

Bildung von Stammzahl und bereichsspezifischem Personenkennzeichen (bPK)		Konvention
		SZ-bPK-Algo - 1.1.1
		Ergebnis der AG
Kurzbeschreibung	<p>Das E-Government-Gesetz (E-GovG) definiert die Begriffe Stammzahl und bereichsspezifisches Personenkennzeichen (bPK). In diesem Dokument wird die dazu gehörende Verfahrensvorschrift definiert.</p> <p><i>Dieses Dokument wurde im Zuge der Konsolidierung der E-Government Spezifikationen und Konventionen in einen formellen Status übergeführt. Editorielle Änderungen, wie das Hinzufügen des Deckblattes, wurden vorgenommen; inhaltlich blieb das Dokument unverändert.</i></p>	
Autor(en):	Arno Hollosi BKA/CIO Rainer Hörbe (BMI-SUZMR)	Projektteam / Arbeitsgruppe AG Bürgerkarte
Beiträge von:		

Vorgelegt am **31.01.2007**

Abgelehnt von:

Zur Kenntnis genommen von:

Anregungen von:

Angenommen von:

(mit der Option von allen bzw. allen übrigen Ländern bei ablehnenden Stellungnahmen)

Inhalt

Einleitung.....	3
Ermittlung der Stammzahl	4
Algorithmus	4
Beispiel	4
Ermittlung des bPK.....	5
Algorithmus	5
Ermittlung des bPK für Organwalter	6
Algorithmus	6
Beispiel	6
Ermittlung des Wirtschafts-bPK.....	7
Algorithmus	7
Verschlüsselung des bPK.....	9
Algorithmus	9
Referenzen	11
Historie	12

Einleitung

Das E-Government Gesetz (E-GovG), welches mit 1.3.2004 in Kraft trat, definiert die Stammzahl, das bereichsspezifische Personenkennzeichen und deren Bildung wie folgt:

§2 Z8 "Stammzahl": eine zur Identifikation von natürlichen und juristischen Personen und sonstigen Betroffenen herangezogene Zahl, die demjenigen, der identifiziert werden soll, eindeutig zugeordnet ist und hinsichtlich natürlicher Personen auch als Ausgangspunkt für die Ableitung von (wirtschafts)bereichsspezifischen Personenkennzeichen (§§ 8 und 14) benützt wird;

§6 (2) Für natürliche Personen, die im Zentralen Melderegister einzutragen sind, wird die Stammzahl durch eine mit starker Verschlüsselung gesicherte Ableitung aus ihrer ZMR-Zahl (§ 16 Abs. 1 des Meldegesetzes 1991, BGBl. Nr. 9/1992) gebildet. Für alle anderen natürlichen Personen ist ihre Ordnungsnummer im Ergänzungsregister (Abs. 4) für die Ableitung der Stammzahl heranzuziehen.

§9 (1) Das bereichsspezifische Personenkennzeichen wird durch eine Ableitung aus der Stammzahl der betroffenen natürlichen Person gebildet. Die Identifikationsfunktion dieser Ableitung ist auf jenen staatlichen Tätigkeitsbereich beschränkt, dem die Datenanwendung zuzurechnen ist, in der das Personenkennzeichen verwendet werden soll (bereichsspezifisches Personenkennzeichen, bPK).

§9 (3) Die zur Bildung des bPK eingesetzten mathematischen Verfahren (Hash-Verfahren über die Stammzahl und die Bereichskennung) werden von der Stammzahlenregisterbehörde festgelegt.

Diese Spezifikation beschreibt die Algorithmen zur Bildung der Stammzahl und des bereichsspezifischen Personenkennzeichens. Sie bezieht sich nur auf natürliche Personen, da für nicht-natürliche Personen keine Ableitungen aus den Basisbegriffen (z.B. Firmenbuchnummer, Nummer im Vereinsregister) vorgesehen sind.

Diese Spezifikation macht die Spezifikation „Ableitung für die bereichsspezifische Personenkennzeichnung“ Version 1.0.2 vom 2003-04-16 **obsolet**.

Ermittlung der Stammzahl

Grundlage für die Ermittlung der Stammzahlen für natürliche Personen sind für

- o Personen, die in Österreich meldepflichtig sind, die Zahl der Eintragung im Zentralen Melderegister (ZMR-Zahl) (§6(2) E-GovG)
- o alle anderen Personen die Zahl der Eintragung im Ergänzungsregister (ER-Zahl) (§6(4) E-GovG)

Diese natürliche Personen eindeutig identifizierenden Zahlen (ZMR-Zahl oder ER-Zahl) werden im Folgenden als Basiszahl bezeichnet.

Algorithmus

1. Ausgangsdaten: Basiszahl (12 Dezimalstellen)
2. Umwandeln in Binärdarstellung (5 Byte)
3. Vergrößerung der Berechnungsbasis auf 128 Bit (16 Byte) mittels folgendem Format: >> Basiszahl Seed Basiszahl Basiszahl << Seed ist ein geheimer, konstanter 8-Bit Wert, der nur der Stammzahlregisterbehörde bekannt ist.
4. Die binäre Repräsentation wird mittels Triple-DES [DES] im CBC-Modus verschlüsselt. Der dazu verwendete Schlüssel ist geheim und nur der Stammzahlregisterbehörde bekannt.
5. Base64 [RFC2054] Kodierung des Ergebnisses (schließt Kodierung in ASCII [ISO-646] mit ein).

Beispiel

Basiszahl	000247681888 (Bsp: ZMR-Zahl, 12-stellige Dezimalzahl)
Binärdarstellung	00 0E C3 53 60 (5 Byte, Darstellung hexadezimal)
Verbreiterung auf 128 Bit	00 0E C3 53 60 FF 00 0E C3 53 60 00 0E C3 53 60 (16 Byte, Seed-Wert beispielhaft auf 'FF' gesetzt)
Triple-DES Verschlüsselung, hexadezimal	42 AD 37 74 FA E0 70 7B 31 DC 6D 25 29 21 FA 49 (16 Byte)
Stammzahl, Base64	Qq03dPrgcHsx3G0lKSH6SQ== (24 Zeichen)

Ermittlung des bPK

Das bPK wird in zwei Schritten ermittelt. Der erste Schritt ist die Bildung einer ISO-8859-1 Zeichenkette aus der Stammzahl und dem Bereich. Der zweite Schritt ist die sichere kryptographische Einwegableitung dieser Zeichenkette welcher das bPK ergibt.

Algorithmus

1. Ausgangsdaten:
 - o Stammzahl, base64 kodiert
 - o Bereich: ISO-8859-1 Zeichenfolge der Abkürzung des Bereiches laut Bereichsabgrenzungsverordnung des Bundeskanzleramtes (in der Regel 2, maximal 5 Zeichen in Großbuchstaben)
2. Bildung der Zeichenkette als Verbindung (string concatenation) aus Stammzahl und „+“ (als Zeichen) und URN-Präfix und Bereichskürzel.
3. Über die entstehende Zeichenkette (den entstehenden String) wird der SHA-1 Algorithmus wie in FIPS PUB 180-1 [SHA-1] beschrieben berechnet. Das Resultat dieser Berechnung ist eine 160bit-Zahl (5x32 bit)
4. Diese 160bit-Zahl kann für programminterne Zwecke direkt verwendet werden, bei Übertragung bzw. in schriftlicher Form ist diese Zahl Base64 zu kodieren.

URN-Präfix

URN-Präfix := "urn:publicid:gv.at:cdid+"

Der URN-Präfix ist definiert über:

- o URN (RFC 2141 / RFC 2396)
- o URN für Public Identifier (RFC 3151)
- o Owner: gv.at
- o Class: cdid+XXXXX (cdid = context dependent id)

Beispiel

Stammzahl, Base64	Qq03dPrgcHsx3G0lKSH6SQ== (24 Zeichen)
Bereichskürzel	BW (ISO-8859-1, Beispiel: Bauen und Wohnen)
Eingangsdaten für die Hashberechnung	Qq03dPrgcHsx3G0lKSH6SQ==+urn:publicid:gv.at:cdid+BW
Hashwert nach SHA-1, hexadezimal	8FF3717514 21A7EB4DC8 4F56847741 498BB2DE10 (5 x 32bit; Darstellung hexadezimal)
BPK, Base64	j/NxdRQhp+tNyE9WhHdBSYuy3hA= (28 Zeichen)

Ermittlung des bPK für Organwalter

Das E-Government Gesetz sieht ein spezielles (rückführbares) Personenkennzeichen für Organwalter (innerhalb der Verwaltung) vor.

§ 13 (1) Bereichsspezifische Personenkennzeichen sind durch nicht-umkehrbare Ableitungen aus der Stammzahl zu bilden. Dies gilt im Interesse der Nachvollziehbarkeit staatlichen Handelns nicht für bereichsspezifische Personenkennzeichen, die ausschließlich im Zusammenhang mit der Tätigkeit einer Person als Organwalter verwendet werden.

Diese rückführbaren bPK können nur durch Abfrage des Stammzahlenregisters gebildet werden. Es wird eine symmetrische Triple-DES Verschlüsselung mit einem geheimen Schlüssel durchgeführt.

Algorithmus

1. Ausgangsdaten: Stammzahl in Binärrepräsentation (16 Byte)
2. Die binäre Repräsentation wird mittels Triple-DES im CBC-Modus verschlüsselt. Der dazu verwendete Schlüssel ist geheim und nur der Stammzahlenregisterbehörde bekannt. Der Schlüssel unterscheidet sich vom Schlüssel zur Bildung der Stammzahl.
3. Base64 Kodierung des Ergebnisses.

Beispiel

Stammzahl, hexadezimal	42 AD 37 74 FA E0 70 7B 31 DC 6D 25 29 21 FA 49 (16 Byte)
Triple-DES Verschlüsselung, hexadezimal	64 BB 1C 4A 82 DD CC B0 FA 70 99 66 E5 76 05 14 (16 Byte)
Triple-DES Verschlüsselung, Base64	ZLscSj/dzLD6cD9m5XYFFA== (24 Zeichen)

Ermittlung des Wirtschafts-bPK

Die Bildung des wirtschaftsbereichsspezifische Personenkennzeichen (wbPK) erfolgt analog zur Bildung des gewöhnlichen bPK. Das E-GovG hält fest:

§ 14 (1) Für die Identifikation von natürlichen Personen im elektronischen Verkehr mit einem Auftraggeber des privaten Bereichs (§ 5 Abs. 3 DSG 2000) kann durch Einsatz der Bürgerkarte eine spezifische Ableitung aus dem Hashwert gebildet werden, der aus der Stammzahl des Betroffenen und der Stammzahl des Auftraggebers als Bereichskennung erzeugt wird (wirtschaftsbereichsspezifisches Personenkennzeichen, wbPK). Voraussetzung hierfür ist, dass der Auftraggeber des privaten Bereichs eine für den Einsatz der Bürgerkarte taugliche technische Umgebung eingerichtet hat, in der seine Stammzahl als Bereichskennung im Errechnungsvorgang für das wbPK zur Verfügung gestellt wird.

Algorithmus

Identisch mit dem Algorithmus zur Berechnung des bPK mit Ausnahme veränderter Ausgangsdaten.

1. Ausgangsdaten:
 - Stammzahl der natürlichen Person, base64 kodiert
 - Stammzahl des Auftraggebers als Bereichskennung
2. Bildung der Zeichenkette als Verbindung (string concatenation) aus Stammzahl der natürlichen Person und „+“ (als Zeichen) und URN-Präfix und Stammzahl des Auftraggebers.
 - Ist die Stammzahl eine Firmenbuchnummer, so ist diese inklusive des Prüfzeichens anzugeben. Führende Nullen werden unterdrückt. Leerzeichen oder Bindestriche vor dem Prüfzeichen werden nicht angeführt.
3. Über die entstehende Zeichenkette (den entstehenden String) wird der SHA-1 Algorithmus wie in FIPS PUB 180-1 [SHA-1] beschrieben berechnet. Das Resultat dieser Berechnung ist eine 160bit-Zahl (5x32 bit)
4. Diese 160bit-Zahl kann für programminterne Zwecke direkt verwendet werden, bei Übertragung bzw. in schriftlicher Form ist diese Zahl Base64 zu kodieren.

URN-Präfix

URN-Präfix := "urn:publicid:gv.at:wbpk+XXX+"

Wobei 'XXX' folgenden Wert annimmt, falls es sich bei der Stammzahl des Auftraggebers um

- eine Firmenbuchnummer handelt: „FN“.
- eine Vereinsregisternummer handelt: „VR“
- eine Zahl im Ergänzungsregister für nicht natürliche Personen handelt: „ERJ“
- eine Stammzahl einer natürlichen in Österreich meldepflichtigen Person handelt: „ZMR“
- eine Stammzahl einer natürlichen Person mit Eintrag im Ergänzungsregister handelt: „ERN“

Beispiel

Stammzahl, Base64	Qq03dPrgcHsx3G0lKSH6SQ== (24 Zeichen)
Stammzahl des Auftraggebers	468924 i
Präfix für Firmenbuchnummer	urn:publicid:gv.at:wbpk+FN+
Eingangsdaten für die Hashberechnung	Qq03dPrgcHsx3G0lKSH6SQ==+urn:publicid:gv.at:wbpk+FN+468924i (Leerzeichen vor „i“ entfernt – siehe Schritt 2)
Hashwert nach SHA-1, hexadezimal	43B8485AB5 6A3FE55946 24E2966DFE 9A2A082B9C (5 x 32 bit)
Hashwert nach SHA-1, Base64	Q7hIWrvQp+vZRiTilm3+mioIK5w= (28 Zeichen)

Verschlüsselung des bPK

Laut E-GovG §10(2) und §13(2) können bereichsspezifische Personenkennzeichen auch in verschlüsselter Form abgefragt und gespeichert werden.

§10 (2) ... Bei der Anforderung von bPKs aus einem Bereich, in dem der Anfordernde nicht zur Vollziehung berufen ist (Fremd-bPKs), dürfen nur Personenkennzeichen zur Verfügung gestellt werden, die nach Maßgabe des § 13 Abs. 2 verschlüsselt sind.

§13 (2) Ist es zum Zweck der eindeutigen Identifikation eines Betroffenen gemäß § 10 Abs. 2 zulässig, von der Stammzahlenregisterbehörde ein bereichsspezifisches Personenkennzeichen anzufordern, ist dieses, sofern es sich um ein Fremd-bPK handelt - das ist ein bPK aus einem Bereich, in dem der Anfordernde nicht zur Vollziehung berufen ist - von der Stammzahlenregisterbehörde nur verschlüsselt zur Verfügung zu stellen. Die Verschlüsselung ist so zu gestalten, dass

- 1. nur derjenige entschlüsseln kann, in dessen Datenanwendung das bPK in entschlüsselter Form zulässigerweise verwendet werden darf (Abs. 3), und*
- 2. durch Einbeziehung von zusätzlichen, dem Anfordernden nicht bekannten variablen Angaben in die Verschlüsselungsbasis das bPK auch in verschlüsselter Form keinen personenbezogenen Hinweis liefert.*

Das zur Verschlüsselung zugelassene Verfahren ist RSA mit einer Schlüssellänge von 1024bit.

Algorithmus

1. Ausgangsdaten: bPK in Base64 Darstellung, RSA-Public Key (1024 Bit)
2. Erstellung der zu verschlüsselnden Daten entsteht durch Verbinden von ISO-8859-1 Strings (string concatenation) von folgenden Strings:
 1. „V1::“
 2. URN-Präfix und bPK Bereich laut Berechnungs-Algorithmus des bPK.
 3. „::“
 4. bPK in Base64 Darstellung
 5. „::“
 6. Datum und Uhrzeit nach ISO-8601 §5 „extended format“: „YYYY-MM-DDThh:mm:ss“ [ISO-8601]
3. Der so gebildete String dient als Eingangsparameter der RSA-Verschlüsselung nach PKCS#1 RSAES-OAEP Spezifikation [PKCS#1].
4. Das Resultat der Verschlüsselung wird Base64 kodiert.

Anmerkung: Die notwendige geforderte „variable“ Verschlüsselung beruht darauf, dass einerseits der Zeitpunkt der Erstellung einbezogen wird, andererseits der verwendete RSAES-OAEP Algorithmus blockorientiert arbeitet und die fehlenden Zeichen auf die Blocklänge durch zufällige Werte auffüllt.

Beispiel

BPK, Base64	8lujqZzaRNTPkIIzxx3VfM/zCZs= (28 Zeichen)
Kürzel bPK-Bereich	T1 (für Testbereich 1 im SZR)
Datum und Uhrzeit	2006-10-09T15:54:14
Eingangsdaten für Verschlüsselung	V1::urn:publicid:gv.at:cdid+T1::8lujqZzaRNTPkIIzxx3VfM/zCZs=:2006-10-09T15:54:14 (Kodierung in ISO-8859-1)
RSA-Public Key	public exponent: 10001 (3 Bytes) modulus: B9 3E 0E 7C 1D 15 F9 85 15 0A DD A7 86 03 0D 05 90 DE 12 90 90 3C 19 EC 23 8A DE 36 02 63 A5 6F 41 67 30 CC B4 43 C5 4C 80 32 7C 2B 7A A8 21 84 12 59 3F 6D B1 19 45 9D DF 35 39 0D 98 41 22 44 34 D5 A9 7C C7 81 98 BB B3 B9 A7 A7 F7 5F 56 EE 8C BD BE 95 2B 44 71 8C D4 2E 5D 8C 31 BA 2F 0A 7C 91 07 DE B7 87 BC 90 64 2E 40 A2 19 30 49 84 68 F7 7D 47 41 A9 D9 A6 F3 B1 F8 1A 71 53 E4 51 (1024 bits = 128 Bytes)
Verschlüsseltes bPK, hexadezimal	73 5B 56 0C 8A D7 1F 70 50 F7 96 D4 28 D5 17 15 AC 4A A1 8E 28 D6 DD 35 9F 9F 57 C0 4D 96 0A 0B 12 BA 30 04 5A C9 58 42 69 F9 AC 46 55 35 F0 64 8E 3A 9D 18 87 0E 39 13 76 B1 B8 BC 3D 24 12 FB 78 75 DF 57 BB B8 EF 94 D8 AA 17 03 F8 CD DD 5C 04 48 B0 35 23 4B 1B 69 B4 D4 0A 16 35 9C 1C E5 B9 B9 4B AE 30 B2 23 FB 09 D2 E0 CB C3 C5 10 34 46 E1 0A 16 69 C0 A0 8F 49 2A 7D B6 12 F3 29 02 (128 Bytes)
Verschlüsseltes bPK, Base64	c1tWDIrXH3BQ95bUKNUXFaxKoY4o1t01n59XwE2WCgsSujAEWslYQ mn5rEZVNfBkjqqdGIcOORN2sbi8PSQS+3h131e7uO+U2KoXA/jN3V wESLA1I0sbabTUChY1nBz1ublLrjCyI/sJ0uDLw8UQNEbhChZpwKC PSSp9thLzKQI= (172 Zeichen)

Referenzen

[SHA-1]

FIPS PUB 180-1, U.S. Department of Commerce, National Institute of Standards and Technology: "Secure Hash Standard", April 1995

<http://csrc.nist.gov/publications/fips/fips180-1/fips180-1.pdf>

[DES] [Triple-DES]

FIPS PUB 46-3, U.S. Department of Commerce, National Institute of Standards and Technology: "Data Encryption Standard", October 1999

<http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf>

ANSI X9.52-1998, American National Standards Institute, „Triple Data Encryption Algorithm Modes of Operation“, 1998.

[Base64] [RFC 2045]

RFC 2045, Borenstein, Freed: "Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies", Kapitel 6.8. "Base64 Content-Transfer-Encoding." , September 1993

<http://www.ietf.org/rfc/rfc2045.txt>

[ISO-8859-1]

ISO/IEC 8859-1:1998 – Information technology - 8-bit single-byte coded graphic character sets --

Part 1: Latin alphabet No. 1, Stage date: 1998-04-16

[RFC 2141]

RFC 2141, Moats, "URN Syntax", Mai 1997

<http://www.ietf.org/rfc/rfc2141.txt>

[RFC 2396]

RFC 2396, T. Berners-Lee et al, "Uniform Resource Identifiers (URI): Generic Syntax", August 1998

<http://www.ietf.org/rfc/rfc2396.txt>

2004-06-03 SZ-bPK-Algo V1.0.2 Seite 10/11

[RFC 3151]

RFC 3151, Walsh, Cowan, Grosso, "A URN Namespace for Public Identifiers", August 2001

<http://www.ietf.org/rfc/rfc3151.txt>

[ISO-8601]

ISO 8601:2000 – Data elements and interchange formats -- Information interchange -- Representation of dates and times, Stage date: 2000-12-21

[ISO-646]

ISO/IEC 646:1991 – Information technology -- ISO 7-bit coded character set for information interchange, Stage date: 2002-08-16

Historie

Version Datum Änderungen

1.1.1 2006-10-09

FremdBPK Beispiel angepasst.

1.1.0 2006-10-02

Abschnitt Verschlüsselung des bPK:

Änderung von Prefix „Ver: 1::“ auf „V1::“, um 5-stellige Bereiche zu ermöglichen.

Entfernung obsoleter Referenzen und Korrektur von orthografischen Fehlern.

1.0.2 2004-06-03 •

Abschnitt Verschlüsselung des bPK:

Änderung von Prefix „Version: 1::“ auf „Ver: 1::“

Im Beispiel zur Verschlüsselung des bPK werden nun Echtwerte für Verschlüsselung und Base64- Kodierungen verwendet.

1.0.1 2004-05-28 •

In den Beispielen sind die Ergebnisse von

Hashwertberechnungen und Base64-Kodierungen nun Echtwerte.

1.0.0 2002-02-04 • Erstellt.