
69 bildausweises in einer Registrierungsstelle des Zertifizierungsdiensteanbieters. Im Zuge dieser Reg-



70 istrierung dokumentiert er durch Vorlage entsprechender Unterlagen die Zugehörigkeit zur im Zerti-
71 fikat zu benennenden Behörde (z. B. ein mit Rundsiegel und Unterschrift eines Approbationsbefugten
72 versehenes Schreiben oder der Dienstausweis des Zertifikatswerbers).

73 **3.4.3 Registrierung durch eine Behörde**

74 Die Registrierungsdienstleistung wird durch eine Behörde selbst für die eigenen Bediensteten erbracht.
75 Zwischen dem Zertifizierungsdiensteanbieter und der die Registrierung durchführenden Behörde existi-
76 tiert ein Vertrag, der Art und Umfang der von der Behörde durchzuführenden Registrierung genau
77 regelt.

78 **3.5 Widerruf**

79 Für das Zertifikat existiert unter der in der Zertifikatserweiterung CRL Distribution Point angegebenen
80 Adresse ein zuverlässiger und hochverfügbarer Widerrufsdienst.

81 Der Widerruf für das Zertifikat kann sowohl vom Zertifikatswerber selbst als auch von einer für die im
82 Zertifikat benannten Behörde handlungsberechtigten Person erfolgen.

83 Ein Widerruf ist vom Zertifizierungsdiensteanbieter binnen 24 Stunden ab Bekanntwerden in seinen
84 Verzeichnissen zu veröffentlichen.

85 **4 Referenzen**

86 **AVG**

87 Allgemeines Verwaltungsverfahrensgesetz 1991 (AVG), idF BGBl. I Nr. 10/2004.
88 <http://ris.bka.gv.at/bundesrecht/>

89 **E-GovG**

90 E-Government-Gesetz (E-GovG), BGBl. I Nr. 10/2004.
91 <http://ris.bka.gv.at/bundesrecht/>

92 **SpecVE**

93 Arno Hollosi: X509 Zertifikatserweiterungen für die Verwaltung. Version 1.0.3 vom 21. 02.
94 2005.
95 <http://www.cio.gv.at/it-infrastructure/pki/X509ext-1.0.3-20050221.pdf>

5 Historie

Version	Datum	Kommentar
1.0.0	06.04.2005	Erstellt.
Ersteller		
Gregor Karlinger		