Entwurf

Verordnung der Bundesministerin für Gesundheit, Familie und Jugend, mit der die für den elektronischen Gesundheitsdatenaustausch in Betracht kommenden Rollen, die die Rollen bestätigenden Stellen sowie die qualitativen Mindestanforderungen für Verschlüsselung und elektronische Signaturen festgelegt werden – Gesundheitstelematikverordnung (GTelV)

Auf Grund der §§ 5 Abs. 1 und 7 Abs. 5 des Gesundheitstelematikgesetzes (GTelG), BGBl. I Nr. 179/2004, zuletzt geändert durch das Bundesgesetz BGBl. I Nr. 23/2008, wird verordnet:

Rollen

§ 1. (1) Im Rahmen des elektronischen Gesundheitsdatenaustausches haben Gesundheitsdiensteanbieterinnen/Gesundheitsdiensteanbieter Rollen gemäß Anlage 1 Abschnitt A zu verwenden.

(2) Bestandgeber ist, wer die Zuordnung einer Rolle zu einer Gesundheitsdiensteanbieterin/einem Gesundheitsdiensteanbieter authentisch bestätigt. Bestandgeber ist die Bundesministerin/der Bundesminister für Gesundheit, Familie und Jugend. Außerdem dürfen für die in der Anlage 1 Abschnitt A

1. in den Z 1 bis 3 genannten Rollen die Österreichische Ärztekammer,
2. in den Z 4 bis 7 genannten Rollen die Österreichische Zahnärztekammer,
3. in Z 12 genannte Rolle das Österreichische Hebammengremium,
4. in Z 28 genannte Rolle die Österreichische Apothekerkammer sowie
5. in Z 40 genannte Rolle der Hauptverband der österreichischen Sozialversicherungsträger

als Bestandgeber tätig werden.

(3) Nimmt ein gemäß Abs. 2 Z 1 bis 5 berechtigter Bestandgeber seine Aufgaben nicht wahr oder wird die Bescheinigung gemäß § 5 Abs. 6 widerrufen, hat die authentische Bestätigung der Rollen durch die Bundesministerin/den Bundesminister für Gesundheit, Familie und Jugend zu erfolgen.

(4) Bestandgeber haben der Bundesministerin/dem Bundesminister für Gesundheit, Familie und Jugend schriftlich bekannt zu geben, welche natürlichen Personen mit Aufgaben nach dieser Verordnung betraut wurden.

GDA-Token

§ 2. (1) Für den Nachweis bzw. die Prüfung von Identität und Rolle(n) von Gesundheitsdiensteanbieterinnen/Gesundheitsdiensteanbietern mittels elektronischer Bescheinigung ist die Datenstruktur „GDA-Token“ zu verwenden. Die Spezifikation der Datenstruktur GDA-Token ist von der Bundesministerin/vom Bundesminister für Gesundheit, Familie und Jugend zu veröffentlichen.

(2) Die Antragstellung, Bildung, Zustellung und Dokumentation von GDA-Token hat in elektronischer Form zu erfolgen. Die dafür erforderliche Infrastruktur ist von der Bundesministerin/vom Bundesminister für Gesundheit, Familie und Jugend bereitzustellen.

(3) GDA-Token, in denen mehrere Rollen einer Gesundheitsdiensteanbieterin/eines Gesundheitsdiensteanbieters bestätigt werden, dürfen nur gebildet werden, wenn derselbe Bestandgeber (§ 1) zur Bestätigung sämtlicher Rollen berechtigt ist.

(4) GDA-Token dürfen auch für organisatorische Gliederungen von Gesundheitsdiensteanbieterinnen/Gesundheitsdiensteanbietern, die weder natürliche Personen noch Dienstleister gemäß Anlage 1 Abschnitt A Z 52 sind, gebildet werden.

Antrag

§ 3. (1) GDA-Token dürfen ausschließlich auf Grund elektronischer Anträge von Gesundheitsdiensteanbieterinnen/Gesundheitsdiensteanbietern oder einer gemäß Abs. 2 berechtigten Person gebildet werden. Der Antrag ist unter Verwendung der Bürgerkartenfunktion elektronisch zu signieren.

(2) Gesundheitsdiensteanbieterinnen/Gesundheitsdiensteanbieter, die keine natürlichen Personen sind, haben der Bundesministerin/dem Bundesminister für Gesundheit, Familie und Jugend schriftlich bekanntzugeben, welche natürlichen Personen berechtigt sind, in ihrem Namen die Bildung von GDA-Token zu beantragen.

(3) Der Antrag auf Bildung eines GDA-Token hat insbesondere zu enthalten:

1. den Namen oder die Bezeichnung der Gesundheitsdiensteanbieterin/des Gesundheitsdiensteanbieters,
2. bei natürlichen Personen das Geschlecht,
3. die Angabe der postalischen und elektronischen Erreichbarkeiten,
4. die Rolle(n),
5. einen Vorschlag für einen symbolischen Bezeichner gemäß § 10 Abs. 1 Z 3 GTelG,
6. die Angaben, die für die elektronische Zustellung des GDA-Tokens erforderlich sind,
7. die Verschlüsselungszertifikatsdatei(en) oder die elektronische(n) Adresse(n), an der die zur Verschlüsselung von Gesundheitsdaten erforderlichen Angaben aufgefunden werden können,
8. die Stammzahl der Gesundheitsdiensteanbieterin/des Gesundheitsdiensteanbieters oder des Rechtsträgers der Gesundheitsdiensteanbieterin/des Gesundheitsdiensteanbieters, wenn die Bildung des GDA-Tokens für eine nicht natürliche Person beantragt wird,
9. das Zertifikat (die Zertifikate) oder eine eindeutige Referenz auf das Zertifikat (die Zertifikate), das (die) die Gesundheitsdiensteanbieterin/der Gesundheitsdiensteanbieter zur Signatur gemäß § 7 GTelG verwendet. Erfolgt die Signatur gemäß § 7 GTelG im Rahmen der Bürgerkartenfunktion, dürfen diese Angaben unterbleiben.

(4) Wird die Bildung von GDA-Token für eine organisatorische Gliederung (§ 2 Abs. 4) beantragt, hat der Antrag auch die Bezeichnung dieser organisatorischen Gliederung zu enthalten.

(5) Der Antrag darf weiters umfassen:

1. den Antrag zur Eintragung in den eHealth-Verzeichnisdienst sowie
2. die Angabe jener Datenformate, die von der Gesundheitsdiensteanbieterin/vom Gesundheitsdiensteanbieter elektronisch verarbeitet werden können.

Prüfung des Antrages

§ 4. (1) Die Bundesministerin/Der Bundesminister für Gesundheit, Familie und Jugend hat den Antrag auf Vollständigkeit und Plausibilität zu prüfen, erforderlichenfalls ergänzende Auskünfte einzuholen und die Identität der Gesundheitsdiensteanbieterin/des Gesundheitsdiensteanbieters bzw. der Antragstellerin/des Antragstellers zu prüfen. Hiezu sind die Register des E-Government gemäß § 6 Abs. 3 und 4 E-Government-Gesetz (E-GovG), BGBl. I Nr. 10/2004 in der Fassung des Bundesgesetzes BGBl. I Nr. 59/2008, heranzuziehen.

(2) Als Identifikationsbegriff für eine Gesundheitsdiensteanbieterin/einen Gesundheitsdiensteanbieter, die/der eine natürliche Person ist, ist der Health Professional Identifier (HPI) in Form einer eindeutigen und nicht-umkehrbaren Ableitung des bereichsspezifischen Personenkennzeichens (bPK) gemäß § 9 E-GovG des Bereichs Gesundheit (§ 3 Abs. 1 und Anlage E-Government-Bereichsabgrenzungsverordnung [E-Gov-BerAbgrV], BGBl. II Nr. 289/2004) zu bilden und zu verwenden.

(3) Als Identifikationsbegriff für eine Gesundheitsdiensteanbieterin/einen Gesundheitsdiensteanbieter, die/der keine natürliche Person ist, ist deren/dessen Stammzahl bzw. die Stammzahl des Rechtsträgers der Gesundheitsdiensteanbieterin/des Gesundheitsdiensteanbieters zu verwenden.

Bearbeitung des Antrages durch Bestandsgeber

§ 5. (1) Die Antragsdaten sind dem Bestandgeber (§ 1) zur Verfügung zu stellen.

(2) Dem Bestandgeber obliegen:

1. die Prüfung der Berechtigung zur Ausübung der angegebenen Rolle(n),

2. die Bestätigung oder Ablehnung der Bestätigung der Rolle(n),
3. die Veranlassung der Sperre oder des Widerrufs eines GDA-Tokens sowie
4. die Veranlassung der Aufhebung der Sperre eines GDA-Tokens.

(3) Ist auf Grund der Angaben im Antrag und der dem Bestandgeber gegebenenfalls vorliegenden Informationen eine abschließende Beurteilung der Berechtigung zur Ausübung der Rolle(n) nicht möglich, hat der Bestandgeber die Antragstellerin/den Antragsteller unter Angabe der Gründe zur Aufklärung, erforderlichenfalls zur Vorlage entsprechender Nachweise, aufzufordern oder diesbezügliche Auskünfte einzuholen.

(4) Die Bestätigung der Rolle(n) ist vom Bestandgeber abzulehnen, wenn

1. eine Berechtigung zur Ausübung der angegebenen Rolle(n) nicht besteht oder
2. der Verbesserungsversuch gemäß Abs. 3 erfolglos geblieben ist oder
3. eine Berechtigung zur Bestätigung einer Rolle (§ 1) nicht besteht.

(5) Sowohl die Bestätigung als auch die Ablehnung der Bestätigung der Rolle(n) sind mit einer fortgeschrittenen elektronischen Signatur des Bestandgebers im Sinne des § 2 Z 3 Signaturgesetz (SigG), BGBl. I Nr. 190/1999, in der Fassung des Bundesgesetzes BGBl. I Nr. 59/2008, zu versehen. Die Prüfbarkeit dieser Signatur muss durch eine Referenz auf die Bescheinigung gemäß Abs. 6 sichergestellt werden.

(6) Von der Bundesministerin/Vom Bundesminister für Gesundheit, Familie und Jugend ist den Bestandgebern eine elektronische Bescheinigung zur Verfügung zu stellen, die insbesondere die Bezeichnung des Bestandgebers und die Bestandgebereigenschaft zu enthalten hat.

(7) Der Schutz der Signaturerstellungsdaten gegen Missbrauch ist von den Bestandgebern durch technische und organisatorische Maßnahmen, die in einem Sicherheitskonzept zu dokumentieren sind, zu gewährleisten.

Bildung und Zustellung des GDA-Tokens

§ 6. (1) Das GDA-Token ist anhand der geprüften Antragsdaten und der Bestätigung der Rollen(n) durch den Bestandgeber zu bilden.

(2) In das GDA-Token sind folgende Daten aufzunehmen:

1. der Name oder die Bezeichnung der Gesundheitsdiensteanbieterin/des Gesundheitsdiensteanbieters,
2. gegebenenfalls die Bezeichnung der organisatorischen Gliederung,
3. der Identifikationsbegriff gemäß § 4 Abs. 2 oder Abs. 3,
4. die Rolle(n),
5. die Kennung (OID) gemäß § 10 Abs. 1 Z 3 und Abs. 2 GTelG,
6. die Bezeichnung des Bestandgebers,
7. das Datum der Bildung und die Gültigkeitsdauer, die maximal fünf Jahre betragen darf,
8. die Verschlüsselungszertifikatsdatei(en) oder die elektronische(n) Adresse(n), an der/denen die zur Verschlüsselung von Gesundheitsdaten erforderlichen Angaben aufgefunden werden können,
9. das Zertifikat (die Zertifikate) oder (eine) eindeutige Referenz(en) auf das Zertifikat (die Zertifikate), das (die) die Gesundheitsdiensteanbieterin/der Gesundheitsdiensteanbieter zur Signatur gemäß § 7 GTelG verwendet. Erfolgt die Signatur gemäß § 7 GTelG im Rahmen der Bürgerkartenfunktion, darf die Aufnahme dieser Angaben in das GDA-Token unterbleiben.

(3) Wird das GDA-Token für eine organisatorische Gliederung einer Gesundheitsdiensteanbieterin/eines Gesundheitsdiensteanbieters gebildet, ist anstelle der Kennung (OID) gemäß Abs. 2 Z 5 eine aus dieser Kennung abgeleitete (erweiterte) Kennung aufzunehmen. Die Gesundheitsdiensteanbieterin/Der Gesundheitsdiensteanbieter kann dafür einen entsprechenden Vorschlag erstatten, der zu berücksichtigen ist, wenn die Eindeutigkeit gegeben ist. Gleiches gilt für den diesbezüglichen Vorschlag des symbolischen Bezeichners (§ 3 Abs. 3 Z 5).

(4) Wurde ein Antrag gemäß § 3 Abs. 5 Z 1 gestellt, hat gleichzeitig mit der Bildung des GDA-Tokens die Registrierung (Eintragung) im eHealth-Verzeichnisdienst zu erfolgen; die Gesundheitsdiensteanbieterin/der Gesundheitsdiensteanbieter ist hierüber gemäß § 12 Abs. 5 GTelG zu informieren.

(5) Der Gesundheitsdiensteanbieterin/Dem Gesundheitsdiensteanbieter ist das GDA-Token entsprechend den Angaben im Antrag im elektronischen Weg zur Verfügung zu stellen oder eine mit den Gründen über das Unterbleiben der Bildung des GDA-Tokens und – im Falle eines Antrages gemäß § 3

Abs. 5 Z 1 über das Unterbleiben der Registrierung im eHealth-Verzeichnisdienst – versehene Information formlos zu übermitteln.

Sperre und Widerruf des GDA-Tokens

§ 7. (1) Die Bundesministerin/Der Bundesminister für Gesundheit, Familie und Jugend hat einen Widerrufsdienst für GDA-Token zu führen.

(2) Die Sperre, die Aufhebung der Sperre oder der Widerruf eines GDA-Tokens haben auf Grund der Mitteilung der Gesundheitsdiensteanbieterin/des Gesundheitsdiensteanbieters oder auf Grund eigener Wahrnehmungen des Bestandgebers zu erfolgen. Der Widerruf infolge Ablauf der Gültigkeitsdauer darf automationsunterstützt durchgeführt werden.

(3) Das GDA-Token ist zu sperren, wenn die Gesundheitsdiensteanbieterin/der Gesundheitsdiensteanbieter

1. die Berechtigung zur Ausübung der Rolle(n) für einen befristeten, jedoch drei Monate nicht überschreitenden Zeitraum verliert oder
2. die mit der (den) Rolle(n) verbundenen Tätigkeiten mehr als drei Monate, jedoch einen sechs Monate nicht überschreitenden Zeitraum, einstellt.

(4) Die Sperre ist aufzuheben, wenn die Voraussetzung dafür weggefallen ist.

(5) Das GDA-Token ist zu widerrufen, wenn

1. sich eine der in § 6 Abs. 2 Z 1 bis 5, 7 oder 9 genannten Angaben ändert,
2. die zur Signatur des GDA-Tokens verwendeten Algorithmen oder Verfahren kompromittiert wurden,
3. die Gesundheitsdiensteanbieterin/der Gesundheitsdiensteanbieter die Berechtigung zur Ausübung der Rolle(n) für einen drei Monate überschreitenden Zeitraum verliert,
4. die Gesundheitsdiensteanbieterin/der Gesundheitsdiensteanbieter auf die Ausübung der Rolle(n) verzichtet oder die mit der (den) Rolle(n) verbundenen Tätigkeiten für einen sechs Monate übersteigenden Zeitraum einstellt,
5. die Gültigkeit vor dem sich aus Abs. 3 ergebenden Zeitpunkt für die Aufhebung der Sperre endet,
6. es bei Kenntnis aller Umstände nicht hätte gebildet werden dürfen.

(6) Das GDA-Token ist jedenfalls zu widerrufen, wenn es mehrere Rollen enthält und eine dieser Rollen zu sperren oder zu widerrufen ist. Gleichzeitig ist für die aufrechte(n) Rolle(n) ein neues GDA-Token zu bilden, wenn sich die zur Bildung des GDA-Tokens sonst erforderlichen Daten nicht geändert haben. Die Prüfung der Identität gemäß § 4 kann in diesen Fällen unterbleiben.

(7) Die Gesundheitsdiensteanbieterin/Der Gesundheitsdiensteanbieter ist über die Sperre, die Aufhebung der Sperre oder den Widerruf des GDA-Tokens zu verständigen.

Initiale Bildung von GDA-Token

§ 8. (1) Abweichend von § 3 Abs. 1 darf die Bundesministerin/der Bundesminister für Gesundheit, Familie und Jugend die in einem bestehenden Verzeichnis enthaltenen Daten von der Verzeichnis führenden Stelle automationsunterstützt übernehmen und zur erstmaligen Bildung von GDA-Token verwenden, wenn

1. das abgebende Verzeichnis von einer Körperschaft des öffentlichen Rechts oder in deren Auftrag geführt wird,
2. die Daten in ausreichender Qualität, insbesondere mit der korrekten Bezeichnung der Rollen gemäß Anlage 1, bereit gestellt werden, wobei die Angaben gemäß § 3 Abs. 3 Z 7 bzw. 9 auch der Mitteilung gemäß Z 3 angeschlossen werden dürfen und
3. die Gesundheitsdiensteanbieterin/der Gesundheitsdiensteanbieter bei der Bundesministerin/beim Bundesminister für Gesundheit, Familie und Jugend mit einer formlosen elektronischen Mitteilung die Bildung des GDA-Tokens beantragt. Enthalten die aus dem Verzeichnis übernommenen Daten oder die Mitteilung der Gesundheitsdiensteanbieterin/des Gesundheitsdiensteanbieters keinen Vorschlag für einen symbolischen Bezeichner, ist dieser von der Bundesministerin/vom Bundesminister für Gesundheit, Familie und Jugend festzulegen.

(2) Die automationsunterstützte Übernahme von Daten darf nur hinsichtlich jener Gesundheitsdiensteanbieterinnen/Gesundheitsdiensteanbieter erfolgen, für die der Auftraggeber des abgebenden Verzeichnisses zur authentischen Bestätigung der Rolle(n) als Bestandgeber gemäß § 1 berechtigt ist.

Dokumentation

§ 9. (1) Sämtliche Vorgänge im Zusammenhang mit der Antragstellung, Bildung, Zustellung, Sperre, Aufhebung der Sperre und dem Widerruf von GDA-Token sind elektronisch zu dokumentieren.

(2) Die Dokumentation ist zehn Jahre ab dem in das GDA-Token eingetragenen Ende der Gültigkeit aufzubewahren.

Serverzertifikate

§ 10. (1) Für den Nachweis bzw. die Prüfung der Identität im Rahmen der programmgesteuerten Abwicklung des elektronischen Gesundheitsdatenaustausches gemäß § 4 Abs. 3 GTelG dürfen Zertifikate auf einem Server zur laufenden Verwendung hinterlegt werden.

(2) Für Serverzertifikate sind Algorithmen und Parameter entsprechend dem jeweiligen Stand der Technik zu verwenden, die hinsichtlich ihrer Schlüssellänge und Verwendbarkeit den Anforderungen für qualifizierte Zertifikate gemäß § 2 Z 9 SigG entsprechen. Die Schlüssel sind so zu verwahren, dass sie Dritten nicht zur Kenntnis gelangen können.

(3) Serverzertifikate müssen als Zertifikatserweiterung (Attribut) eindeutige Kennungen (OID) enthalten, die jeweils aus der Kennung (OID) jener Gesundheitsdiensteanbieterin/jenes Gesundheitsdiensteanbieters abzuleiten sind, die/der solche Zertifikate verwendet. Die Kennungen sind von der Gesundheitsdiensteanbieterin/vom Gesundheitsdiensteanbieter zu dokumentieren und auf Verlangen der Bundesministerin/des Bundesministers für Gesundheit, Familie und Jugend offen zu legen.

(4) Die Gesundheitsdiensteanbieterin/Der Gesundheitsdiensteanbieter, die/der zur programmgesteuerten Abwicklung des Gesundheitsdatenaustausches Serverzertifikate verwendet, hat ein Sicherheitskonzept zu erstellen sowie Störfälle und besondere Betriebssituationen elektronisch zu dokumentieren. Das Sicherheitskonzept sowie die Dokumentation sind der Bundesministerin/dem Bundesminister für Gesundheit, Familie und Jugend oder einem hiezu von ihr/ihm beauftragten Dritten auf Aufforderung offen zu legen.

Vertraulichkeit und Integrität

§ 11. (1) Die Vertraulichkeit und die Integrität von Gesundheitsdaten sind im elektronischen Verkehr mit Gesundheitsdaten dadurch sicherzustellen, dass

1. der Gesundheitsdatenaustausch über Netzwerke durchgeführt wird, die entsprechend dem Stand der Netzwerksicherheit hinreichend gegenüber anderen Netzen abgesichert sind, oder
2. Protokolle und Verfahren verwendet werden, die einen dem Stand der Technik entsprechenden verschlüsselten Gesundheitsdatenaustausch ermöglichen und einen wirksamen Schutz gegen Angriffe Dritter bieten, oder
3. kryptographische Verfahren und elektronische Signaturen eingesetzt werden, wobei die für die kryptographischen Verfahren verwendeten Algorithmen und Parameter gemäß Anlage 2 eine starke Verschlüsselung der Gesundheitsdaten gewährleisten müssen.

(2) Beim elektronischen Verkehr mit Gesundheitsdaten gemäß Abs. 1 Z 1 und 2, ausgenommen beim Gesundheitsdatenaustausch zwischen der Sozialversicherung und ihren Vertragspartnern im Rahmen der über das Gesundheitsinformationsnetz bereitgestellten Dienste, ist den Gesundheitsdaten das GDA-Token oder der Identifikationsbegriff gemäß § 6 Abs. 1 Z 3 der Gesundheitsdiensteanbieterin/des Gesundheitsdiensteanbieters beizufügen. Beim Gesundheitsdatenaustausch gemäß Abs. 1 Z 2 dürfen die allenfalls von der Verschlüsselung ausgenommenen Informationen weder Hinweise auf die von den Gesundheitsdaten Betroffenen (Personenbezug) noch allfällige Authentisierungs- bzw. Authentifizierungsdaten enthalten.

(3) Zur Verschlüsselung von Gesundheitsdaten gemäß Abs. 1 Z 3 können asymmetrische Verfahren, symmetrische Verfahren oder hybride Verfahren (Schlüsselaustausch über asymmetrische Verfahren und Verschlüsselung der Gesundheitsdaten mittels symmetrischer Verfahren) verwendet werden. Bei Verwendung hybrider Verschlüsselungsverfahren müssen sowohl die Algorithmen und Parameter der asymmetrischen als auch jene der symmetrischen Verfahren der Anlage 2 entsprechen. Die Schlüssel sowie das Verfahren des Schlüsseltausches im Rahmen symmetrischer Verfahren müssen durch technische und organisatorische Vorkehrungen entsprechend dem Stand der Technik abgesichert werden. Die Schlüssel sind so zu verwahren, dass sie Dritten nicht zur Kenntnis gelangen können.

(4) Abweichend von der Anlage 2 dürfen zur Verschlüsselung gemäß Abs. 1 Z 3 auch andere Algorithmen und Parameter verwendet werden, wenn sie von einer Bestätigungsstelle gemäß § 19 SigG als denen der Anlage 2 zumindest gleichwertig festgestellt wurden. Gesundheitsdiensteanbieterinnen/Gesundheitsdiensteanbieter, die solche Algorithmen und Parameter verwenden wollen, haben die schriftliche Feststellung der Gleichwertigkeit der Bundesministerin/dem

Bundesminister für Gesundheit, Familie und Jugend vorzulegen, die/der die Bekanntmachung im Internet zu veranlassen hat. Als gleichwertig veröffentlichte Algorithmen und Parameter dürfen von allen Gesundheitsdiensteanbieterinnen/Gesundheitsdiensteanbietern ab dem der Veröffentlichung folgenden Tag im elektronischen Verkehr mit Gesundheitsdaten verwendet werden.

(5) Die für den Gesundheitsdatenaustausch gemäß Abs. 1 Z 3 maßgebenden Gründe, die technischen und organisatorischen Vorkehrungen im Sinne des Abs. 3 sowie Art, Umfang und Frequenz von Überprüfungen der Einhaltung dieser technischen und organisatorischen Vorkehrungen sind von der Gesundheitsdiensteanbieterin/vom Gesundheitsdiensteanbieter in einem Sicherheitskonzept darzustellen, das auf Anforderung der Bundesministerin/des Bundesministers für Gesundheit, Familie und Jugend oder einer/einem von ihr/ihm beauftragten Dritten offen zu legen ist.

Signaturen im elektronischen Verkehr mit Gesundheitsdaten

§ 12. (1) Beim elektronischen Verkehr mit Gesundheitsdaten gemäß § 11 Abs. 1 Z 3 sind zum Nachweis bzw. zur Prüfung der Integrität von Gesundheitsdaten gemäß § 7 Abs. 1 GTelG fortgeschrittene elektronische Signaturen zu verwenden.

(2) Die Signaturprüfung ist über eine gemäß § 6 Abs. 1 Z 9 in das GDA-Token aufgenommene Angabe sicherzustellen. Wurde eine solche Angabe nicht in das GDA-Token aufgenommen oder erfolgt der Nachweis bzw. die Prüfung von Identität und Rolle gemäß den §§ 4 Abs. 2 und 5 Abs. 3 GTelG, muss der Identifikationsbegriff gemäß § 6 Abs. 1 Z 3 oder § 10 Abs. 1 Z 1 GTelG den zu signierenden Gesundheitsdaten beigefügt werden und von der elektronischen Signatur umfasst sein.

(3) Der Schutz der Signaturerstellungsdaten gegen Missbrauch ist durch technische und organisatorische Maßnahmen entsprechend dem Stand der Technik zu gewährleisten und im Sicherheitskonzept gemäß § 11 Abs. 5 zu dokumentieren.

(4) Die Verpflichtung zur Dokumentation gemäß Abs. 3 besteht nicht, wenn qualifizierte elektronische Signaturen im Sinne des § 2 Z 3a SigG verwendet werden.

Schlussbestimmungen

§ 13. (1) Personenbezogene Bezeichnungen werden in dieser Verordnung in weiblicher und männlicher oder in geschlechtsneutraler Form verwendet. Sofern diese Bezeichnungen mangels Verfügbarkeit oder zur Erleichterung der technischen Umsetzung in geschlechtsspezifischer Form verwendet werden, beziehen sie sich auf Frauen und Männer in gleicher Weise.

(2) Diese Verordnung tritt mit 1. Jänner 2009 in Kraft.

(3) Die Bildung von GDA-Token ist nach Maßgabe der Verfügbarkeit der dafür erforderlichen Infrastruktur zu einem früheren Zeitpunkt zulässig.

Vorblatt

Problem:

Im Gesundheitstelematikgesetz ist für den elektronischen Gesundheitsdatenaustausch der Nachweis der rollenbasierten Identität festgelegt, wofür die konkret zu verwendenden Rollen definiert werden müssen. Weiters sind vom Gesundheitstelematikgesetz ergänzende Datensicherheitsmaßnahmen, wie etwa die Sicherstellung der Vertraulichkeit und der Integrität von Gesundheitsdaten, vorgesehen, deren qualitative Mindestanforderungen der Konkretisierung bedürfen.

Inhalt, Problemlösung:

Die für den elektronischen Gesundheitsdatenaustausch in Betracht kommenden Rollen sowie jene Stellen, die die Zuordnung von Rollen zu einer Gesundheitsdiensteanbieterin/einem Gesundheitsdiensteanbieter authentisch bestätigen, werden festgelegt. Das Konzept der rollenbasierten Identität wird anhand der Datenstruktur GDA-Token (elektronische Bescheinigung) präzisiert. Dabei wird – soweit wie möglich – auf bewährte Entwicklungen im E-Government Bedacht genommen. Die Mindestanforderungen für die Gewährleistung der Vertraulichkeit und die Unverfälschtheit der Gesundheitsdaten beim Gesundheitsdatenaustausch werden nicht zuletzt im Hinblick auf die zu verwendenden Zertifikate, Verschlüsselungsverfahren und elektronischen Signaturen festgelegt.

Alternativen:

Keine.

Auswirkungen des Regelungsvorhabens:

– Finanzielle Auswirkungen:

Die Umsetzung der Verordnungsinhalte ist mit einem finanziellen Mehraufwand verbunden, der auf Grund der Heterogenität der in der Praxis vorzufindenden technischen Umgebungen seriös nicht quantifiziert werden kann.

– Wirtschaftspolitische Auswirkungen:

Durch die festzulegenden Inhalte wird die Investitionssicherheit sowohl für Gesundheitsdiensteanbieter als auch für einschlägig tätige IT-Unternehmen erhöht. Die konzeptionelle Angleichung bzw. Einbindung der vorgesehenen Methoden und Verfahren in die E-Government-Strukturen kann einer breiteren Verwendung der Bürgerkartenfunktion im Gesundheitswesen zusätzliche Impulse geben.

– Auswirkungen auf die Verwaltungslasten für Unternehmen:

Unbeschadet vereinzelter Dokumentationspflichten werden keine wesentlichen Auswirkungen auf die Verwaltungslasten für Unternehmen verursacht.

– Auswirkungen in umweltpolitischer, konsumentenschutzpolitischer sowie sozialer Hinsicht:

Die Datensicherheitsmaßnahmen operationalisieren die Zielsetzung des GTelG zur Erhöhung der Datensicherheit und können damit wesentlich zur Verbesserung des Vertrauens der Bevölkerung (der Betroffenen) in den Umgang mit Gesundheitsdaten beitragen.

– Geschlechtsspezifische Auswirkungen:

Die Rollen (Anlage 1) sind – soweit wie möglich – geschlechtsneutral definiert, wodurch geschlechtsspezifische Bezeichnungen auf ein Mindestmaß reduziert werden konnten. Für manche Rollen stehen jedoch keine geschlechtsneutralen Bezeichnungen zur Verfügung bzw. erscheint in manchen Fällen die Verwendung geschlechtsspezifischer Formulierungen für elektronische Bescheinigungen schon auf Grund der Länge der Bezeichnung technisch nicht zweckmäßig. In diesen Fällen musste daher der geschlechtsspezifischen Formulierung der Vorzug gegeben werden.

Verhältnis zu Rechtsvorschriften der Europäischen Union:

Die vorgesehenen Regelungen fallen nicht in den Anwendungsbereich des Rechts der Europäischen Union.

Besonderheiten des Normerzeugungsverfahrens:

Keine.

Erläuterungen

Allgemeiner Teil

1. Umsetzung des Konzepts der rollenbasierten Identität

Das Gesundheitstelematikgesetz (GTelG) verfolgt die Intention, das Vertrauen und die Sicherheit im elektronischen Verkehr mit Gesundheitsdaten zu verbessern. Die Kernelemente dazu sind im Wesentlichen der Nachweis von Identität und Rolle sowie die Sicherstellung der Vertraulichkeit und der Unverfälschtheit von Gesundheitsdaten durch Verwendung kryptographischer Verfahren und elektronischer Signaturen. Für eine inhaltlich und ökonomisch zweckmäßige Umsetzung werden weitgehend in der Praxis verfügbare Instrumente und Werkzeuge sowie die vom E-Government entwickelten Verfahren und Methoden referenziert. Die intensive Einbettung in das E-Government wird nicht zuletzt durch die Bereitstellung bestimmter Funktionalitäten in der Bürgerkartenumgebung zur Umsetzung des GDA-Token-Konzepts evident.

Für den elektronischen Verkehr mit Gesundheitsdaten wird entsprechend dem Konzept der rollenbasierten Identität gefordert, dass für die Kommunikationspartner die Funktion, in der sie Gesundheitsdaten anfordern oder erhalten, in Verbindung mit der Identität überprüfbar ist. Für den qualitätsvollen Nachweis bzw. die Überprüfung der Rolle sieht das GTelG im Wesentlichen zwei Möglichkeiten vor: Einerseits durch eine elektronische Bescheinigung gemäß den §§ 4 Abs. 1 und 5 Abs. 2 GTelG, andererseits durch Überprüfung, ob ein Gesundheitsdiensteanbieter in den eHealth-Verzeichnisdienst (eHVD) eingetragen ist (§§ 4 Abs. 2 und 5 Abs. 3 GTelG). Für bestimmte Ausprägungen des elektronischen Verkehrs mit Gesundheitsdaten sind technisch bedingte abweichende Regelungen vorgesehen.

Die sich speziell an der sogenannten gerichteten Kommunikation orientierenden Regelungen werden für die künftigen Anforderungen der ungerichteten Kommunikation im Gesundheitswesen, aber auch im Hinblick auf neue elektronische Gesundheitsdienste, dynamisch weiterzuentwickeln sein.

2. Rollen im elektronischen Gesundheitsdatenaustausch

Es wird ein Set jener Rollen festgelegt, die bereits derzeit für den elektronischen Gesundheitsdatenaustausch von hoher Relevanz sind. Parallel dazu werden die Stellen („Bestandgeber“) festgelegt, die die Zuordnung der Rollen zu einem Gesundheitsdiensteanbieter authentisch bestätigen.

Das Basisset der Rollen wird entsprechend dem in der Praxis vorzufindenden Bedarf dynamisch zu ergänzen sein. In diesem Zusammenhang zu nennen ist insbesondere die Aufnahme weiterer Rollen für den elektronischen Gesundheitsdatenaustausch an den Nahtstellen zum Sozialwesen. Ebenso kann auch einem allfälligen zusätzlichen Bedarf für weitere Bestandgeber entsprochen werden.

3. Der GDA-Token als elektronische Bescheinigung

Die nähere Ausgestaltung der elektronischen Bescheinigung erfolgt mittels der XML-Datenstruktur GDA-Token, die mit einer elektronischen Signatur zu versehen und dem Gesundheitsdiensteanbieter elektronisch zur Verfügung zu stellen ist. Durch die Einbeziehung von Bestandgebern soll ein hoher Aktualitätsgrad der durch die Rollen manifestierten Berechtigungen erzielt werden.

Das Grundkonzept GDA-Token wird um die Bildung von GDA-Token für organisatorische Gliederungen ergänzt, womit dem seitens institutioneller Gesundheitsdiensteanbieter artikulierten Bedarf der Praxis Rechnung getragen wird.

4. Vertraulichkeit und Integrität

Der gleichsam professionelle Umgang mit sensiblen Daten bedingt hohe Anforderungen an die Vertraulichkeit und die Erkennbarkeit von Veränderungen während des Transports. Bei der Konkretisierung dieser Anforderungen muss jedoch einerseits den bereits eingeführten guten Praktiken und andererseits den - auch wirtschaftlich verkraftbaren - technischen Möglichkeiten Rechnung getragen werden, damit die Erreichung des Ziels einer verbesserten Datensicherheit nicht konterkariert wird. Eine differenzierte Vorgangsweise erschien aber auch deshalb geboten, weil „Sicherheit“, nämlich die Sicherheit konkreter Daten, die Netzwerksicherheit oder die Informationssicherheit ganz allgemein, kein statisch definierbarer Zustand ist, sondern den Kontext und seine potenziellen Veränderungen durch die (technische) Weiterentwicklung berücksichtigen muss. Ausgehend davon und unter Bedachtnahme auf die vorzufindende Praxis werden unterschiedliche Möglichkeiten zur Sicherstellung von Vertraulichkeit und Integrität von Gesundheitsdaten vorgeschlagen, die jedoch bereits aus der Reihenfolge ihrer Regelung eine deutliche Präferenz für ein höheres Sicherheitsniveau erkennen lassen. Stringente

Verschlüsselung(sverfahren) in Verbindung mit elektronischen Signaturen müssen demzufolge vor allem in jenen Fällen verwendet werden, in denen die präferierten Maßnahmen nicht in Betracht kommen. Aber auch diesbezüglich wurde auf praktikable Lösungen geachtet, indem etwa für die Verschlüsselung „marktgängige“ Verfahren festgelegt werden.

Besonders wird darauf hingewiesen, dass die Regelungen entsprechend den Vorgaben des GTelG Mindestanforderungen darstellen und es den GDA (bzw. den Dienstleistern) selbstverständlich unbenommen bleibt, diese zu überschreiten. Das Ziel, ein höheres Qualitätsniveau zu erreichen, ist insbesondere in Bezug auf die Signaturanforderungen klar zu erkennen.

Bewusst sein muss jedoch, dass Vertraulichkeit und Integrität von Gesundheitsdaten zwar als besondere, jedoch die Datensicherheit nicht vollständig charakterisierende Aspekte nicht allein durch den präventiven Einsatz technischer Werkzeuge, sondern insbesondere auch durch zusätzliche organisatorische Maßnahmen, die auch den Faktor Mensch als Nutzer der Technologien einbeziehen, zu verbessern sein werden.

5. Finanzielle Auswirkungen

Der für die Umsetzung der Verordnung erforderliche finanzielle Aufwand für die Gebietskörperschaften ist von mehreren, jedoch quantitativ (und qualitativ) weitgehend unbekannten Einflussgrößen entscheidend abhängig. Zum Einen sind dies Art und Anzahl der allenfalls zu adaptierenden Anwendungen, zum Anderen sind dies die jeweils festgelegten innerorganisatorischen Vorgaben.

Eine seriöse Quantifizierung des Aufwandes wäre daher nur bei ausreichender Kenntnis dieser jeweils spezifisch unterschiedlichen Einflussfaktoren möglich. Selbst der für die Bildung und Verwaltung von GDA-Token erforderliche Aufwand kann im Hinblick auf die im GTelG normierte Wahlfreiheit (Verwendung der elektronischen Bescheinigung oder Eintragung in den eHVD) nicht schlüssig bemessen bzw. durch die synergetische Abwicklung mit derselben Applikation nicht eindeutig zugeordnet werden. Als generisch kostenwirksam im Gefolge der Implementierung bzw. Verwendung der in dieser Verordnung vorgesehenen Mechanismen und Verfahren sind jedenfalls anzusehen:

- die Beantragung der Bildung von GDA-Token;
- die für die Bildung, Verwaltung und Dokumentation von GDA-Token erforderliche personelle und technische Infrastruktur;
- die Einbettung von GDA-Token in die jeweilige Betriebsumgebung;
- die Implementierung der Verschlüsselungsmechanismen und der elektronischen Signaturen in die jeweilige Betriebsumgebung einschließlich der Bereitstellung/Verfügbarkeit der dafür notwendigen Zertifikate;
- gegebenenfalls die Integration von Serverzertifikaten in den programmgesteuerten Gesundheitsdatenaustausch.

Eine Grobanalyse der verfügbaren Kennzahlen über den aktuellen Stand des elektronischen Verkehrs mit Gesundheitsdaten außerhalb des direkten Datenaustauschs zwischen der Sozialversicherung und ihren Vertragspartnern führte zum Ergebnis, dass die Krankenanstalten nahezu vollständig und eine hohe Anzahl der niedergelassenen Ärzte (insgesamt rd. 6.500) den Gesundheitsdatenaustausch schon derzeit über das Gesundheitsinformationsnetz abwickeln und daher diese Zielgruppen nicht mit unvertretbaren Kosten belastet werden. Die Einsetzbarkeit marktgängiger Verschlüsselungsverfahren, teilweise sogar kostenlos verfügbarer Produkte (Protokolle), die Verwendung fortgeschrittener Signaturen sowie die Nutzung personeller und infrastruktureller Synergien mit dem eHealth-Verzeichnisdienst werden überdies dazu beitragen, die Kosten so gering wie möglich zu halten.

Besonderer Teil

Zu § 1:

Die in Abschnitt A der Anlage 1 definierten Rollen stellen das Basisset dar; die Art und Anzahl der Rollen wird bei entsprechendem Bedarf zu erweitern sein. Ebenso wird die Granularität der Rollen anhand der Anforderungen der Praxis zu evaluieren sein. Abschnitt B der Anlage 1 enthält Rollen (Berufsbilder), die in verschiedenen Rechtsgrundlagen näher geregelt sind. Diese Rollen dürfen nicht freiberuflich ausgeübt werden, die Bildung von GDA-Token für diese Rollen ist nicht zulässig. Mit ihrer ergänzenden Darstellung wird daher lediglich eine gewisse begriffliche Harmonisierung, etwa bei ihrer Verwendung in internen Berechtigungssystemen, angestrebt.

Die in den Z 1 bis 23 des Abschnittes A genannten Rollen stellen auf Gesundheitsdiensteanbieter ab, die auf Grund der für sie jeweils geltenden berufsrechtlichen Vorschriften die Rollen auch freiberuflich ausüben können. Die in den Z 24 bis 52 genannten Rollen beziehen sich auf Gesundheitsdiensteanbieter, die im Gesundheitsdatenaustausch als Organisationen auftreten.

In den Z 1 bis 3 sind die Rollen der Allgemeinmediziner und Fachärzte, in den Z 4 bis 7 die Rollen der zahnmedizinischen Versorgung enthalten. In den Z 9 bis 23 finden sich die gesetzlich geregelten, freiberuflich ausübbaren, nicht-ärztlichen Gesundheitsberufe. Die in den Z 32 bis 36 angeführten Rollen beziehen erste gewerbliche Einrichtungen ein.

Hinsichtlich der Rolle Krankenanstalt wurde auf eine weitergehende Differenzierung verzichtet; der Z 24 sind somit alle Krankenanstalten gemäß § 2 Abs. 1 Z 1 bis 6 KAKuG zuzuordnen. Als Grobraster für die organisatorischen Gliederungen einer Krankenanstalt sollen in erster Linie folgende Organisationsbezeichnungen herangezogen werden: Referenzzentrum, Abteilung, Department, Fachschwerpunkt, Interdisziplinäre Einrichtung, Tagesklinik, Ambulanz, Verwaltung. Sie sind – wie auch die Gliederungen anderer Gesundheitsdiensteanbieter - im Zuge der Antragstellung entsprechend den eingeführten bzw. in der Kommunikation nach außen üblichen Bezeichnungen näher zu präzisieren. Zur Abgrenzung der Z 24 und 25 sind insbesondere die diesbezüglichen Bewilligungsbescheide bzw. der Krankenanstalten-Kataster heranzuziehen.

Der Z 37 sind ausschließlich auf gesundheitsbezogene Notfälle spezialisierte Einrichtungen, die auch eine medizinische Erstversorgung durchführen, zuzuordnen. Nicht darunter fallen andere im allgemeinen Sprachgebrauch als solche bezeichnete Rettungsorganisationen, wie etwa die Feuerwehr.

Der Z 40 sind alle im Hauptverband zusammengeschlossenen Sozialversicherungsträger zugeordnet. Die mit unterschiedlicher Bezeichnung und Trägerschaft eingerichteten Krankenfürsorgeeinrichtungen (einschließlich der Unfallfürsorge) sind der in Z 42 zusammengefasst. Für die Z 45 kommen jene Rechtsträger in Betracht, die private Versicherungen für gesundheitsbezogene Risiken anbieten. Z 46 ist für Betriebsgesellschaften, Verbünde oder Holdings, aber auch für konfessionelle und private Rechtsträger sowie Gebietskörperschaften als Träger heranzuziehen. Die Abgrenzung, insbesondere zu Z 47, ist anhand der Umstände des Einzelfalles vorzunehmen. Die Z 47 ist für die Verwaltungseinrichtungen (Geschäftsapparate) und Behörden (z.B. Bezirksverwaltungsbehörden, Magistrate) der Gebietskörperschaften, aber auch für institutionalisierte Planungseinrichtungen der Gesundheitsverwaltung, vorgesehen. Unter Patientenvertretung (Z 48) sind Patientenanwaltschaften, Pflegeanwaltschaften und Vereinssachwalterschaften u.dgl. - unbeschadet ihrer jeweiligen rechtlichen Konstruktion - zu verstehen. In Bezug auf die Dienstleister (gemäß Definition des DSG 2000) wurde zunächst auf eine Differenzierung verzichtet, ein allfälliger Bedarf für spezielle Dienstleister-Rollen wird daher zu evaluieren sein.

Die Festlegung jener Stellen, die zur authentischen Bestätigung von Rollen berechtigt sind (Bestandgeber), geht davon aus, dass die angeführten Stellen über eine für diese Tätigkeit erforderliche ausreichende technisch-organisatorische Infrastruktur verfügen und/oder auf der Grundlage besonderer Rechtsvorschriften bereits derzeit Verzeichnisse führen und somit über die notwendigen Beurteilungsgrundlagen der Berechtigung zur Ausübung der Rolle(n) verfügen.

Zu § 2:

Das Konzept des „GDA-Tokens“ stellt die Umsetzung der elektronischen Bescheinigung im Sinne der §§ 4 Abs. 1 bzw. 5 Abs. 2 GTelG dar. Im GDA-Token erfolgt die elektronische Verknüpfung von Identität und Rolle(n) gemäß dem Konzept der rollenbasierten Identität. Grundsätzlich ist für jede Rolle ein GDA-Token zu bilden; mehrere Rollen können jedoch dann in einem GDA-Token enthalten sein, wenn zur Bestätigung aller Rollen derselbe Bestandgeber berechtigt ist.

Mit der Zulässigkeit der Bildung von GDA-Token für Organisationsformen ohne eigene Rechtspersönlichkeit, insbesondere auch für deren organisatorischen Gliederungen, wird einer Forderung vor allem aus dem Krankenanstaltenbereich Rechnung getragen, bei denen der elektronische Gesundheitsdatenaustausch vorwiegend auf der Ebene dieser Entitäten abgewickelt wird.

Zu § 3:

GDA-Token werden – sofern für ihre initiale Bildung nicht die Ausnahmeregelung des § 8 zum Tragen kommt – nur auf Grund eines elektronisch signierten Antrages gebildet. Für die vertretungsweise Antragstellung von Organisationen bedarf es der in Abs. 2 aufgenommenen Regelung.

Da mit dem Antrag aus Synergiegründen gleichzeitig die Registrierung im eHealth-Verzeichnisdienst beantragt werden kann, müssen die Antragsdaten für die Bildung des GDA-Tokens weitgehend mit den Antragsdaten für die Registrierung übereinstimmen. Die Kennung (OID) wird zur Sicherstellung der Eindeutigkeit von der Bundesministerin/vom Bundesminister für Gesundheit, Familie und Jugend vergeben.

Zu § 4:

Die Vollständigkeit und die Plausibilität des Antrages werden vor allem durch die in die Antragsapplikation integrierten Routinen geprüft. Die Prüfung der Identität erfolgt über die Register des E-Government (Stammzahl- und Ergänzungsregister). Als Identifikationsbegriff für das GDA-Token ist der Health Professional Identifier - HPI als Einweg-Ableitung des bPK zu bilden bzw. die Stammzahl zu verwenden.

Zu § 5:

Bei der Prüfung der Berechtigung zur Ausübung der vom Antragsteller angegebenen Rolle(n) hat der Bestandgeber geeignete Informationen beim Antragsteller oder bei Dritten einzuholen, falls die Angaben im Antrag oder eigene Informationen keine abschließende Beurteilung zulassen. Sowohl die Bestätigung als auch die Ablehnung der Bestätigung einer Rolle ist vom Bestandgeber zu signieren; die dafür zu verwendenden Zertifikate werden von der Bundesministerin/vom Bundesminister für Gesundheit, Familie und Jugend zur Verfügung gestellt.

Zu § 6:

Das GDA-Token wird auf der Grundlage der vom Bestandgeber bestätigten Rolle(n) gebildet. Die in das GDA-Token aufzunehmenden Daten müssen insbesondere auch die Prüfkette im Kontext der zu verwendenden Signaturen sicherstellen. Die Zustellung kann im Wege von Zustelldiensten oder durch Abholung auf Grund einer entsprechenden elektronischen Benachrichtigung erfolgen. Wurde auch die Registrierung im eHealth-Verzeichnisdienst beantragt, erfolgen diese Vorgänge parallel. Die Ableitung der Kennung (OID) impliziert, dass GDA-Token für organisatorische Gliederungen erst dann gebildet werden können, wenn ein solches für den organisatorisch übergeordneten Gesundheitsdiensteanbieter bereits besteht. Ebenso ist die Rolle des organisatorisch übergeordneten Gesundheitsdiensteanbieters zu übernehmen.

Zu § 7:

GDA-Token (wie auch die Registrierung im eHVD) sind zeitlich befristet und nach Zeitablauf automationsunterstützt für ungültig erklärt (widerrufen). Vorzeitig notwendige Maßnahmen (Sperre oder Widerruf) wegen befristeten oder dauernden Wegfalls der mit der Rolle verbundenen Berechtigung werden im Wesentlichen auf Grund bereits bestehender Meldepflichten oder sonstiger Kenntnis (z.B. Disziplinarmaßnahmen) von den Bestandgebern zu veranlassen sein. Der dafür notwendige Dienst ist von der Bundesministerin/vom Bundesminister für Gesundheit, Familie und Jugend vorzuhalten.

Zu § 8:

Um für Gesundheitsdiensteanbieter, die bereits in einschlägigen Verzeichnissen registriert sind, eine ökonomisch zweckmäßige Vorgangsweise für die Bildung von GDA-Token zur Verfügung zu stellen, ist eine automationsunterstützte Übernahme der für die initiale Bildung von GDA-Token erforderlichen Daten vorgesehen. Voraussetzung für eine solche Datenübernahme ist allerdings die Sicherstellung der Datenqualität, die Einhaltung der Datenformat- und sonstigen Vorgaben (Schnittstellendefinitionen) und die Berücksichtigung der Freiwilligkeit.

Zu § 9:

Alle Vorgänge betreffend Antragstellung, Bildung, Bereitstellung und Ungültigerklärung von GDA-Token sind zu dokumentieren. Die Aufbewahrungsfrist der Dokumentation wurde mit der doppelten maximalen Gültigkeitsdauer des GDA-Tokens bemessen.

Zu § 10:

Für den programmgesteuerten Gesundheitsdatenaustausch (Serverkommunikation) sind Serverzertifikate zu verwenden, die technisch die Anforderungen für qualifizierte Zertifikate gemäß SigG erfüllen müssen. Sie müssen ferner in einer Zertifikatserweiterung (Attribut) eine abgeleitete Kennung (OID) des Gesundheitsdiensteanbieters enthalten. Für ihre Verwendung sind spezielle Dokumentationsanforderungen vorgesehen.

Zu § 11:

Abs. 1 normiert die zur Sicherstellung von Vertraulichkeit und Integrität bestehenden Möglichkeiten in der aus der Sicht der Datensicherheit zu präferierenden Reihenfolge. Obwohl der Begriffsinhalt der „hinreichenden“ Absicherung des für den Gesundheitsdatenaustausch verwendeten Netzwerks (Z 1) auf Grund der Dynamik der technologischen Entwicklung nicht abschließend beschrieben werden kann, können doch wesentliche Elemente für seine Eingrenzung detektiert werden: Das Netzwerk ist durch entsprechende Vorkehrungen zumindest logisch gegenüber anderen Netzen abgegrenzt, eine physikalische Trennung kann, muss aber nicht erfolgen. Die Schutzmechanismen bestehen sowohl aus

technischen als auch aus organisatorischen Vorkehrungen. Technische Vorkehrungen bestehen insbesondere in der kryptographischen Absicherung des Datenverkehrs end-to-end, beispielsweise durch Verwendung von Tunneltechnologien, der Vorhaltung von Intrusion-Detection- und/oder Intrusion-Prevention-Systemen, bis hin zu (konfigurierbaren) Firewall-Systemen, Honeypots u. dgl. mehr bis hin zu Maßnahmen im Kontext sogenannter kritischer Infrastruktur. Organisatorische Vorkehrungen regeln den Zugang zum Netz, der zumeist nur einer geschlossenen oder abgrenzbaren Benutzergruppe gewährt und durch Authentisierungs- und Autorisierungsmechanismen sichergestellt wird. Darüber hinaus sehen organisatorische Vorkehrungen auch besondere Betriebsbedingungen (z.B. redundante Systeme, Datensicherung, Protokollierung) sowie die Überprüfung (Audits) der Maßnahmen zur Risikominimierung vor. Vereinzelt wird von Netzbetreibern bereits eine Sicherheitszertifizierung nach anerkannten Standards, von denen insbesondere der BS 7799, die ITIL oder der Common Criteria-Standard zu nennen sind, verlangt. Ausgehend davon, kann mit guten Gründen angenommen werden, dass insbesondere der Gesundheitsdatenaustausch über das als Teil der e-card-Infrastruktur betriebene Gesundheitsinformationsnetz (GIN), das aus zwei logisch von einander getrennten und nach außen abgeschotteten Netzen besteht, die Anforderungen der Z 1 nicht nur hinsichtlich des SV-VPN, über das die SV-Dienste und Anwendungen abgewickelt werden, sondern auch hinsichtlich des MWD-VPN, über das die sogenannten Mehrwertdienste durch private Dienstleister („Befundprovider“) abgewickelt werden, erfüllt.

Die Z 2 referenziert eine weitere Möglichkeit des Gesundheitsdatenaustausches, bei der zwar nicht die umfassenden Anforderungen der Z 1 erfüllt werden, jedoch durch entsprechende technische Vorkehrungen die Vertraulichkeit und Integrität sichergestellt erscheinen. Diese technischen Vorkehrungen betreffen insbesondere die Verwendung marktüblicher Kommunikations- bzw. Netzwerkprotokolle, die überwiegend (aber nicht ausschließlich) auf den Schichten 2 bis 4 des OSI-Referenzmodells aufsetzen (z.B. IPsec, SSL, TLS, SSH) und/oder darauf aufbauende Tunneltechniken (z.B. VPN) verwenden. Da diese Protokolle, wenn sie dem Stand der Technik entsprechen, die Verschlüsselung und den Nachweis der Integrität (über Hashfunktionen) von Daten ermöglichen, sind aus der Sicht der geforderten Datensicherheit zusätzliche Maßnahmen im Sinne der §§ 6 und 7 GTelG nicht erforderlich. Es gibt allerdings auch Protokolle und Verfahren, bei denen sogenannte Header-Informationen oder Authentifizierungsprozeduren von der Verschlüsselung nicht umfasst sind. Abs. 2 zweiter Satz stellt daher klar, dass erstere keinen Personenbezug enthalten dürfen und die Verwendung letzterer unzulässig ist, da sie in Bezug auf den Schutz gegenüber Dritten nicht dem geforderten Stand der Technik entsprechen.

Z 3 in Verbindung mit den Abs. 3 bis 5 und § 12 regeln die qualitativen Anforderungen zur Sicherstellung der Vertraulichkeit und Integrität von Gesundheitsdaten, wenn der Gesundheitsdatenaustausch gemäß Z 1 oder 2 nicht in Betracht kommt. Demnach sind für die Verschlüsselung die in Anlage 2 genannten marktgängigen Algorithmen und Parameter zu verwenden und die Gesundheitsdaten elektronisch zu signieren. Darüber hinaus können auch Algorithmen und Parameter zu Verschlüsselung eingesetzt werden, wenn deren Gleichwertigkeit zu denen der Anlage 2 festgestellt und veröffentlicht wurde.

Mit diesen Bestimmungen wird nunmehr klargestellt, dass der Gesundheitsdatenaustausch mit herkömmlichen analogen Faxgeräten die Verwendung eines unsicheren Mediums im Sinne des § 6 GTelG darstellt, weil damit die Vertraulichkeit und die Integrität der Gesundheitsdaten nicht wirksam sichergestellt werden können. Dies kann aber auch auf den Gesundheitsdatenaustausch über ein ungesichertes WLAN oder über andere technisch mögliche Lösungen zutreffen. Diesbezüglich muss allerdings die abschließende (Risiko-)Beurteilung und die Umsetzung allenfalls notwendiger Maßnahmen durch den Nutzer erfolgen.

Zu § 12:

Als Mindestanforderung im Sinne des GTelG wird die Verwendung fortgeschrittener elektronischer Signaturen festgelegt. Für ein entsprechend hohes Qualitätsniveau können (und sollen) selbstverständlich auch qualifizierte elektronische Signaturen verwendet werden. Die Signaturprüfung ist durch die Aufnahme von Zertifikaten bzw. Referenzen sicherzustellen, anderenfalls hat die Einbindung des Identifikationsbegriffs in die Signatur zu erfolgen.

Mit den Dokumentationspflichten kann zwar die Qualifikation als fortgeschrittene Signatur erleichtert, nicht jedoch das den fortgeschrittenen Signaturen inhärente Problem der Erkennbarkeit der qualitätsvollen Erstellung beseitigt werden. Eine diesbezüglich generelle Lösung wird vermutlich nur in der Adaptierung der Signaturvorschriften zu finden sein. Bei der Verwendung qualifizierter Signaturen tritt dieses Problem nicht auf, weshalb die Dokumentationsverpflichtung entfällt.

Zu § 13:

Das In-Kraft-Treten der Verordnung orientiert sich an der Übergangsbestimmung des § 19 Abs. 2 GTelG. Um eine möglichst reibungslose Implementierung zu gewährleisten, kann jedoch entsprechend der Verfügbarkeit der dafür erforderlichen Infrastruktur das vorgesehene Instrumentarium bereits zu einem früheren Zeitpunkt verwendet werden.

BMGFJ-72300/0024-I/A/15/2008

Verordnung der Bundesministerin für Gesundheit, Familie und Jugend, mit der die für den elektronischen Gesundheitsdatenaustausch in Betracht kommenden Rollen, die die Rollen bestätigenden Stellen, sowie die qualitativen Mindestanforderungen für Verschlüsselung und elektronische Signaturen festgelegt werden - Gesundheitstelematikverordnung (GTelV); Begutachtungsverfahren

Sehr geehrte Damen und Herren!

Das Bundesministerium für Gesundheit, Familie und Jugend übermittelt in der Anlage den im Betreff genannten Entwurf.

Dieser Entwurf samt Materialien sowie die Liste der Adressaten sind auch im E-Recht verfügbar.

Das Bundesministerium für Gesundheit, Familie und Jugend ersucht zu dem übermittelten Verordnungsentwurf

bis längstens 5. September 2008

Stellung zu nehmen und die Stellungnahmen (auch) auf elektronischem Weg an die Adresse begutachtung@bmgfj.gv.at zu übermitteln.
Sollte bis zu diesem Zeitpunkt keine Stellungnahme eingelangt sein, wird angenommen, dass von Ihrer Seite keine Bedenken bestehen.

Es wird darauf hingewiesen, dass dieses Begutachtungsverfahren auch als Befassung gemäß Art. 1 Abs. 2 und 4 der Vereinbarung zwischen dem Bund, den Ländern und den Gemeinden über einen Konsultationsmechanismus und einen künftigen Stabilitätspakt der Gebietskörperschaften, BGBl. I Nr. 35/1999, anzusehen ist.

Mit freundlichen Grüßen
Für die Bundesministerin:
SL Dr. Clemens Martin AUER

Anlage 1: Rollen

Abschnitt A:

1. Approbierter Arzt
2. Arzt für Allgemeinmedizin
3. Facharzt, unter Beifügung des Wortes „für“ und des folgenden, jeweils zutreffenden Sonderfachs
   – Anästhesiologie und Intensivmedizin
   – Anatomie
   – Arbeitsmedizin
   – Augenheilkunde und Optometrie
   – Blutgruppenserologie und Transfusionsmedizin
   – Chirurgie
   – Frauenheilkunde und Geburtshilfe
   – Gerichtsmedizin
   – Hals-, Nasen- und Ohrenkrankheiten
   – Haut- und Geschlechtskrankheiten
   – Herzchirurgie
   – Histologie Embryologie
   – Hygiene und Mikrobiologie
   – Immunologie
   – Innere Medizin
   – Kinder- und Jugendchirurgie
   – Kinder- und Jugendheilkunde
   – Kinder- und Jugendpsychiatrie
   – Lungenkrankheiten
   – medizinische Biophysik
   – medizinische Genetik
   – medizinische und chemische Labordiagnostik
   – medizinische Leistungsphysiologie
   – Mund-, Kiefer- und Gesichtschirurgie
   – Neurobiologie
   – Neurochirurgie
   – Neurologie
   – Neuropathologie
   – Nuklearmedizin
   – Orthopädie und orthopädische Chirurgie
   – Pathologie
   – Pathophysiologie
   – Pharmakologie und Toxikologie
   – physikalische Medizin und allgemeine Rehabilitation
   – Physiologie
   – plastische, ästhetische und rekonstruktive Chirurgie
   – Psychiatrie und psychotherapeutische Medizin
   – Radiologie
   – Sozialmedizin
   – spezifische Prophylaxe und Tropenmedizin
   – Strahlentherapie-Radioonkologie
   – Thoraxchirurgie
   – Unfallchirurgie
   – Urologie
   – Virologie
4. Facharzt für Zahn-, Mund- und Kieferheilkunde

5. Zahnarzt
6. Approbierter Zahnarzt
7. Dentist
8. Psychotherapeutischer Dienst
9. Klinisch-psychologischer Dienst
10. Gesundheitspsychologischer Dienst
11. Musiktherapeutischer Dienst
12. Hebamme
13. Physiotherapeutischer Dienst
14. Medizinisch-technischer Laboratoriumsdienst
15. Radiologisch-technischer Dienst
16. Diätdienst und ernährungsmedizinischer Beratungsdienst
17. Ergotherapeutischer Dienst
18. Logopädisch-phoniatrisch-audiologischer Dienst
19. Orthoptischer Dienst
20. Allgemeine Gesundheits- und Krankenpflege
21. Kinder- und Jugendlichenpflege
22. Psychiatrische Gesundheits- und Krankenpflege
23. Heilmasseur
24. Krankenanstalt
25. Ambulatorium
26. Gesundheitsversorgung Strafvollzug
27. Kuranstalt
28. Öffentliche Apotheke
29. Organ-, Gewebe- oder Stammzellspende
30. Blutspende/Eigenblutvorsorge
31. Untersuchungseinrichtung
32. Augenoptik
33. Kontaktlinsenoptik
34. Bandagist
35. Hörgeräteakustik
36. Orthopädietechnik
37. Rettung
38. Patiententransport
34. Pflege und Altenbetreuung
39. Hauptverband der Sozialversicherungsträger
40. Sozialversicherungsträger
41. Zuschusskasse öffentlichen Rechts
42. Krankenfürsorge
43. Privatkrankenanstaltenfinanzierung
44. Betriebskrankenkasse
45. Personenversicherung Gesundheitsrisiken
46. Krankenanstaltenträger
47. Gesundheitsverwaltung
48. Patientenvertretung
49. Forschung
50. Lehre
51. Statistik
52. Dienstleister Gesundheitswesen

Abschnitt B:

1. Amtsarzt

2. Amtszahnarzt
3. Polizeiarzt
4. Arbeitsinspektionsarzt
5. Schularzt
6. Notarzt
7. Konsiliararzt
8. Turnusarzt
9. Apotheker
10. Anstaltsapotheker
11. Konsiliarapotheker
12. Krankenhaushygieniker
13. Hygienebeauftragter
14. Kardiotechnischer Dienst
15. Pflegehilfe
16. Medizinisch-technischer Fachdienst
17. Medizinischer Masseur
18. Rettungssanitäter
19. Notfallsanitäter
20. Operationshilfe
21. Laborhilfe
22. Prosekturhilfe
23. Ordinationshilfe
24. Heilbadhilfe
25. Ergotherapiehilfe
26. Desinfektionshilfe

Anlage 2: Verschlüsselung

1. Als asymmetrische Verfahren sind zur Verschlüsselung Algorithmen und Parameter entsprechend dem jeweiligen Stand der Technik geeignet, die hinsichtlich ihrer Schlüssellänge und Verwendbarkeit der qualifizierten elektronischen Signatur im Sinne § 2 Z 3a SigG entsprechen.
2. Als asymmetrische Verfahren sind zum Schlüsselaustausch geeignet, wobei die Schlüssellänge jeweils mindestens der qualifizierten elektronischen Signatur gemäß § 2 Z 3a SigG entsprechen muss:
   - Diffie Hellman (DH) [RFC 3370]
   - Elliptic Curve Diffie Hellman (ECDH) [RFC3278] [IEEE1363]
   - PKCS#1 v1.5 [RFC3370].
   - RSAES-OAEP [RFC3560]
3. Als symmetrische Verfahren sind geeignet, wobei eine effektive Schlüssellänge von mindestens 100 Bit gegeben sein muss:
   - Advanced Encryption Standard (AES) [FIPS197]
   - TripleDES [ANSI X9.52]

   jeweils in CBC oder CTR Modus [NIST 800-38A]
4. Die in den Verfahren zur Schlüsselerzeugung, zur Verschlüsselung oder zum Schlüsseltausch verwendeten Zufallszahlen müssen den Anforderungen an physikalische Zufallszahlengeneratoren trueran oder Pseudozufallszahlengeneratoren pseuran des Anhanges zur Signaturverordnung, SigV, BGBl. II Nr. 527/2004, entsprechen. Ein Initialisieren von Pseudozufallszahlengeneratoren (pseuran) mit einer echten Zufallszahl (trueran) ist nicht erforderlich.

Abkürzungen (zitierte Referenzen):

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

[FIPS197] „Advanced Encryption Standard (AES)“, National Institute of Standards and Technology (NIST), Federal Information Processing Standards Publication, FIPS 197, November 2001.

[IEEE1363] „Standard Specifications For Public Key Cryptography“, Institute of Electrical and Electronics Engineers, IEEE P1363, 2000.

[NIST 800-38A] M. Dworkin: „Recommendation for Block Cipher Modes of Operation“, National Institute of Standards and Technology, NIST Special Publication 800-38A, 2001.

[RFC3278] S. Blake-Wilson, D. Brown, P. Lambert: „Use of Elliptic Curve Cryptography (ECC) Algorithms in Cryptographic Message Syntax (CMS)“, Internet Engineering Task Force, IETF RFC 3278, April 2002.

[RFC3370] R. Housley: „Cryptographic Message Syntax (CMS) Algorithms“, Internet Engineering Task Force, IETF RFC 3370, August 2002.

[RFC3560] R. Housley: „Use of the RSAES-OAEP Key Transport Algorithm in Cryptographic Message Syntax (CMS)“, Internet Engineering Task Force, IETF RFC 3560, July 2003.