BM.I REPUBLIK ÖSTERREICH
BUNDESMINISTERIUM FÜR INNERES
SEKTION III-RECHT

GZ.: BMI-LR1420/0031-III/1/a/2007 Wien, am 25. September 2007

An das

Präsidium des
Nationalrates

Parlament
1017 W I E N

Rita Ranftl
BMI - III/1 (Abteilung III/1)
Herrengasse 7, 1014 Wien
Tel.: +43 (01) 531262046
Pers. E-Mail: Rita.Ranftl@bmi.gv.at
Org.-E-Mail: BMI-III-1@bmi.gv.at
WWW.BMI.GV.AT
DVR: 0000051
Antwortschreiben bitte unter Anführung der GZ an die Org.-E-Mail-Adresse.

Betreff: Legistik und Recht; Fremdlegistik; BG-BKA
Bundesgesetz, mit dem das E-Government-Gesetz geändert wird (E-GovG-Novelle 2007);
Stellungnahme des Bundesministeriums für Inneres

In der Anlage wird zu dem im Betreff bezeichneten Entwurf die Stellungnahme des Bundesministeriums für Inneres übermittelt.

Beilage

Für den Bundesminister:

Mag. Sabine Halbauer

elektronisch gefertigt

BM.I REPUBLIK ÖSTERREICH
BUNDESMINISTERIUM FÜR INNERES
SEKTION III-RECHT

GZ.: BMI-LR1420/0031-III/1/a/2007 Wien, am 25. September 2007

An das

Bundeskanzleramt

Ballhausplatz 2
1014 W I E N

Zu Zl. BKA-410.004/0024-I/11/2007

Rita Ranftl
BMI - III/1 (Abteilung III/1)
Herrengasse 7, 1014 Wien
Tel.: +43 (01) 531262046
Pers. E-Mail: Rita.Ranftl@bmi.gv.at
Org.-E-Mail: BMI-III-1@bmi.gv.at
WWW.BMI.GV.AT
DVR: 0000051
Antwortschreiben bitte unter Anführung der GZ an die Org.-E-Mail-Adresse.

Betreff: Legistik und Recht; Fremdlegistik; BG-BKA
Bundesgesetz, mit dem das E-Government-Gesetz geändert wird (E-GovG-Novelle 2007);
Stellungnahme des Bundesministeriums für Inneres

Aus der Sicht des Bundesministeriums für Inneres ergeben sich zu dem im Betreff bezeichneten Entwurf folgende Bemerkungen:

Zu Z 1 (§ 2 Z 3):

Die Streichung der Wiederholungsidentität wird ausdrücklich begrüßt, da diese Regelung sehr kompliziert und deshalb nur schwer anzuwenden war.

Zu Z 10 (§ 7 Abs. 2)

Das BM.I sieht keinerlei zwingenden Anlass für die vorgeschlagene Änderung, wonach das BM.I nicht mehr zwangsläufig als Dienstleister für den Betrieb des SZR herangezogen werden soll.

Zu der vorgeschlagenen Änderung wird in den Erläuternden Bemerkungen im Allgemeinen Teil folgendes ausgeführt: „*das Basisregister für eindeutige Identitäten von natürlichen Personen in Österreich stellt das Zentrale Melderegister mit der darin enthaltenen ZMR-Zahl dar. Ausgangspunkt für die eindeutige elektronische Identität ist in der Folge die kryptographische Einwegableitung aus der ZMR-Zahl – die sog. Stammzahl. Zur Führung des (virtuellen) Stammzahlenregisters bedient sich die Stammzahlenregisterbehörde derzeit des Bundesministeriums für Inneres, welches auch das ZMR betreibt, als gesetzlichen Dienstleister. Die Führung beider Register durch ein und dieselbe Organisation hat trotz einer entsprechenden technischen Trennung zu Kritik geführt.*“

Eine diesbezügliche Kritik ist dem BM.I gegenüber nie geäußert worden.
Die gewählte Formulierung legt die Vermutung nahe, dass die geäußerte Kritik auf einem Fehlverständnis der Funktionsweise des SZR beruhen könnte:
Einleitend darf festgehalten werden, dass es sich bei der Stammzahl nicht um eine kryptographische Einwegableitung aus der ZMR-Zahl handelt. Allerdings stellen die durch das SZR errechneten bPK jeweils kryptographische Einwegableitungen aus der ZMR-Zahl dar. Dies ergibt sich eindeutig aus den einschlägigen Bestimmungen im E-Government-Gesetz (§ 6 und 13)
Beim SZR handelt es sich um ein reines Rechenregister, in dem selbst keine Daten (insbesondere nicht die Stammzahl (!)) gespeichert werden. Stellt ein Auftraggeber des öffentlichen Bereichs einen Request zur Berechnung eines bPK, dann werden die Daten der Anforderung gespeichert, nicht aber das diesem übermittelte bPK. Ebensowenig wird die Stammzahl gespeichert, wenn diese an eine Bürgerkarten-Registrierungsstelle übermittelt wird. Da die einzigen Daten, welche im Zusammenhang mit dem Betrieb des SZR gespeichert werden, die Protokolldaten der jeweiligen Anfragen sind, ist es aus Sicht der SU-ZMR nicht leicht nachvollziehbar, wieso die Führung des ZMR und des SZR durch dieselbe Stelle problematisch sein soll.

Die Übertragung der Funktion des Dienstleisters für das SZR an eine andere Organisation als das BM.I würde hingegen erhebliche Probleme aufwerfen:

Die Grundlage für die Funktionstüchtigkeit des SZR-Systems inklusive bereichsspezifische Kennzeichen (bPK) und verschlüsselte Fremd-bPKs bilden:
• Die sichere Verwahrung der Ausgangsdaten (ZMR-Zahlen; derzeit nur im ZMR gespeichert)
• Die zuverlässige Absicherung des (geheimen) 3DES Schlüssels, durch den die ZMR-Zahl in die Stammzahl übergeführt wird,
• Die Verspeicherung der Stammzahl, die ausschließlich auf der Bürgerkarte gespeichert wird,
• Die Unumkehrbarkeit der Erzeugung einer bPK mittels Hashfunktion aus einer Stammzahl und Bereichsinformationen – dieser Vorgang ist zuverlässig wiederholbar, aber nicht umkehrbar,
• Und schließlich die Verwendung von asymmetrischer Verschlüsselung für Fremd-bPKs, die nur dem rechtmäßigen Empfänger eine Entschlüsselung erlaubt.

Aufgrund der gesetzlichen Anforderungen erfolgt die Erzeugung sowohl der Stammzahl als auch des bPK durch eine mit starker Verschlüsselung gesicherte Ableitung aus der ZMR-Zahl. Diese wird im Rahmen des SZR durch eine 3DES-Verschlüsselung erreicht.
Die Methode der 3DES-Verschlüsselung gehört zu den sichersten kryptographischen Methoden, die derzeit in Verwendung sind. Ein realistischer Angriff auf 3DES ist derzeit nur durch Diebstahl des Schlüssels möglich.

Neben der Datenhaltung selbst ist der 3DES Schlüssel der empfindlichste Punkt des Systems. Der 3DES Schlüssel garantiert nicht nur, dass niemand außerhalb des SZR-Systems eine Überführung einer ZMR-Zahl in eine Stammzahl durchführen kann, sondern garantiert außerdem die Authentizität von Bürgerkarten und bPKs, somit die Eindeutigkeit der Personenbindung.
In der Beilage wird die derzeit angewandte Methode veranschaulicht.

Der Sicherung des 3DES-Schlüssels kommt deshalb besondere Bedeutung zu.
Zur Ausfalls-Sicherung sind derzeit zwei komplett unabhängige Systeme gleicher Bauart innerhalb des Rechenzentrums des BM.I an zwei räumlich getrennten Stellen untergebracht. Die Sicherheit der Systeme entspricht der höchsten Sicherheitsstufe, die das US National Institute of Standards and Technology (NIST) für Computersysteme vergibt.
Diese Räume besitzen ein Höchstmaß an Zutrittssicherung. Der Zugriff auf die Schlüssel erfordert mehrere Personen höchster Autorisierungsstufe. Damit sind selbst Angriffe, die über einen Geheimnisträger gehen, mit großer Sicherheit auszuschließen.
Technisch wurde dieses Konzept so implementiert, dass im BM.I eine Krypto-Box installiert wurde, in welcher ein geheimer Schlüssel unter Verwendung auch des geheimen Systemschlüssels des BM.I (und zweier weiterer Schlüssel) generiert wurde. Ein Einsatz der Krypto-Box in einer anderen Systemumgebung als des BM.I wäre deshalb nicht möglich. Einzige Möglichkeit der Transferierung des bisher nur in der Krypto-Box vorhandenen geheimen Schlüssels an eine andere Organisationseinheit als das BM.I wäre es, diesen in Klartext auszulesen, auf ein Trägermedium zu überspielen und danach an einen anderen Ort zu transferieren.
Ob nach diesem Vorgang aber noch von einer starken Verschlüsselung gesprochen werden kann muss erheblich bezweifelt werden, weil durch das notwendige Auslesen in Klartext der Schlüssel einem begrenzten Personenkreis jedenfalls bekannt wird. Ist die durch § 6 Abs. 2 E-GovG geforderte starke Verschlüsselung nicht mehr gegeben, würden die bisher ausgestellten Bürgerkarten ungültig und wären zunächst einzuziehen und dann neu auszustellen. Ebenso wären die bisher berechneten bPK (insgesamt rund 33 Mio.) neu zu berechnen. Die geplante Möglichkeit, einen anderen Dienstleister als das BM.I als

Dienstleister für das SZR heranzuziehen, führt also einerseits zu einem rechtsunsicheren Zustand und andererseits zu sehr erheblichen technischen Problemen, die zu einem enormen Verwaltungsaufwand und auch zu einer Kostenexplosion führen würde und kann daher nicht nachvollzogen werden.
Abschließend darf noch bemerkt werden, dass sich die Stammzahlenregisterbehörde bei allen anderen Betroffen des BM.F zu bedienen hat, während es der genannten Behörde hinsichtlich des BM.I freigestellt wird sich seiner zu bedienen (…kann...).

Zu Z 15 (§ 12 Abs. 1 Z 4)

Augrund der Umbenennung des „wirtschaftsbereichsspezifischen Personenkennzeichens“ in den Ausdruck „bPK für die Verwendung im privaten Bereich“ wäre auch § 16 Abs. 1 Meldegesetz entsprechend anzupassen.

Die gegenständliche Stellungnahme wird dem Präsidium des Nationalrates in elektronischer Form zugemittelt.

Beilage

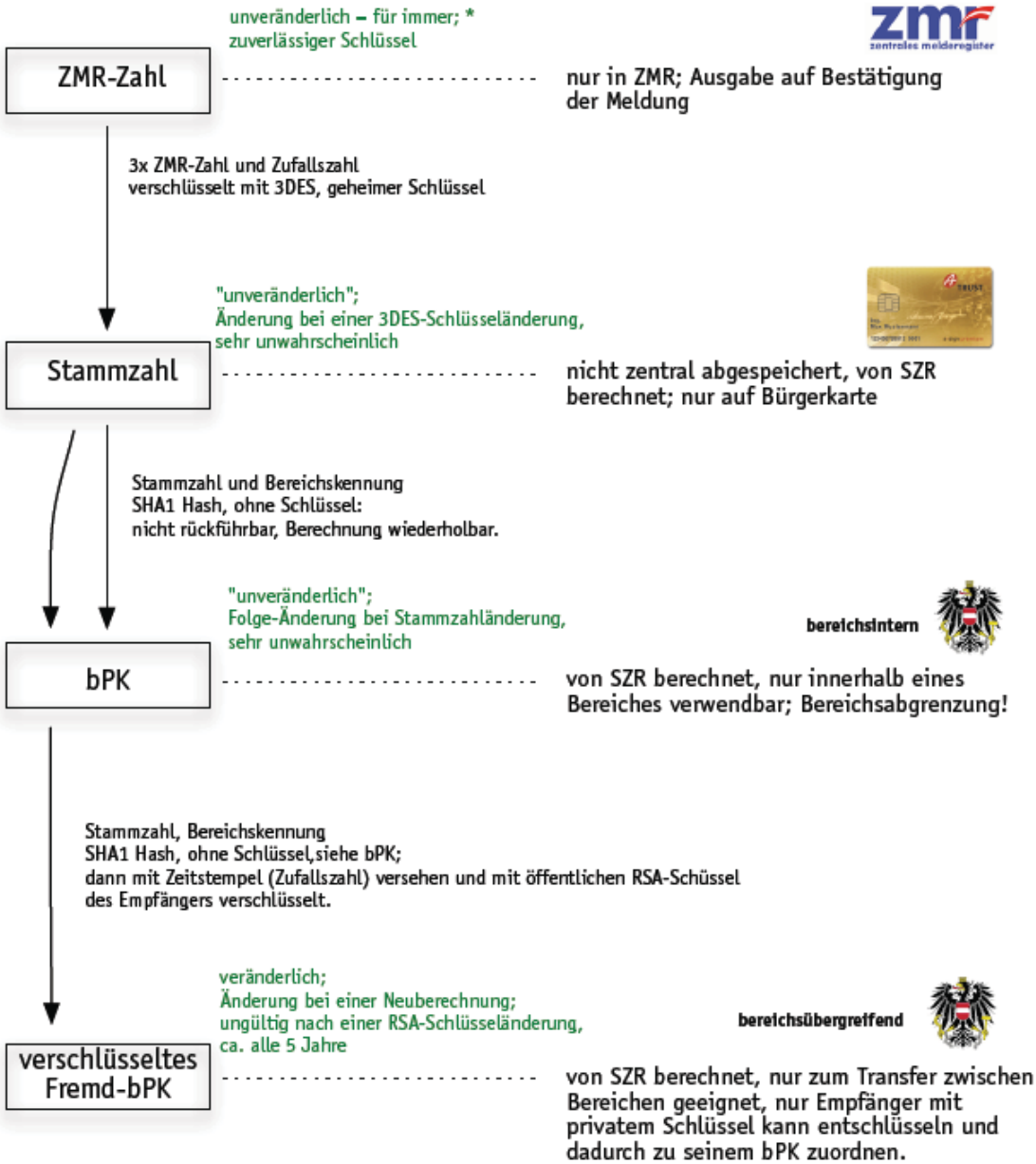
Für den Bundesminister:

Mag. Sabine Halbauer

elektronisch gefertigt

BM.I REPUBLIK ÖSTERREICH
BUNDESMINISTERIUM FÜR INNERES
SEKTION IV – SUPPORT UNIT ZMR

Zusammenhänge
ZMR-Zahl, Stammzahl, bPK



*) bei Personen-Split oder Kit kann eine Person eine neue ZMR-Zahl erhalten, die alte(n) ZMR-Zahlen werden historisiert – Suche danach weiter möglich