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

Layout Amtssignatur

Spezifikation

Graz, am 21.Juni 2007

DI Thomas Rössler – thomas.roessler@iaik.tugraz.at

Das Dokument legt das Aussehen von Amtssignatur im Detail fest, um einerseits ein einheitliches Auftreten gegenüber den BürgerInnen zu erreichen, andererseits um die automatisierte Rekonstruktion von PDF-Amtssignaturen zu erleichtern.

Inhalt

1 Standardisiertes Layout von Amtssignaturblöcken

Das Layout von Amtssignaturblöcken soll ein möglichst einheitliches sein, um einerseits einen konsistenten Auftritt gegenüber den BürgerInnen zu erreichen, und andererseits um die technische Rekonstruktion von Amtssignaturen zu erleichtern. Zudem trägt dieses Papier all jenen Anfragen Rechnung, in denen um genauere Vorgaben zum Aussehen von Amtssignaturblöcken – insbesondere in Verbindung mit der Applikation PDF-Amtssignaturen – gebeten wurde.

Die in diesem Papier spezifizierten Layouts sind vorrangig zur Anwendung in Verbindung mit der PDF-Amtssignaturapplikation (PDF-AS) entwickelt worden. Darüberhinaus können und sollen diese Layouts aber auch in Verbindung mit anderen Amtssignaturtechnologien ihre Anwendung finden. Die Spezifikation wurde daher bewusst allgemein und technologieneutral gehalten.

Die hier vorgestellten Anforderungen basieren auf dem zum Zeitpunkt der Spezifikationserstellung anwendbaren E-Government Gesetzt [1]. In den nächsten Monaten ist eine Novellierung des E-Government Gesetzes zu erwarten; diese Novellierung wird ggf. auch unmittelbare Auswirkungen auf die optische Repräsentation von Amtssignaturen mit sich bringen. Daher ist diese Spezifikation laufend, jedoch insbesondere in Bezug auf die unmittelbar zu erwartenden Novellierung, zu aktualisieren.

2 Grundlage

Das E-Government Gesetz [1] definiert das Minimum der anzuzeigenden Inhalte einer Amtssignatur wie folgt:

> [..]
>
> ***Besonderheiten elektronischer Aktenführung Amtssignatur***
>
> *§ 19. (1) Die Amtssignatur ist eine elektronische Signatur im Sinne des Signaturgesetzes, deren Besonderheit durch ein entsprechendes Attribut im Signaturzertifikat ausgewiesen wird.*
>
> *(2) Die Amtssignatur dient der erleichterten Erkennbarkeit der Herkunft eines Dokuments von einer Behörde. Sie darf daher ausschließlich von Behörden unter den näheren Bedingungen des Abs. 3 bei der elektronischen Unterzeichnung und bei der Ausfertigung der von ihnen erzeugten Dokumente verwendet werden.*
>
> *(3) Die Darstellung der Amtssignatur in Ansichten elektronischer Dokumente geschieht durch eine Bildmarke, die die Behörde im Internet als die ihre gesichert veröffentlicht hat. Neben der Bildmarke sind in der Ansicht zumindest die Seriennummer sowie der Name und das Herkunftsland des Zertifizierungsdiensteanbieters und der eigentliche Signaturwert anzugeben. Die Signaturprüfung muss über die Rückführung der Ansicht des gesamten Dokuments in eine Form, die die Signaturprüfung zulässt, möglich sein. Jene zusätzlichen Informationen, die für die Wiederherstellung des elektronischen Dokuments aus der Ansicht notwendig sind, hat der Aussteller des Dokuments ebenfalls im Internet gesichert zu veröffentlichen.*
>
> [..] [1]

Absatz (3) legt für die Darstellung folgende Mindestinhalte fest:

a) eine Bildmarke
b) Seriennummer des zur Signatur verwendeten Zertifikates
c) Name und Herkunftsland des Zertifizierungsdiensteanbieters (Herausgeber des Zertifikates)
d) Signaturwert

Auf dieser Grundlage wurden die nachfolgend vorgeschlagenen Amtssignaturblöcke entworfen.

3 Amtssignaturblock für die öffentliche Verwaltung

Es werden zwei Amtssignaturblöcke standardisiert: einer mit deutschen Feldbezeichnungen und einer mit englischen Feldbezeichnungen.

Dieses Dokument verwendet die Schlüsselwörter MUSS, DARF NICHT, ERFORDERLICH, SOLLTE, SOLLTE NICHT, EMPFOHLEN, DARF, und OPTIONAL zur Kategorisierung der Anforderungen. Diese Schlüsselwörter sind analog zu ihren englischsprachigen Entsprechungen MUST, MUST NOT, REQUIRED, SHOULD, SHOULD NOT, RECOMMENDED, MAY, und OPTIONAL zu handhaben, deren Interpretation in RFC 2119 festgelegt ist.

3.1 Amtssignaturblock (Deutsch)

Die Struktur und Feldbezeichnungen werden wie folgt festgelegt:

Signaturwert	XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX	
	**Unterzeichner**	XXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
	Datum/Zeit-UTC	XXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
	Aussteller-Zertifikat	XXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
	Serien-Nr.	XXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
	Methode	XXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
	Parameter	XXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
Prüfhinweis	XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX	

Feldbezeichnungen und deren Bedeutung:

Die Feldbezeichner in der Spalte „Feld“ sind sowohl in Deutsch (oberer Bezeichner in der Tabellenzelle) als auch in Englisch (unterer Bezeichner in der Tabellenzelle) angeführt.

#	Feld	M/K/S	Beschreibung
1	**Signaturwert** **Signature Value**	MUSS	Signaturwert; ist erforderlich.
2	**Unterzeichner** **Signatory**	KANN	Name des Unterzeichners; ist ein optionales Feld und kann zur Verdeutlichung des Unterzeichners verwendet werden.
3	**Datum/Zeit-UTC** **Date/Time-UTC**	MUSS	Datum und Zeitpunkt der Signatur (im UTC-Format); ist erforderlich.
4	**Aussteller-Zertifikat** **Issuer-Certificate**	MUSS	Angaben zum Aussteller des Signaturzertifikates, zumindest dessen Namen und Herkunftsland; ist erforderlich.
5	**Serien-Nr.** **Serial-No.**	MUSS	Seriennummer des Signaturzertifikates; ist erforderlich.
6	**Methode** **Method**	KANN	Optionales Element zur näheren Kennzeichnung des verwendeten Signaturverfahrens. Dieses Element kann verwendet werden, um bspw. den angewandten Signaturstandard zu identifizieren. Dieses Feld ist besonders dann zu verwenden, wenn die Amtssignatur auch auf Basis eines Ausdruckes rückführbar sein soll.
7	**Parameter** **Parameter**	KANN	Optionales Element zur Formulierung von für das/den angewandte Signaturverfahren/-standard notwendigen näheren Bestimmungsparametern. Dieses Feld ist sozusagen eine detailliertere und zusätzliche Möglichkeit, weitere Signaturparameter anzuführen; diese sind vom angewandten Signaturstandard bzw. von der verwendeten Signaturtechnologie abhängig. Dieses Feld ist besonders dann zu verwenden, wenn die Amtssignatur auch auf Basis eines Ausdruckes rückführbar sein soll.
8	**Prüfhinweis**	SOLL	Ein einfach verständlicher Hinweis für BürgerInnen, wie man die gegenständliche Amtssignatur verifizieren kann. Hierin kann bspw. ein Verweis auf ein Prüfservice im Internet beschrieben werden. Dieses Feld soll bei einem Signaturblock

	Verification		immer verwendet werden, um den BürgerInnen eine Unterstützung bei der Prüfung zu bieten. Hierin soll jedenfalls ein Hinweis stehen, ob und wie die gegenständliche Signatur auf Basis eines Papierausdruckes rekonstruiert, rückgeführt und geprüft werden kann.
9	[Bildmarke] keine textuelle Bezeichnung	MUSS	Die Bildmarke ist das optische und bildhafte Pendant zum Rundsiegel; ist erforderlich. Informationen zur Gestaltung und Bestellung von Bildmarken sind unter http://.... zu finden.

3.2 Amtssignaturblock (Englisch)

Die Struktur und Feldbezeichnungen werden wie folgt festgelegt:

Signature Value	XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX	
	**Signatory**	XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
	Date/Time-UTC	XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
	Issuer-Certificate	XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
	Serial-No.	XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
	Method	XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
	Parameter	XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
Verification	XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX	

Feldbezeichnungen und deren Bedeutung:

Siehe Tabelle in Abschnitt 3.1; die Feldbezeichnungen dort sind sowohl in Deutsch als auch in Englisch definiert.

4 Signaturblock für andere Anwendungsbereiche

Das Layout und die Struktur der Amtssignaturblöcke SOLL identisch und analog auch fernab von hoheitlichen Tätigkeiten der öffentlichen Verwaltung Anwendung finden. Das heißt, dass sowohl im privatwirtschaftlichen Tätigkeitsfeld der öffentlichen Verwaltung, als auch im privaten Umfeld generell Signaturinformationen auf diese Art und Weise dargestellt werden sollen. Es gelten daher die selben Struktur- und Layoutempfehlungen wie in Abschnitt 3.1 und 3.2 definiert.

Als Bildmarke wird für derartige Anwendungsfälle die folgende empfohlen:

Diese wird in entsprechender Qualität unter http://... veröffentlicht.

5 Beispiele

Dieser Abschnitt zeigt anhand einiger einfacher Beispiele, wie Signaturblöcke laut der vorliegenden Spezifikation aussehen können. Diese Beispiele repräsentieren allerdings nicht die volle Bandbreite an Möglichkeiten und erheben keinen Anspruch auf Vollständigkeit.

5.1 Signaturblock (Deutsch)

Die nachfolgenden Beispiele wurden mit PDF-AS unter Verwendung des folgenden Profils erzeugt (Muster-Profil für PDF-AS Applikation, ab Version 2.0.0):

```
#####################################################
# Signatur Profil (Deutsch)

sig_obj.SIGNATUR.start_text=Signaturwert
sig_obj.SIGNATUR.description=Standardsignaturblock Deutsch

sig_obj.SIGNATUR.key.SIG_VALUE=Signaturwert
sig_obj.SIGNATUR.key.SIG_NAME=Unterzeichner
sig_obj.SIGNATUR.key.SIG_DATE=Datum/Zeit-UTC
sig_obj.SIGNATUR.key.SIG_ISSUER=Aussteller-Zertifikat
sig_obj.SIGNATUR.key.SIG_NUMBER=Serien-Nr.
sig_obj.SIGNATUR.key.SIG_KZ=Methode
sig_obj.SIGNATUR.key.SIG_ID=Parameter
sig_obj.SIGNATUR.key.SIG_META=Prüfhinweis


sig_obj.SIGNATUR.value.SIG_META=Prüfservice:      http://demo.a-
sit.at/el_signatur/pdf-as/verify
sig_obj.SIGNATUR.value.SIG_LABEL=./cfg/bildmarke.jpg

#---------------------- MAIN TABLE -------------------------
sig_obj.SIGNATUR.table.main.1=SIG_VALUE-cv
sig_obj.SIGNATUR.table.main.2=SIG_LABEL-i|TABLE-info
sig_obj.SIGNATUR.table.main.3=SIG_META-cv

sig_obj.SIGNATUR.table.main.ColsWidth=1 5
sig_obj.SIGNATUR.table.main.Style.bgcolor=245 245 240
sig_obj.SIGNATUR.table.main.Style.padding=3
sig_obj.SIGNATUR.table.main.Style.border=0.1
sig_obj.SIGNATUR.table.main.Style.halign=left
```

```
sig_obj.SIGNATUR.table.main.Style.valign=middle
sig_obj.SIGNATUR.table.main.Style.font=HELVETICA,8,NORMAL
sig_obj.SIGNATUR.table.main.Style.valuefont=COURIER,8,NORMAL

#---------------------- INFO TABLE -------------------------
sig_obj.SIGNATUR.table.info.ColsWidth=1 4
sig_obj.SIGNATUR.table.info.1=SIG_NAME-cv
sig_obj.SIGNATUR.table.info.2=SIG_DATE-cv
sig_obj.SIGNATUR.table.info.3=SIG_ISSUER-cv
sig_obj.SIGNATUR.table.info.4=SIG_NUMBER-cv
sig_obj.SIGNATUR.table.info.5=SIG_KZ-cv
sig_obj.SIGNATUR.table.info.6=SIG_ID-cv
```

5.1.1 Beispiel: Textuelle PDF-Signatur

Beispiel eines Signaturblockes mit den optionalen Feldern „Parameter“, „Methode“ und „Unterzeichner“.

Signaturwert	sGnbG4pIymM6HRBPowty7NrmaSy8WwBR8ATwEtS/xDyM3SQ3xNLbBQ4K+2toH2vU	
SIGNATURINFORMATIONEN DIGITALES ÖSTERREICH	Unterzeichner	C=AT, OU=VSig, O=Hauptverband österr. Sozialvers., CN=Thomas Rössler
	Datum/Zeit-UTC	2007-06-25T11:38:51Z
	Aussteller-Zertifikat	C=AT,O=Hauptverband österr. Sozialvers.,CN=VSig CA 2
	Serien-Nr.	171767978488753704510848871729686142359 87
	Methode	urn:pdfsigfilter:bka.gv.at:text:v1.0.0
	Parameter	etsi-bka-1.0@1182771532-1990609@4480-7742-20016-7558-11510
Prüfhinweis	Prüfservice: http://demo.a-sit.at/el_signatur/pdf-as/verify	

5.1.2 Beispiel: Textuelle PDF-Signatur

Beispiel eines Signaturblockes mit den optionalen Feldern „Unterzeichner“ und „Methode“.

Signaturwert	LybIR0LIt/L9pvMGA1zyEz0ewmisBvuKXGi26ZqA5C28BzzfS4A6m8keBh5tzHT+1oM1euCrEMsABlpbPYUY 8h0RKM77skAeGlaFpi8Bszl98bDOr5lsHN2iGr4veHsdVMVtEbjj0xVgcrczueyfVLb9dwGODxn3TiKCDXlN uKW=	
SIGNATURINFORMATIONEN DIGITALES ÖSTERREICH	Unterzeichner	CN=Demo-Amtssignatur, OU=E-Government Innovation Center (EGIZ), O=IAIK TU-Graz, C=AT
	Datum/Zeit-UTC	2007-06-25T11:37:43
	Aussteller-Zertifikat	CN=IAIK Test CA Sign,OU=IAIK Test CA,OU=Insitute for Applied Information Processing and Communications,O=GRAZ UNIVERSITY OF TECHNOLOGY,C=AT
	Serien-Nr.	108917544637412104297303986745969744066161700059
	Methode	urn:pdfsigfilter:bka.gv.at:text:v1.0.0
Prüfhinweis	Prüfservice: http://demo.a-sit.at/el_signatur/pdf-as/verify	

5.2 Signaturblock (Englisch)

Die nachfolgenden Beispiele wurden mit PDF-AS unter Verwendung des folgenden Profils erzeugt (Muster-Profil für PDF-AS Applikation, ab Version 2.0.0):

```
#####################################################
# Signatur Profil (Englisch)

sig_obj.SIGNATURE.start_text=Signaturwert
sig_obj.SIGNATURE.description=Standardsignaturblock Deutsch
```

```
sig_obj.SIGNATURE.key.SIG_VALUE=Signature Value
sig_obj.SIGNATURE.key.SIG_NAME=Signatory
sig_obj.SIGNATURE.key.SIG_DATE=Date/Time-UTC
sig_obj.SIGNATURE.key.SIG_ISSUER=Issuer-Certificate
sig_obj.SIGNATURE.key.SIG_NUMBER=Serial-No.
sig_obj.SIGNATURE.key.SIG_KZ=Method
sig_obj.SIGNATURE.key.SIG_ID=Parameter
sig_obj.SIGNATURE.key.SIG_META=Verification


sig_obj.SIGNATURE.value.SIG_META=Service:          http://demo.a-
sit.at/el_signatur/pdf-as/verify
sig_obj.SIGNATURE.value.SIG_LABEL=./cfg/bildmarke.jpg

#---------------------- MAIN TABLE -------------------------
sig_obj.SIGNATURE.table.main.1=SIG_VALUE-cv
sig_obj.SIGNATURE.table.main.2=SIG_LABEL-i|TABLE-info
sig_obj.SIGNATURE.table.main.3=SIG_META-cv

sig_obj.SIGNATURE.table.main.ColsWidth=1 5
sig_obj.SIGNATURE.table.main.Style.bgcolor=245 245 240
sig_obj.SIGNATURE.table.main.Style.padding=3
sig_obj.SIGNATURE.table.main.Style.border=0.1
sig_obj.SIGNATURE.table.main.Style.halign=left
sig_obj.SIGNATURE.table.main.Style.valign=middle
sig_obj.SIGNATURE.table.main.Style.font=HELVETICA,8,NORMAL
sig_obj.SIGNATURE.table.main.Style.valuefont=COURIER,8,NORMAL

#---------------------- INFO TABLE -------------------------
sig_obj.SIGNATURE.table.info.ColsWidth=1 4
sig_obj.SIGNATURE.table.info.1=SIG_NAME-cv
sig_obj.SIGNATURE.table.info.2=SIG_DATE-cv
sig_obj.SIGNATURE.table.info.3=SIG_ISSUER-cv
sig_obj.SIGNATURE.table.info.4=SIG_NUMBER-cv
sig_obj.SIGNATURE.table.info.5=SIG_KZ-cv
sig_obj.SIGNATURE.table.info.6=SIG_ID-cv
```

5.2.1 Beispiel: Textuelle PDF-Signatur

Beispiel eines Signaturblockes mit den optionalen Feldern „Parameter“, „Method“ und „Signatory“.

Signature Value	BQyRSsDOJQWj77/WDXmTkHnmo1mnoouPCkgrUtj1kA8e5m+us4SMnT5BomhSifnu	
	Signatory	C=AT, OU=VSig, O=Hauptverband österr. Sozialvers., CN=Thomas Rössler
	Date/Time-UTC	2007-06-25T12:18:44Z
	Issuer-Certificate	C=AT,O=Hauptverband österr. Sozialvers.,CN=VSig CA 2
	Serial-No.	171767978488753704510848871729686142359 87
	Method	urn:pdfsigfilter:bka.gv.at:text:v1.0.0
	Parameter	etsi-bka-1.0@1182773924-4383140@12295-5799-6738-17691-19983
Verification	Service: http://demo.a-sit.at/el_signatur/pdf-as/verify	

5.2.2 Beispiel: Textuelle PDF-Signatur

Beispiel eines Signaturblockes mit den optionalen Feldern „Signatory“ und Method“.

Signature Value	lwz/jOPYCiAOBVrYjTN4BAgSwxeKl2xBUwfOPp9BWsezqiYLE3bwlvrswRhHMz4hN7DzQQoc2wJhz+BLhdLmBMH/XVVghJJ9ON9NSYIVlTSpUBT3KwauTwRnxkYdftAJSv41kM3oQznzCMLUZuYRtah5FiaIcnxZO0M8Uo2a5vU=	
SIGNATURE DIGITAL AUSTRIA	Signatory	CN=Demo-Amtssignatur, OU=E-Government Innovation Center (EGIZ), O=IAIK TU-Graz, C=AT
	Date/Time-UTC	2007-06-25T12:17:37
	Issuer-Certificate	CN=IAIK Test CA Sign,OU=IAIK Test CA,OU=Insitute for Applied Information Processing and Communications,O=GRAZ UNIVERSITY OF TECHNOLOGY,C=AT
	Serial-No.	108917544637412104297303986745969744066161700059
	Method	urn:pdfsigfilter:bka.gv.at:text:v1.0.0
Verification	service: http://demo.a-sit.at/el_signatur/pdf-as/verify	

6 Referenzen

[1] BUNDESGESETZBLATT FÜR DIE REPUBLIK ÖSTERREICH: Bundesgesetz über Regelungen zur Erleichterung des elektronischen Verkehrs mit öffentlichen Stellen (E-Government-Gesetz – E-GovG). BGBl. I Nr. 10/2004 vom 27. 2. 2004.

Dokumentenhistorie

Version:	**Datum:**	**Kommentar:**
1.0.0D	21.06.2007	- Erstellt.
Autor: Thomas Rössler, EGIZ		
Version:	**Datum:**	**Kommentar:**
1.0.0	25.06.2007	- Signature Value - Ergänzung um Beispiele
Autor: Thomas Rössler, EGIZ		