

Beschluss
der Bundesregierung
zur
**Sicherheit im elektronischen Rechts- und Geschäftsverkehr
mit der Bundesverwaltung**

vom 16. Januar 2002

I.
Beschluss

Mit dem Ziel, beim elektronischen Rechts- und Geschäftsverkehr mit ihren Partnern (Bürgerinnen und Bürger, Wirtschaft, Verwaltungen)

- rechtsverbindlich zu handeln und
- IT-Grundschutz zu gewährleisten,

strebt die Bundesregierung Sicherheitsmaßnahmen an, die für die jeweilige Anwendung oder Nutzung erforderlich und angemessen sind. Das erstreckt sich auf Vertraulichkeit (Schutz vor unbefugter Kenntnisnahme), Integrität (Schutz vor Manipulation), Authentizität (Schutz vor gefälschter Identität / Herkunft) und Verfügbarkeit (Schutz vor Ausfall der IT-Systeme) der Kommunikation.

Mit dem Ziel, die Leichtigkeit des elektronischen Rechts- und Geschäftsverkehrs zu fördern, sollen einheitliche Standards genutzt werden.

Die Maßnahmen umfassen

- den anwendungsbezogenen flächendeckenden Einsatz qualifizierter elektronischer Signaturen als eine Grundlage für die e-Government-Initiative "BundOnline2005",
- den flächendeckenden Einsatz von IT-Grundschutz für elektronische Kommunikation an den Arbeitsplätzen, sofern nicht Maßnahmen getroffen werden, die ein höheres Sicherheitsniveau garantieren, und
- die Gewährleistung größtmöglicher Wirtschaftlichkeit durch anwendungsbezogen angemessene Sicherheit und Ausstattung der Behörden auf Basis einheitlicher Standards, insbesondere ISIS-MTT.

1.

Kommunikation von der Bundesverwaltung zu ihren Kommunikationspartnern

Die Bundesverwaltung stellt in ihren eigenen Anwendungen für das eGovernment Sicherheitsmaßnahmen zur Verfügung und berücksichtigt die Sicherheitsanforderungen ihrer Kommunikationspartner.

Sie wird hierzu

- 1.1. Dokumente mit einer qualifizierten elektronischen Signatur versehen, soweit dies aufgrund von Formvorschriften (Rechtsverbindlichkeit) oder aufgrund der Anwendung erforderlich oder geboten ist,
- 1.2. E-Mails zum Schutz der Integrität und Authentizität nachprüfbar mit einer Absenderkennung versehen und zum Schutz der Vertraulichkeit auf der Grundlage allgemein bekannter Verfahren verschlüsseln, wenn der Adressat dazu sein Zertifikat mit seinem öffentlichen Schlüssel zur Verfügung stellt,
- 1.3. bei Online-Transaktions-Dienstleistungen Mechanismen zur Authentisierung und Verschlüsselung zur sicheren Identifikation und zum Schutz der Vertraulichkeit anbieten sowie
- 1.4. Standardsicherheitsmaßnahmen zur Gewährleistung der Verfügbarkeit ihrer Anwendungen umsetzen.

Die Bundesverwaltung stellt sicher, dass ihren Kommunikationspartnern kostenlos eine Verifikationssoftware zur Überprüfung von Rechtsverbindlichkeit, Integrität und Authentizität der Kommunikation der Bundesverwaltung zur Verfügung steht.

2.

Kommunikation zur Verwaltung

Den Kommunikationspartnern der Bundesverwaltung sollen ausreichend sichere, anwenderfreundliche und kostengünstige Verfahren für die Kommunikation mit der Bundesverwaltung zur Verfügung stehen. Die Bundesregierung fördert dies. Dabei soll es den Kommunikationspartnern im Rahmen der rechtlichen Anforderungen freistehen, welche Mittel sie für die Sicherheit der Kommunikation wählen.

Die Bundesverwaltung wird

- 2.1. elektronische Signaturen und Absenderkennungen ihrer Kommunikationspartner zur Prüfung der Rechtsverbindlichkeit, Integrität und Authentizität akzeptieren, soweit sie eine anwendungsbezogenen ausreichende Sicherheit gewährleisten und das übermittelte elektronische Dokument für die jeweilige Behörde zur Bearbeitung geeignet ist,
- 2.2. ihre Zertifikate mit den öffentlichen Schlüsseln zur Verschlüsselung von E-Mail zur Verfügung stellen (Schutz der Vertraulichkeit) und
- 2.3. die Daten ihrer Kommunikationspartner bei Online-Transaktionen verschlüsseln.

II. Begründung und Erläuterungen zur Umsetzung

1. Allgemeines

Durch den Beschluss soll insbesondere der rechtsverbindliche und sichere elektronische Rechts- und Geschäftsverkehr (eGovernment) der Bundesverwaltung mit ihren Partnern (Bürgerinnen und Bürger, Wirtschaft, Verwaltungen) gefördert werden:

- Durch die Nutzung qualifizierter elektronischer Signaturen in der Verwaltung und bei ihren Kommunikationspartnern kann die Rechtsverbindlichkeit signierter elektronischer Dokumente bei Anwendungen mit Schriftformerfordernis erreicht und darüber hinaus bei einer breiten Palette weiterer Anwendungen die Beweiskraft erhöht werden.
- IT-Grundschutz beim elektronischen Geschäftsverkehr (Vertraulichkeit, Integrität, Authentizität) wird insbesondere durch die Bereitstellung von Zertifikaten zur Kommunikationssicherheit von E-Mail-Verkehr und Online-Transaktionen erreicht.
- Die Leichtigkeit des elektronischen Rechts- und Geschäftsverkehrs wird durch Schaffung geeigneter Rahmenbedingungen, insbesondere die breite Verwendung einheitlicher Standards, und den Abbau technischer, administrativer und sonstiger Hemmnisse gefördert.

Die Sicherheitsmaßnahmen sind eine wichtige Voraussetzung für die Umsetzung des Programms BundOnline 2005, in dessen Rahmen alle online-fähigen Dienstleistungen der Bundesverwaltung bis 2005 im Internet angeboten werden sollen. Die Bundesregierung unternimmt die notwendigen Schritte zur Implementierung von Signatur- und Verschlüsselungstechniken in der Verwaltung im Rahmen des Umsetzungsplans. In zahlreichen Anwendungen, auch in Formular- und Vorgangsbearbeitungssystemen sowie in digitalen Archivierungssystemen müssen Signatur, Authentisierung und Verschlüsselung integriert werden.

Auch vor dem Hintergrund der aktuellen Bedrohungslage nach dem 11. September 2001 erscheint es angezeigt, eine umfassende Sicherheit des elektronischen Rechts- und Geschäftsverkehrs zu gewährleisten.

Die Maßgabe einer anwendungsbezogen angemessenen Sicherheit gewährleistet größtmögliche Wirtschaftlichkeit.

2. Rechtlicher Rahmen

Mit der Neufassung des Signaturgesetzes und den Gesetzesvorhaben zur Anpassung der Formvorschriften, die eine Gleichstellung der qualifizierten elektronischen Signatur mit der eigenhändigen Unterschrift im Privatrecht und im öffentlichen Recht ermöglichen, gibt der Bund ein Signal für den breiten Einsatz elektronischer Signaturen.

a) Signaturgesetz und Signaturverordnung

Mit dem Signaturgesetz von 1997 hat Deutschland im internationalen Vergleich eine führende Rolle eingenommen. Das Gesetz hat wichtige Impulse gegeben für die Richtlinie 1999/93/EG vom 13. Dezember 1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen (im Folgenden *Richtlinie* genannt).

Das neue „Gesetz über Rahmenbedingungen für elektronische Signaturen (Signaturgesetz – SigG)“ vom 16. Mai 2001 (BGBl. I S. 876) ist am 22. Mai 2001, die Signaturverordnung vom 16. November 2001 (BGBl. I S. 3074) am 22. November 2001 in Kraft getreten. Die novellierten Rechtsvorschriften setzen die Richtlinie um und tragen gleichzeitig den Ergebnissen der Evaluierung des Signaturgesetzes von 1997 Rechnung.

b) Anerkennung der elektronischen Form im Privat- und öffentlichen Recht

Das Gesetz zur Anpassung der Formvorschriften des Privatrechts und anderer Vorschriften an den modernen Rechtsgeschäftsverkehr vom 13. Juli 2001 (BGBl. I S. 1542) ist am 1. August 2001 in Kraft getreten und schafft die Grundlage für die Einführung der elektronischen Form im Privatrecht. Mit der neuen Vorschrift in § 126a BGB wird die elektronische Form zur Alternative für die eigenhändige Unterschrift.

Das 3. Gesetz zur Änderung verwaltungsverfahrenrechtlicher Vorschriften des Bundes (Verwaltungsverfahrensgesetz, Sozialgesetzbuch X und Abgabenordnung) wird derzeit erarbeitet. Damit soll auch in Verwaltungsverfahren rechtsverbindliches elektronisches Handeln weitestgehend ermöglicht werden. Vergleichbare Regelungen sollen in den Verwaltungsverfahrenen der Länder getroffen werden.

Diese Gesetze regeln, dass die Schriftform durch die mit einer qualifizierten elektronischen Signatur verbundene elektronische Form ersetzt werden kann. Bei Anwendungen ohne Formerfordernis kann weiterhin jede Form elektronischer Kommunikation verwendet werden.

3.

Umsetzung in der Bundesverwaltung

a) Kommunikation von der Bundesverwaltung zu ihren Kommunikationspartnern

zu 1.1. des Beschlusses:

Die Bundesverwaltung wird Dokumente mit einer qualifizierten elektronischen Signatur versehen, soweit dies aufgrund von Formvorschriften (Rechtsverbindlichkeit) oder aufgrund der Anwendung erforderlich oder geboten ist.

Für eGovernment-Anwendungen mit Schriftformerfordernis kommen qualifizierte elektronische Signaturen flächendeckend zum Einsatz. Die technischen Voraussetzungen sind gegeben. Hierbei wird nach heutigem Stand der Technik ein hohes Sicherheitsniveau auf Basis von Chipkarten erreicht. Im Zuge der Umsetzung von BundOnline 2005 werden die betroffenen Bediensteten mit Chipkarten-basierten kryptografischen Schlüsseln und entsprechenden Zertifikaten, ihre Arbeitsplätze mit der erforderlichen Infrastruktur, insbesondere Chipkartenlesegeräten ausgestattet. Die qualifizierte Signatur

wird in entsprechende eGovernment-Anwendungen implementiert; hierbei wird in der Regel ein **Dokument**, d. h. eine Datei signiert (und ggf. als Anlage einer E-Mail verschickt) werden.

Zertifikate und Ausstattung für qualifizierte Signaturen werden am Markt beschafft. Für die Verifikation der signierten Dokumente wird eine Software allgemein bereitgestellt, die ggf. verschiedene Standards unterstützt.

Die Bundesregierung begrüßt, dass Zertifizierungsdiensteanbieter auf der Basis freiwilliger Akkreditierung Signatur-Produkte und -Dienstleistungen anbieten, die hohe Anforderungen an die Signatur und das ihr zu Grunde liegende Zertifikat, insbesondere hinsichtlich

- deren dauerhafter Überprüfbarkeit und
- deren technischer und administrativer Sicherheit

nachgewiesen erfüllen und zugleich die erforderliche Interoperabilität gewährleisten. Es ist anwendungsbezogen zu entscheiden, ob qualifizierte elektronische Signaturen mit Anbieter-Akkreditierung erforderlich sind.

zu 1.2. des Beschlusses:

Die Bundesverwaltung wird E-Mails zum Schutz der Integrität und Authentizität nachprüfbar mit einer Absenderkennung versehen und zum Schutz der Vertraulichkeit auf der Grundlage allgemein bekannter Verfahren verschlüsseln, wenn der Adressat dazu sein Zertifikat mit seinem öffentlichen Schlüssel zur Verfügung stellt.

E-Mail kommt wegen ihrer flächendeckenden Verfügbarkeit besondere Bedeutung für das eGovernment zu. Es gibt Anwendungen ohne besondere Formerfordernis, z. B. informelles oder formfreies Verwaltungshandeln, die per E-Mail abgewickelt werden können. Gleichzeitig ist E-Mail ein Transportmedium für ggf. signierte Dokumente. Hierzu sind Maßnahmen zur IT-Sicherheit (IT-Grundschutz) erforderlich.

Es wird angestrebt, Verfahren zur Sicherheit von E-Mails (Vertraulichkeit, Integrität und Authentizität) bis Ende 2003 flächendeckend in der Bundesverwaltung einzuführen, beginnend auf Basis des Standards MailTrust V.2 (MTT) und mit dem Ziel der Migration nach ISIS-MTT bis Ende 2003. Die kryptografischen Schlüssel können Software- oder Chipkarten-basiert zur Verfügung gestellt werden. Dieses entscheiden die Behörden in Abhängigkeit von Marktentwicklung (Standards, Preise) und Bedarf (Einführung digitaler Dienstaussweise, vermehrte elektronische Durchführung formgebundener Anwendungen) bei Gewährleistung der Wirtschaftlichkeit. Diese Entscheidung kann jeweils bei Ablauf der Zertifikate nach in der Regel drei Jahren einer Überprüfung aufgrund der Erfahrungen und der Entwicklung unterzogen werden. Für die Verifikation der sicher übertragenen E-Mails wird eine Software allgemein bereitgestellt.

Die Bundesverwaltung verschlüsselt E-Mails an ihre Kommunikationspartner per S/MIME, falls deren öffentliche Schlüssel mit X.509v3-Zertifikaten verfügbar sind. Weitere Standards werden bei Bedarf unterstützt.

zu 1.3. des Beschlusses:

Die Bundesverwaltung wird bei Online-Transaktions-Dienstleistungen Mechanismen zur Authentisierung und Verschlüsselung zur sicheren Identifikation und zum Schutz der Vertraulichkeit anbieten.

Viele eGovernment-Anwendungen werden als Online-Transaktions-Dienstleistungen in der Regel Web-basiert zwischen einem Behörden-Server und den Clients der Kommunikationspartner angeboten werden. Hierbei erfolgen Authentisierung und Verschlüsselung anwendungsbezogen durch die jeweiligen Server.

zu 1.4. des Beschlusses:

Die Bundesverwaltung wird Standardsicherheitsmaßnahmen zur Gewährleistung der Verfügbarkeit ihrer Anwendungen umsetzen.

Neben den spezifischen IT-Grundschutzmaßnahmen zur Kommunikationssicherheit werden, soweit erforderlich, Standardsicherheitsmaßnahmen nach dem IT-Grundschutzhandbuch umgesetzt.

b) Kommunikation zur Verwaltung**zu 2.1. des Beschlusses:**

Die Bundesverwaltung wird elektronische Signaturen und Absenderkennungen ihrer Kommunikationspartner zur Prüfung der Rechtsverbindlichkeit, Integrität und Authentizität akzeptieren, soweit sie eine anwendungsbezogen ausreichende Sicherheit gewährleisten und das übermittelte elektronische Dokument für die jeweilige Behörde zur Bearbeitung geeignet ist.

Den Bundesbehörden wird eine Software zur Verfügung gestellt, die die Verifikation von Signaturen nach unterschiedlichen Standards ermöglicht.

zu 2.2. des Beschlusses:

Die Bundesverwaltung wird ihre Zertifikate mit den öffentlichen Schlüsseln zur Verschlüsselung von E-Mail zur Verfügung stellen (Schutz der Vertraulichkeit).

Um möglichst viele Verschlüsselungsprogramme zu unterstützen, stellt die Bundesverwaltung die öffentlichen Schlüssel mit X.509v3-Zertifikaten zur Verfügung, damit die Kommunikationspartner per S/MIME verschlüsselte E-Mails an sie senden können.

c) Begleitende Maßnahmen**(1) Sicherheitskultur**

Die Bundesregierung fördert die Entwicklung einer „Sicherheitskultur“. Sowohl Bürgerinnen und Bürger als auch Bedienstete der Verwaltungen sind gefordert, sich an die neuen Begriffe und Verfahren zu gewöhnen, ihren Zweck zu verstehen und die sinnvolle Anwendung zu erlernen.

(2) Interoperabilität

Für die Kommunikation mit elektronischen Signaturen und Verschlüsselung zwischen heterogen ausgestatteten Kommunikationspartnern sind Standards erforderlich, die

- die Interoperabilität zwischen verschiedenen Software- und Hardwareprodukten (horizontale Interoperabilität) und
- die Interoperabilität zwischen fortgeschrittenen und qualifizierten Signaturen (vertikale Interoperabilität)

gewährleisten.

Für den wirtschaftlichen Einsatz bei den Behörden des Bundes soll die Ausstattung der Arbeitsplätze mit einer interoperablen technischen Lösung erfolgen, die alle Arten von elektronischer Kommunikation zwischen der Bundesverwaltung und ihren Kommunikationspartnern ermöglicht.

Für sichere interoperable Abläufe zwischen den Instanzen einer Zertifizierungsinfrastruktur steht die Industrial Signature Interoperability Specification (ISIS) zur Verfügung. Für den gesicherten interoperablen E-Mail-Austausch steht der Standard MailTrust V2 (MTT) einschließlich entsprechender (Software-) Produkte (horizontale Interoperabilität) am Markt zur Verfügung.

Die Bundesregierung begrüßt die Aktivitäten der Wirtschaft (Arbeitsgruppe „Trustcenter“ der Trustcenter-Betreiber T7 e. V. und Arbeitsgruppe „MailTrust“ der Hersteller- und Anwendervereinigung TeleTrust Deutschland e. V.) zur Einführung des einheitlichen Interoperabilitätsstandards „ISIS-MTT“. Die ersten Spezifikationen liegen vor. Die Bundesregierung unterstützt diese Arbeiten, damit ISIS-MTT rasch bei Anwendungen eingesetzt werden kann. ISIS-MTT basiert auf den globalen Standards S/MIME und X.509V3 und ermöglicht, ggf. nach Ergänzung von Festlegungen für Attributzertifikate und Dokumentensignatur, die Etablierung einer Vielfalt an Produkten für verschiedene Plattformen und Anwendungen.

Die Bundesverwaltung erwartet, dass der Interoperabilitätsstandard ISIS-MTT sich rasch am Markt etabliert und für die jeweiligen Anwendungen geeignete Produkte auf Basis von ISIS-MTT zur Verfügung stehen. Sie wird ISIS-MTT dann umfassend einsetzen und bei Ausschreibungen zu Grunde legen.

Die Bundesregierung unterstützt die von der europäischen Kommission geforderte Harmonisierung und Interoperabilität elektronischer Signaturen innerhalb des EG-Binnenmarktes und die Schaffung marktkonformer und gleichzeitig sicherer und vertrauenswürdiger Systeme auf globaler Ebene.

(3) Zertifizierungsinfrastrukturen (PKI)

Nach dem Signaturgesetz ist die Regulierungsbehörde für Telekommunikation und Post (RegTP) für die Zertifizierung der öffentlichen Schlüssel von akkreditierten Zertifizierungsdiensteanbietern zuständig. Sie hat darüber hinaus die Aufsicht über alle Anbieter von Zertifikaten für qualifizierte elektronische Signaturen.

Für die Kommunikationssicherheit auf Basis von IT-Grundschutzmaßnahmen (insbesondere E-Mail-Sicherheit) in der öffentlichen Verwaltung in Deutschland wurde die Verwaltungs-PKI eingerichtet, die die Einhaltung von Sicherheits- und Interoperabilitätsstandards, auch für so genannte technische Signaturen (Server-Server-Kommunikation) gewährleistet. An der Verwaltungs-PKI beteiligen sich nach einem Beschluss des Kooperationsausschusses ADV Bund / Länder / kommunaler Bereich auch Länder und Gemeinden. Damit wird eine Grundlage für den IT-Grundschutz bei der sicheren Kommunikation der öffentlichen Verwaltung in Deutschland geschaffen.

Die Bundesregierung fördert den Aufbau von Zertifizierungsinfrastrukturen (Public Key Infrastructure - PKI) für Signatur, Authentisierung und Verschlüsselung mit dem Ziel, Zertifikate für die Teilnehmer verfügbar zu machen und leicht nachprüfbar zu halten.

Innerhalb dieser sich ergänzenden Zertifizierungsinfrastrukturen, die aufgrund der unterschiedlichen Aufgaben bis auf Weiteres zunächst erforderlich sind, können alle privaten Zertifizierungsstellen Zertifikate anbieten, die die jeweiligen Anforderungen erfüllen. Die Behörden können damit Zertifikate für qualifizierte Signaturen und für die Kommunikationssicherheit von **einer** Zertifizierungsstelle am Markt beziehen.

Durch das Konzept der Bridge Certification Authority (Bridge-CA), einer Initiative von Wirtschaft und Verwaltung zur Verknüpfung verschiedener Zertifizierungsinfrastrukturen, wird Kommunikation über Verwaltungs- und Unternehmensgrenzen hinweg erleichtert. Das ist, neben dem Signaturgesetz und der Verfügbarkeit interoperabler Produkte, ein wesentlicher Schritt zu einer nationalen und internationalen interoperablen Zertifizierungs- und Sicherheitsinfrastruktur und damit für den Erfolg des elektronischen Rechts- und Geschäftsverkehrs.

Für den verwaltungsinternen E-Mail-Verkehr wird der Verzeichnisdienst im Informationsverbund Berlin-Bonn (IVBB) zu einem Verzeichnis sämtlicher Bundesbediensteter ausgebaut. Er wird mit den Verzeichnissen der Länder und des kommunalen Bereichs verbunden.

(4) Organisation

Die Anwendungen zur Signatur, Authentisierung und Verschlüsselung werden in die organisatorischen Abläufe jeder Behörde eingebettet, insbesondere

- die Rolle der Registrierungsstelle, die die Identität der Bediensteten feststellt und gegenüber der Zertifizierungsstelle bestätigt sowie die Bediensteten hinsichtlich der Sicherheitsfragen betreut,
- die IT-Administration, die die Programme und ggf. Chipkartenlesegeräte installiert, testet und betreibt und die Bediensteten hinsichtlich der IT betreut, und
- die erforderlichen Schulungen.

Zertifizierungsdienstleistungen (TrustCenter-Dienstleistungen) für qualifizierte elektronische Signaturen und für die Kommunikationssicherheit werden in der Regel am Markt beschafft. Die Zertifizierungsdiensteanbieter gewährleisten die Einhaltung der Sicherheits- und Interoperabilitätsanforderungen sowie die Bereitstellung von Zertifikaten in

Verzeichnissen zur Kommunikation mit Teilnehmerinnen und Teilnehmern innerhalb der eigenen und anderer Zertifizierungsinfrastrukturen.

(5) Bereitstellung von Basiskomponenten

Das Bundesministerium des Innern (BMI) prüft den Bedarf für eine „virtuelle Poststelle“. Dabei soll die rechtliche und tatsächliche Möglichkeit der Übernahme von Aufgaben im elektronischen Rechts- und Geschäftsverkehr festgestellt, insbesondere den mit den Aufgaben der Ver- und Entschlüsselung, Signaturprüfung und –bildung, Virenprüfung, Archivierung und Zeitstempelung verbundene Fragestellungen nachgegangen werden. Mit einer „virtuellen Poststelle“ könnten diese Aufgaben ggf. zentral für eine Behörde unterstützt und gleichzeitig die von den Kommunikationspartnern verwendeten Standards unterstützt werden. Hierzu wird das BMI auf Erfahrungen beim MEDIA@Komm-Ansatz „Online Services Computer Interface (OSCI)“ für Online-Transaktionen auf Basis elektronischer Signaturen zurückgreifen. Bei Bedarf wird das BMI den Bundesbehörden die Software für die virtuelle Poststelle bereitstellen.

Das BMI wird den Kommunikationspartnern der Bundesverwaltung eine Verifikationssoftware zur Überprüfung von Rechtsverbindlichkeit, Integrität und Authentizität der Kommunikation der Bundesverwaltung zur Verfügung stellen.

Das BMI wird Informationen zu Einzelthemen im Hinblick auf die Einführung von Signatur, Authentisierung und Verschlüsselung bei den Behörden bereitstellen.

4.

Kosten

Durch die Einführung von Signatur und Verschlüsselung entstehen Einführungskosten (Hard- und Software) und laufende Kosten (Pflege, Zertifizierungsstellendienstleistungen). Diese einmaligen und jährlichen Kosten sowie die Kosten für die Entwicklung und Pflege von Basiskomponenten (Verifikationssoftware) werden zentral und dezentral entsprechend dem Beschluss des Bundeskabinetts zum Umsetzungsplan für die eGovernment-Initiative BundOnline 2005 vom 14. November 2001 bereit gestellt.

Folgende Kosten werden neben den für Pilotprojekte bereits eingeplanten Mitteln zusätzlich in den einzelnen Behörden schätzungsweise anfallen:

- *Vorrangige Ausstattung in einer ersten Stufe von nach erster Schätzung ca. 20.000 Arbeitsplätzen der unmittelbaren Bundesverwaltung, an denen qualifizierte elektronische Signaturen für eGovernment-Anwendungen benötigt werden: einmalig ca. 60 €, jährlich ca. 20 – 40 € pro Arbeitsplatz,*
- *Ausstattung von ca. 200.000 Arbeitsplätzen mit Produkten zur E-Mail-Sicherheit à einmalig ca. 10 € und weiterhin jährlich ca. 10 € für Arbeitsplatzprogramme („Plug-Ins“) und Zertifizierungsstellen-Dienstleistungen,*

- *Schaffung der organisatorischen Rahmenbedingungen bei den Behörden, insbesondere Einrichtung von Registrierungsstellen und Einführungsaufwände à ca. 30.000 € pro Behörde,*
- *Ausstattung weiterer Personalcomputer im Rahmen turnusmäßiger Neubeschaffung mit Chipkartenlesegeräten: je Computer ca. 15 €,*
- *Personalkosten von ca. 1 gD je 1.000 Bediensteten zzgl. Personalaufwände während der Einführungsphase,*
- *Schulungskosten.*

Die Gesamtkosten für die Einführung von Signatur-, Authentisierungs- und Verschlüsselungsverfahren für den elektronischen Rechts- und Geschäftsverkehr sind im Gesamtwert der Finanzbedarfsschätzung gemäß Umsetzungsplan BundOnline 2005 enthalten.

Den Investitionen stehen der Sicherheitsgewinn sowie Wirtschaftsförderung gegenüber. Es ist ein bedeutendes Rationalisierungs- und Einsparpotenzial durch effizientere Gestaltung von Abläufen zum Beispiel aufgrund des Einsatzes von qualifizierten elektronischen Signaturen oder durch verstärkte Nutzung von E-Mail und effizientere Bearbeitung von Vorgängen mit der Einführung von eGovernment-Anwendungen im Rahmen des Regierungsprogramms BundOnline 2005 zu erwarten.

Die heutigen Kosten, zum Beispiel für Chipkartenlesegeräte und Zertifizierungsstellendienstleistungen können aufgrund der mit der breiten Einführung entsprechender Systeme zu erwartenden hohen Stückzahlen stark sinken.

5.

Zusammenarbeit, Öffentlichkeitsarbeit

Aus Sicht der Bundesregierung ist die erfolgreiche Einführung der elektronischen Signatur nur mit einer umfassenden Einbeziehung der Wirtschaft möglich. Die Bundesregierung bietet daher den Herstellern und Verbänden eine umfassende Zusammenarbeit an.

Eine ressortübergreifende Arbeitsgruppe unter Federführung von BMI und BMWi wird das weitere Vorgehen der Bundesregierung koordinieren und dabei eng mit Ländern und Kommunen sowie anderen Anwendern, Herstellern und Verbänden zusammenarbeiten.

Die Bundesregierung wird die Einführung elektronischer Signaturen mit einer breiten Öffentlichkeitsarbeit begleiten.