EGIZ E-Government Innovationszentrum

www.egiz.gv.at
E-Mail: post@egiz.gv.at
Telefon: ++43 (316) 873 5514
Fax: ++43 (316) 873 5520
Inffeldgasse 16a / 8010 Graz / Austria

Amtssignatur How-To

Ein Anwenderleitfaden zur Einführung der Amtssignatur

Dr. Thomas Rössler, EGIZ
Dr. Bernhard Karning, BKA

Graz, am 25. Juni 2008

Zusammenfassung:

Die Einführung der Amtssignatur – besonders vor dem Hintergrund der geänderten Rechtslage – geht für Behörden oft mit einer Reihe von Fragen einher. Diese Leitfaden soll daher eine erste Hilfestellung bieten und für die Einführung der Amtssignatur eine Anleitung liefern: von der Bestellung des Zertifikates bis hin zur Erstellung der Bildmarke und der Auswahl geeigneter technischer Signatur- und Prüfanwendungen.

Inhaltsverzeichnis

Abbildungsverzeichnis

1 Einleitung

Dieses Dokument stellt einen einfachen Leitfaden zur Einführung der Amtssignatur in einer Behörde dar. Es soll erste Anhaltspunkte liefern und vor allem einen zielgerichteten Weg aufzeigen, welche Schritte im Zuge der Einführung von Amtssignaturen zu beachten sind.

Obwohl der Leitfaden mit größter Bedachtnahme in Hinblick auf Vollständigkeit und Detailtiefe erstellt worden ist, können und sollen hier auch nur die wesentlichsten – gesetzlich geforderten – Maßnahmen angesprochen werden. Es ist daher in Ergänzung dazu unumgänglich, die weiterführenden Detail-Dokumente, -Spezifikationen und Anleitungen zu lesen und zu beachten.

Die nachfolgenden Abschnitte beschreiben die notwendigen Maßnahmen zur Einführung der Amtssignatur. Die Reihenfolge ist dabei nicht strikt zu sehen. Je nach Anwendungsfall ist es sogar ratsamer einer anderen Reihenfolge zu folgen, zum Beispiel zuerst die Auswahl der Signaturanwendung und danach Entscheidung bezgl. Art und Form des Signaturzertifikates vorzunehmen.

2 Beantragen eines Signaturzertifikates

Die Amtssignatur muss laut E-GovG (zumindest) eine fortgeschrittene Signatur gem. Vorgaben des SigG darstellen. Es eignen sich zur Amtssignatur daher nicht nur qualifizierte Signaturzertifikate, sondern auch solche, die für fortgeschrittene Signaturen verwendet werden können.

Bei fortgeschrittenen Signaturen kann nicht nur eine natürliche Person (eine befugte Person der Behörde), sondern auch die Behörde selbst als Signator auftreten (z.B. Marktgemeinde Kremsmünster). Mit qualifizierten Zertifikaten dürfen hingegen ausschließlich natürliche Personen (approbationsbefugte Person) signieren.

Das Signaturzertifikat muss die Verwaltungseigenschaft ausweisen. Das ist ein besonderes Attribut, das durch den Zertifizierungsdienst in das Zertifikat geschrieben wird. Geben Sie den Wunsch nach Eintragung der Verwaltungseigenschaft[1] (die OID dafür lautet 1.2.40.0.10.1.1.1) bereits bei der Bestellung des Zertifikates an. Sollte der Zertifizierungsdienst kein Standard-Produkt anbieten, das die Aufnahme der Verwaltungseigenschaft vorsieht, so klären Sie das zuvor im bilateralen Kontakt mit dem jeweiligen Zertifizierungsdiensteanbieter (ZDA) ab.

2.1 Bestellung:

2.1.1 Amtssignatur auf Basis einer qualifizierten Signatur:

A-TRUST ist der einzige ZDA in Österreich der qualifizierte Signaturzertifikate ausstellt. Diese sind jedenfalls kartenbasiert.

Bestellen Sie ein qualifiziertes Signaturzertifikat bei A-TRUST, wobei Sie bereits bei der Bestellung angeben müssen, dass Sie ein Zertifikat für Amtssignaturen benötigen. Daher wird Ihnen der Zertifizierungsdienst die Verwaltungseigenschaft in das Zertifikat aufnehmen (nach Gegenprüfung über den aufrechten Bestand).

[1] siehe Definition im Konventionsdokument „*Object Identifier der öffentlichen Verwaltung*“, http://www.ref.gv.at,

2.1.2 Amtssignatur auf Basis einer fortgeschrittenen Signatur:

Zertifikate für eine fortgeschrittene Signatur müssen nicht auf einer Signaturkarte gehalten werden. Derartige Zertifikate - bzw. die dazu gehörigen Schlüsseldaten - können auch als Software gehalten werden. Um dennoch die Sicherheit der Schlüsseldaten zu garantieren, sind entsprechende organisatorische Maßnahmen zu ergreifen.

Derartige Zertifikate eignen sich daher auch, um bspw. serverseitige Applikationen mit dem Signaturschlüssel auszustatten und so Massensignaturen abwickeln zu können.

Alternativ dazu können aber auch diese Zertifikate auf Basis einer Signaturkarte (Token) oder aber auf Basis eines sogenannten Hardware-Security-Moduls (HSM) ausgestellt werden. Setzen Sie sich dazu mit dem ZDA in Verbindung.

Für die Bestellung von softwarebasierten Zertifikaten müssen Sie in der Regel selbst die Schlüsseldaten erstellen. Die Bestellformulare der meisten ZDA sehen vor, dass Sie im Zuge der Bestellung Ihre öffentlichen Schlüsseldaten bereits bekannt geben müssen. Eine Anleitung und ein Werkzeug zur Erzeugung der Schlüsseldaten finden Sie im Web-Bereich der Arbeitsgruppe Bürgerkarte (http://www.ref.gv.at/Amtssignatur.1095.0.html). Auch hier muss bei der Bestellung bereits angeben werden, dass Sie ein Zertifikat für Amtssignaturen benötigen. Daher wird Ihnen der Zertifizierungsdienst die Verwaltungseigenschaft in das Zertifikat aufnehmen (nach Gegenprüfung über den aufrechten Bestand).

Eine Liste österreichischer Zertifizierungsdienstanbieter ist bspw. bei den Veröffentlichungen im Web-Angebot der Rundfunk und Telekom Regulierungs-GmbH (RTR) zu finden (http://www.rtr.at). Es ist aber im Detail zu prüfen und beim ZDA anzufragen, ob der ausgewählte ZDA auch Zertifikate mit Verwaltungseigenschaft ausstellt.

3 Erstellen einer Bildmarke

Eine weitere Voraussetzung der Amtssignatur ist deren Darstellung durch eine Bildmarke. Die Bildmarke Ihrer Amtssignatur hat im Internet gesichert veröffentlicht zu sein.

Die Bildmarke dient zur erleichterten Erkennbarkeit der Herkunft des amtssignierten Dokuments von einer Behörde. Insofern sollte die Bildmarke ihrer Behörde mit dieser unzweifelhaft in Verbindung gebracht werden können (z.B. Gemeindewappen, Corporate Design der Behörde).

Technisch muss die Bildmarke durch Ihre Signaturanwendung verarbeitet werden können. Wir empfehlen auf eines der gängigen Bildformate zurückzugreifen (JPEG, GIF). Die Größe der Bildmarke soll 120 x 120 Pixel betragen.

Abbildung 1: Beispiel einer Bildmarke.

Beispiel: Sie können eine Bildmarke auch kostenpflichtig unter http://www.fcemedia.com/amtssignatur/ bestellen.

Die von Ihnen gewählte Bildmarke muss letztlich in einem Format vorliegen, die auch von der von Ihnen verwendeten Signatursoftware verarbeitet werden kann. Die nachfolgend

gelisteten Signaturanwendungen der Plattform Digitales:Österreich verarbeiten Bildmarken im Format JPEG und GIF. Wie die Bildmarke in Ihre Signaturanwendung einzubringen ist, entnehmen Sie der jeweiligen Softwarebeschreibung.

4 Gesicherte Veröffentlichung der Bildmarke

Die von Ihnen verwendete Bildmarke muss gesichert als die Ihre im Internet veröffentlicht werden.

Die sichere Veröffentlichung im Internet erfolgt über eine für BürgerInnen einfach aufzufindende Internetseite Ihrer Organisation (vzgw. erreichbar unter der Hauptinternet-Adresse Ihrer Organisation).

Der Zugang zu dieser Seite soll nur gesichert, das heißt via https (SSL), möglich sein. Zur Absicherung des Zugangs verwenden Sie Ihr https-Serverzertifikat (ein SSL-Serverzertifikat – dieses ist nicht jenes, das Sie zur Amtssignatur verwenden) mit Verwaltungseigenschaft.

Ein Beispiel einer gesicherten Veröffentlichung der Bildmarke finden Sie auf der Web-Seite der Stammzahlenregisterbehörde unter folgendem Link:

https://www.stammzahlenregister.gv.at/site/6084/default.aspx

Alternativ dazu sind auch andere Arten einer gesicherten Veröffentlichung denkbar und möglich. So zum Beispiel kann die Veröffentlichung der Bildmarke auch im Rahmen eines amtssignierten PDF-Dokuments erfolgen. Ein Beispiel einer derartigen Veröffentlichung ist unter folgendem Link zu finden:

http://www.kremsmuenster.gv.at/amtssignatur

5 Auswahl der Amtssignatur-Software

Je nach zu Grunde liegender Infrastruktur und dem von Ihnen beabsichtigten Anwendungsszenario steht Ihnen heute schon eine Auswahl an Amtssignatur-Lösungen zur Verfügung. Die nachfolgende Tabelle gibt Ihnen einen Überblick über PDF-Signatur-Lösungen, die die Plattform Digitales:Österreich zur Verfügung stellt (dieser Überblick erhebt keinen Anspruch auf Vollständigkeit und wird auch bei Bedarf ergänzt werden).

Anwendung	Betriebsart		Signaturschlüssel		Anmerkungen / Bezug
	Lokal	Server	Software (pkcs#12)	Signaturkarte (Bürgerkarte)	
PDF-Signer	**X**	**–**	**+***	**X**	• Grafisch zu bedienendes Signaturwerkzug für Microsoft Windows. • Kann optional mit MOA-SS betrieben werden. MOA-SS kann unter Verwendung von Software-Schlüsseln oder eines HSM Signaturen erzeugen. • Bezug: OpenSource-Plattform[2]

[2] PDF-Signer: https://egovlabs.gv.at/frs/?group_id=10

PDF-Signer und Acrobat Plugin	**X**	**–**	**+***	**X**	• Auch diese Anwendung basiert auf der PDF-Signer Anwendung (siehe Beschreibung „PDF-Signer“). • In Ergänzung dazu wurde ein Signatur-Plugin für Adobe Acrobat (Professional oder Enterprise) entwickelt, dass das grafische Platzieren des Amtssignaturblocks per Drag&Drop ermöglicht. • Voraussetzung: das Adobe Acrobat Plugin kann nur in Verbindung mit Adobe Acrobat (Professional oder Enterprise) verwendet werden. • Bezug: OpenSource-Plattform[3]
PDF-AS für Adobe Reader	**X**	**–**	**–**	**X**	• Grafisch zu bedienendes Signaturwerkzeug für Microsoft Windows. • Diese Anwendung ermöglicht die grafische Positionierung von Amtssignaturblöcken im Rahmen des kostenfreien Adobe Reader. • Signatur nur unter Verwendung einer Signaturkarte (Bürgerkarte) möglich. • Bezug: EGIZ-Demo-Server[4]
MOA-AS	**–**	**X**	**X**	**–**	• Web-Service (SOAP-basiert) zur serverseitigen, automatischen Erstellung von Amtssignaturen. • Verwendet zur Erstellung elektronischer Signaturen MOA-SS. • Bezug: EGIZ-Demo-Server[5]
PDF-AS Entwickler-Bibliothek	**X**	**X**	**X**	**X**	• Java Entwicklungsbibliotheken zur Entwicklung eigener PDF-AS Lösungen. • Entwicklungsbibliotheken sind im Rahmen der OpenSource-Initiative der Plattform Digitales:Österreich frei verfügbar (http://egovlabs.gv.at). • Alle zuvor genannten Anwendungen basieren auf dieser Java-Bibliothek.

[3] PDF-Signer mit Adobe Acrobat Plugin: https://egovlabs.gv.at/frs/?group_id=10

[4] PDF-Signatur mit Adobe Reader: http://demo.egiz.gv.at/plain/projekte/signatur_im_e_government/pdf_signatur

[5] MOA-AS: Spezifikation und Prototyp: http://demo.egiz.gv.at/plain/projekte/signatur_im_e_government/moa_amtssignatur_moa_as

					• Bezug: OpenSource-Plattform[6]

Anmerkungen zur Tabelle:

*) Wird MOA-SS zur Signaturerstellung verwendet, so können sowohl softwarebasierte Schlüsseldaten (in Form von PKCS#12-Dateien, etc.) oder auch in Hardware-Security-Modulen gehaltene Schlüssel herangezogen werden.

6 Hinweis auf die Amtssignatur

Das Dokument muss einen Hinweis darauf enthalten, dass es amtssigniert wurde (zB „Dieses Dokument wurde amtssigniert“). Dieser Hinweis kann auch im Signaturblock vorkommen (siehe Überschrift „Layout des Signaturblocks“).

7 Layout des Signaturblocks

Um ein möglichst einheitliches Erscheinungsbild aller Behörden gegenüber den BürgerInnen sicherzustellen, werden die Varianten für die rechtskonforme Darstellung des Signaturblocks im Dokument „Layout Amtssignatur“[7] empfohlen. Je nachdem, ob die Prüfung des Ausdrucks eines amtssignierten Dokuments mittels Rückführbarkeit oder Verifizierung gelöst wird oder ob die Behörde im Rahmen der Hoheitsverwaltung oder der Privatwirtschaftsverwaltung handelt, stehen mehrere Darstellungsformen zu Auswahl.

Signaturwert	nk7EWvq+kuTrlfklYlPI7iRCgZwUHpAYrjGncCqyCgTlamKL4I2oQ9CMK/Btusmf	
REPUBLIK ÖSTERREICH .BPD Demo @ AMTSSIEGEL	Unterzeichner	Amtsdirektor Dr. Max Mustermann
	Datum/Zeit-UTC	2008-03-17T12:03:07Z
	Aussteller-Zertifikat	CN=a-sign-Premium-Sig-02,OU=a-sign-Premium-Sig-02,O=A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH,C=AT
	Serien-Nr.	238730
	Methode	urn:pdfsigfilter:bka.gv.at:text:v1.1.0
	Parameter	etsi-bka-1.0@1205755387-63974421@893-13387-0-23326-29425
Prüfinformation	Informationen zur Prüfung der elektronischen Signatur finden Sie unter: https://demo.a-sit.at/el_signatur/verification Informationen zur Prüfung des Ausdrucks finden Sie unter: https://demo.a-sit.at/el_signatur/	
Hinweis	Dieses Dokument wurde amtssigniert. Auch ein Ausdruck dieses Dokuments hat gemäß § 20 E-Government-Gesetz die Beweiskraft einer öffentlichen Urkunde.	

Abbildung 2: Beispiel eines Signaturblocks gem. den Vorgaben der Layout-Definition.

Wie das Aussehen des Signaturblocks in der jeweiligen Signaturapplikation zu konfigurieren ist, entnehmen Sie bitte der Anleitung.

Die von der Plattform Digitales:Österreich zur Verfügung gestellten Signaturanwendungen sind mit Signaturprofilen nach den Standard-Layout-Vorgaben bereits vorkonfiguriert. Es sind in der Regel nur minimale Anpassungen nötig. Die grafisch zu bedienenden Signaturanwendungen (zum Beispiel PDF-Signer oder das Adobe Acrobat Plugin) bieten die Möglichkeit die Anpassungen sowie das Eintragen Ihrer persönlichen Bildmarke über eine grafische Konfigurationsoberfläche vorzunehmen.

[6] PDF-AS Entwicklungsbibliothek und –daten: https://egovlabs.gv.at/projects/pdf-as/

[7] Das Dokument „Layout Amtssignatur - Spezifikation“ ist im Web-Bereich der AG-Bürgerkarte zu finden: http://www.ref.gv.at/Amtssignatur.1095.0.html

8 Prüfanwendung für das amtssignierte elektronische Dokument

Die Behörde hat entsprechende Informationen bereitzustellen, wie die ausgestellten Amtssignaturen geprüft werden können.

Welches technische Werkzeug dazu herangezogen werden kann, hängt vordergründig von der verwendeten Signaturtechnologie/-anwendung ab.

Alle von der Plattform Digitales:Österreich zur Verfügung gestellten Signaturanwendungen basieren auf der PDF-AS Technologie und beziehen sich in der Standardkonfiguration auf das definierte Signaturblock-Layout. Alle so und damit erzeugten Signaturen können auch durch Signaturprüfanwendungen Dritter geprüft werden. So zum Beispiel stellt das Zentrum für Sichere Informationstechnologie Austria (A-SIT) unter http://www.buergerkarte.at eine Prüfservice zur Verfügung, das zur unabhängigen Prüfung von PDF-Amtssignaturen (PDF-AS Technologie) herangezogen werden kann. Ein Link http://signaturpruefung.gv.at wurde eingerichtet, um eine stabile Referenz auf einen Prüfdienst zu haben.

9 Prüfanwendung für den Ausdruck des amtssignierten elektronischen Dokuments

Für die Prüfung des Ausdruckes kann die Behörde zwischen den Verfahren der Rückführung oder der Verifizierung wählen.

9.1 Rückführung

Die Behörde hat dazu einen Hinweis auf die Fundstelle im Internet, wo das Verfahren der Rückführung des Ausdrucks in das elektronische Dokument und die anwendbaren Prüfmechanismen enthalten sind, im Dokument anzubringen.

Die Rückführung ist ein technischer Prozess, der es ermöglicht, das ursprünglich elektronisch signierte Dokument auf Basis eines Papierausdruckes zu rekonstruieren. Die auf Basis der PDF-AS Technologie entwickelten Signaturapplikationen bieten für sogenannte textuelle Signaturen (d.h. es wird nur der textuelle Inhalt des Dokumentes signiert) den Weg der Rückführung an. Dabei kann die Prüfanwendung nach Eingabe des blanken Textes – bspw. auf Basis einer Papiervorlage – das ursprüngliche elektronisch vorliegende signierte Dokument wiederherstellen und prüfen.

9.2 Verifizierung

Hier hat die Behörde einen entsprechenden Hinweis auf das Verfahren der Verifizierung im Dokument anzubringen. Der Hinweis auf das Verfahren der Verifizierung kann etwa eine Angabe einer Kontaktadresse der Behörde sein, bei der der Ausdruck auf seine Echtheit geprüft werden kann. Freilich muss die Behörde sicherstellen, dass die Verifizierung auch tatsächlich durch das angegebene Verfahren erfolgen kann (z.B.: Kontaktadresse besteht auch noch nach Jahren).

Dokumentenhistorie

Version:	Datum:	Kommentar:
1.0.0	20.06.2007	- Erstellt.
Autor: Thomas Rössler, EGIZ Bernhard Karning, BKA		