RUHR-UNIVERSITÄT BOCHUM

Institut für Sicherheit im E-Business (ISEB)

Nr. 6

Wann wird sich die elektronische Einkommensteuererklärung durchsetzen?

- Zum Sicherheits- und Entwicklungsstand von ELSTER

Frank Hechtner / Jochen Hundsdoerfer / Olaf Siegmund

Bochum, November 2004

RUHR-UNIVERSITÄT BOCHUM

Institut für Sicherheit im E-Business (ISEB)

www.iseb.ruhr-uni-bochum.de

Mit der zunehmenden Verbreitung der Informations- und Kommunikationstechniken haben auch die Abhängigkeiten und Risiken deutlich zugenommen. Die weltweite Vernetzung zwischen und innerhalb der Unternehmungen birgt vielfältige und neuartige Risiken. Das Thema Sicherheit im E-Business entwickelt sich daher zunehmend von einer unterschätzten Gefahr zu einem Schlüsselfaktor für den Erfolg im E-Business.

Die Fakultät für Wirtschaftswissenschaft an der Ruhr-Universität Bochum begegnet dieser Herausforderung durch die Tätigkeiten im **Institut für Sicherheit im E-Business (ISEB)** als Teil des Horst Görtz Instituts und als Partner des eurobits.

Das Institut verfolgt das Ziel, die betriebs- und volkswirtschaftlichen Implikationen von Sicherheit im E-Business zu erforschen und dadurch einen Beitrag zur Entwicklung und zum Einsatz von sicheren und erfolgreichen E-Business-Lösungen zu leisten.

Im Vordergrund stehen dabei ökonomische Analysen und organisatorische Gestaltungsaufgaben. Es werden einerseits ausgewählte Problemstellungen der jeweiligen Disziplinen analysiert, wie z. B. die Sicherheit in E-Logistik-Anwendungen oder die volkswirtschaftlichen Kosten und Risiken unsicherer Datennetze, andererseits aber auch interdisziplinäre Fragestellungen behandelt. Neben Aktivitäten in Forschung und Lehre wird auch ein intensiver Austausch mit Unternehmungen und öffentlichen Institutionen angestrebt. Am Institut für Sicherheit im E-Business beteiligen sich zur Zeit sechs betriebswirtschaftliche und ein volkswirtschaftlicher Lehrstuhl:

- Betriebswirtschaftliche Steuerlehre (Prof. Dr. Jochen Hundsdoerfer)
- Finanzierung und Kreditwirtschaft (Prof. Dr. Stephan Paul)
- Marketing (Prof. Dr. Peter Hammann)
- Produktionswirtschaft (Prof. Dr. Marion Steven)
- Unternehmensforschung und Rechnungswesen (Prof. Dr. Brigitte Werners)
- Wirtschaftspolitik (N. N.)
- Wirtschaftsinformatik (Prof. Dr. Roland Gabriel)

Institut für Sicherheit im E-Business
Ruhr-Universität Bochum
Fakultät für Wirtschaftswissenschaft
Gebäude GC 3/29
D-44780 Bochum

Prof. Dr. Roland Gabriel

Ansprechpartner:
Dipl.-Ök. Klaus Rüdiger
Lehrstuhl für Wirtschaftsinformatik
Tel.: +49 (0)234 – 32 25325
Fax: +49 (0)234 – 32 14350
Klaus.Ruediger@iseb.ruhr-uni-bochum.de
www.iseb.ruhr-uni-bochum.de

Vorwort

Die Ruhr-Universität Bochum entwickelte im Jahre 1999 ein Konzept zur Bildung eines europäischen Kompetenzzentrums für IT-Sicherheit. Dieses Europäische Kompetenzzentrum für Sicherheit in der Informationstechnologie, eurobits genannt, ist innerhalb weniger Jahre zu einem europaweit herausragenden Standort für IT-Sicherheit geworden. Gründe dafür sind seine Interdisziplinarität und die enge Verzahnung von Forschung und Anwendung. Durch die Anbindung an die Ruhr-Universität Bochum fließen neueste wissenschaftliche Erkenntnisse direkt in die Praxis ein. Die Partner des eurobits sind derzeit das Horst Görtz Institut für Sicherheit in der Informationstechnik (HGI), das Institut für Sicherheit im E-Business (ISEB), die Gesellschaft für IT-Sicherheit (GITS AG), die escrypt GmbH Embedded Security (escrypt GmbH) und die Projektgesellschaft für angewandte IT-Sicherheit mbh (GITS Projekt GmbH).

Das im Jahr 2003 gegründete Institut für Sicherheit im E-Business (ISEB) verfolgt das Ziel, die betriebs- und volkswirtschaftlichen Implikationen von Sicherheit im E-Business zu erforschen. Das Institut, bestehend aus sieben Lehrstühlen der Fakultät für Wirtschaftswissenschaft an der Ruhr-Universität Bochum, leistet einen Beitrag zur Entwicklung und zum Einsatz von sicheren und erfolgreichen E-Business-Lösungen. Neben den vielfältigen Forschungsaktivitäten und Kooperationen mit der Praxis sollen auch die IT-sicherheitsrelevanten Inhalte in der universitären Lehre angeboten werden.

Mit dem vorliegenden Arbeitsbericht setzt das Institut für Sicherheit im E-Business (ISEB) seine Schriftenreihe fort. In der Reihe wird in unregelmäßigen Abständen über Aktivitäten des Instituts berichtet, wozu neben der Publikation von Forschungsergebnissen auch Berichte über mit Unternehmen bzw. öffentlichen Institutionen durchgeführte Workshops oder Arbeitskreise und Veranstaltungen mit Studierenden gehören.

Prof. Dr. Jochen Hundsdoerfer ist Inhaber des Lehrstuhls für Betriebswirtschaftslehre, insb. Betriebswirtschaftliche Steuerlehre an der Ruhr-Universität Bochum. Herr Dipl.-Ökonom Frank Hechtner und Herr Dipl.-Ökonom

Olaf Siegmund sind wissenschaftliche Mitarbeiter am Lehrstuhl für Betriebswirtschaftslehre, insb. Betriebswirtschaftliche Steuerlehre von Prof. Dr. Jochen Hundsdoerfer sowie am Institut für Sicherheit im E-Business (ISEB). Der Forschungsschwerpunkt der Autoren liegt insbesondere im Bereich der elektronischen Steuererklärung und damit verbundenen Sicherheitsaspekten. Die Autoren danken Herrn Johann Josef Königs (Rechenzentrum der Finanzverwaltung NRW), Herrn Roland Krebs (OFD München, Projektleiter ELSTER) und Herrn Dr. Heinz-Peter Röhrs (Rechenzentrum der Finanzverwaltung NRW) für hilfreiche Informationen und kritische Anmerkungen.

Der vorliegende Bericht setzt den Arbeitsbericht Nr. 2 „Elster - Vorteile, Nachteile und Sicherheitsrisiken der elektronischen Einkommensteuererklärung“ fort. Untersucht wird, wann sich die elektronische Einkommensteuererklärung durchsetzen wird. Dazu werden in den Kapiteln eins bis drei der derzeitige Stand sowie die einzelnen Bestandteile des Projekts ELSTER dargestellt. Ferner wird darauf eingegangen, inwieweit ELSTER bereits jetzt von den Steuerpflichtigen genutzt wird. Kapitel vier beschreibt die bestehenden Medienbrüche der papiergebundenen Steuererklärung und geht auf Maßnahmen zu ihrer Vermeidung ein. Kapitel fünf beschreibt die verwendeten Sicherheitsmaßnahmen des Projekts ELSTER und analysiert mögliche auftretende Sicherheitsrisiken der elektronischen Einkommensteuererklärung. In Kapitel sechs wird geschildert, in welchem Umfang derzeit ELSTER bei Steuerberatern eingesetzt wird. Im letzten Kapitel werden abschließend Möglichkeiten erörtert, die nach Ansicht der Autoren dazu geeignet sind, das Projekt ELSTER im Bezug auf die Nutzung bei den Steuerpflichtigen weiter zu fördern.

Der Arbeitsbericht wurde in verkürzter Form in der Zeitschrift „Die Wirtschaftsprüfung“ in der Ausgabe 24/2004 veröffentlicht.

Bochum, November 2004

R. Gabriel
K. Rüdiger

Prof. Dr. Jochen Hundsdoerfer
E-Mail: steuerlehre@rub.de

Ruhr Universität Bochum
Lehrstuhl für
Betriebswirtschaftslehre, insb.
Betriebswirtschaftliche Steuerlehre
44801 Bochum

Dipl.-Ök. Frank Hechtner
E-Mail: frank.hechtner@rub.de

Ruhr Universität Bochum
Lehrstuhl für
Betriebswirtschaftslehre, insb.
Betriebswirtschaftliche Steuerlehre
44801 Bochum

Dipl.-Ök. Olaf Siegmund
E-Mail: olaf.siegmund@rub.de

Ruhr Universität Bochum
Lehrstuhl für
Betriebswirtschaftslehre, insb.
Betriebswirtschaftliche Steuerlehre
44801 Bochum

Inhaltsverzeichnis

Abbildungsverzeichnis

Abkürzungsverzeichnis

AO	Abgabenordnung
BMF	Bundesministerium der Finanzen
DDoS	Distributed Denial of Service
DES	Data Encryption Standard
ELSTER	Elektronische Steuer-Erklärung
EOM	ElsterOnlineManager
EStG	Einkommensteuergesetz
eTIN	electronical Taxpayer Identification Number
Fn.	Fußnote
https	Hypertext Transfer Protocol Secure
i.d.F.	in diesem Fall
MAC	Message Authentication Code
o.V.	ohne Verfasser
OFD	Oberfinanzdirektion
PIN	Persönliche Identifikationsnummer
RSA	Rivest, Shamir, Adleman
Rz.	Randziffer
RZF	Rechenzentrum der Finanzverwaltung
SSL	Secure Socket Layer
StDÜV	Steuerdaten-Übermittlungsverordnung
TAN	Transaktionsnummer
URL	Uniform Resource Locator
USB	Universal Serial Bus

1 Problemstellung

In den ersten drei Quartalen des Jahres 2004 sind bereits mehr als 1.5 Mio. Einkommensteuererklärungen online bei den Finanzämtern eingegangen[1]. Damit liegt der Anteil der auf elektronischem Weg eingereichten Steuererklärungen in Deutschland nunmehr bei ca. 5,6 %[2], was freilich im Vergleich zu Ländern wie den USA oder Großbritannien immer noch ein sehr geringer Wert ist[3].

In diesem Beitrag sollen die Konzeption des Projektes ELSTER (**El**ektronische **St**euer-**Er**klärung) und aktuelle Entwicklungen und Verbesserungen erläutert werden. Besonderes Augenmerk wird dabei auf die Sicherheitsrisiken für die Beteiligten gelegt.

2 ELSTER: Vorgehensweise und Akzeptanz

Im Rahmen der E-Goverment-Aktivitäten des Bundes und der Länder wurde im Jahr 2000 erstmals die Möglichkeit geboten, Steuerklärungen online beim zuständigen Finanzamt einzureichen. Neben der Einkommensteuererklärung, auf die sich die folgenden Ausführungen im Wesentlichen beziehen, können die Umsatzsteuer- und Gewerbesteuererklärung, die Umsatzsteuer-Voranmeldung und die Lohnsteueranmeldung online vorgenommen werden. Das Projekt ELSTER steht durch seinen hohen Bekanntheitsgrad repräsentativ für das Angebot von Behörden im Internet. Es soll dem Steuerpflichtigen eine einfache Möglichkeit zur Kommunikation mit der Steuerverwaltung eröffnen. Gleichzeitig sollen so die Kosten der Finanzämter gesenkt werden: Erstens wird die manuelle Eingabe der Erklärungsdaten in die Rechnersysteme der Finanzverwaltung von der Finanzverwaltung auf die Steuerpflichtigen verlagert („Outsourcing")[4]. Zweitens soll die Fehlerquote bei online eingereichten Erklärungen verringert werden, da der Nutzer schon vom Programm auf fehlende oder inkonsistente Angaben hingewiesen wird; dadurch könnten Folgekosten entfallen. Drittens sollen die

---

[1] Bei den im Text angegebenen Daten handelt es sich um Angaben der Finanzverwaltung.

[2] Die Berechnung beruht auf einer Zahl von ca. 27 Mio. Erklärungen, die insgesamt pro Jahr eingereicht werden.

[3] So werden etwa in den USA fast 40% aller Einkommensteuererklärungen online eingereicht. Vgl. www.irs.gov.

[4] Vgl. Röhrs (2002), S. 454.

Kosten für Versand und Erstellung von Steuerformularen reduziert und die Archivierung vereinfacht werden.

In den Jahren 1999 bis einschließlich 3. Quartal 2004 (Veranlagungszeiträume 1998-2003) wurden den Finanzämtern insgesamt 3.679.411 Einkommensteuererklärungen zugesandt. Nach anfänglich sehr zögerlicher Bereitschaft der Steuerpflichtigen, die Möglichkeit der elektronischen Übermittlung der Einkommensteuererklärung zu nutzen, zeigen sich bei der Akzeptanz mittlerweile deutliche Fortschritte. Abbildung 1 zeigt den Anstieg der online eingereichten Erklärungen, wobei für das Jahr 2004 auch die noch erwarteten Erklärungen abgebildet sind. Bei derzeitiger Datenlage kann mit insgesamt 1,8 Mio. Online-Erklärungen allein im Jahr 2004 gerechnet werden. Dies entspricht einem Anteil von ca. 6,7 % der etwa 27 Mio. abgegebenen Erklärungen pro Jahr. Dabei beteiligen sich Steuerberater und Lohnsteuerhilfevereine, über die ein erheblicher Anteil der Erklärungen eingereicht wird, derzeit noch kaum an ELSTER[5].

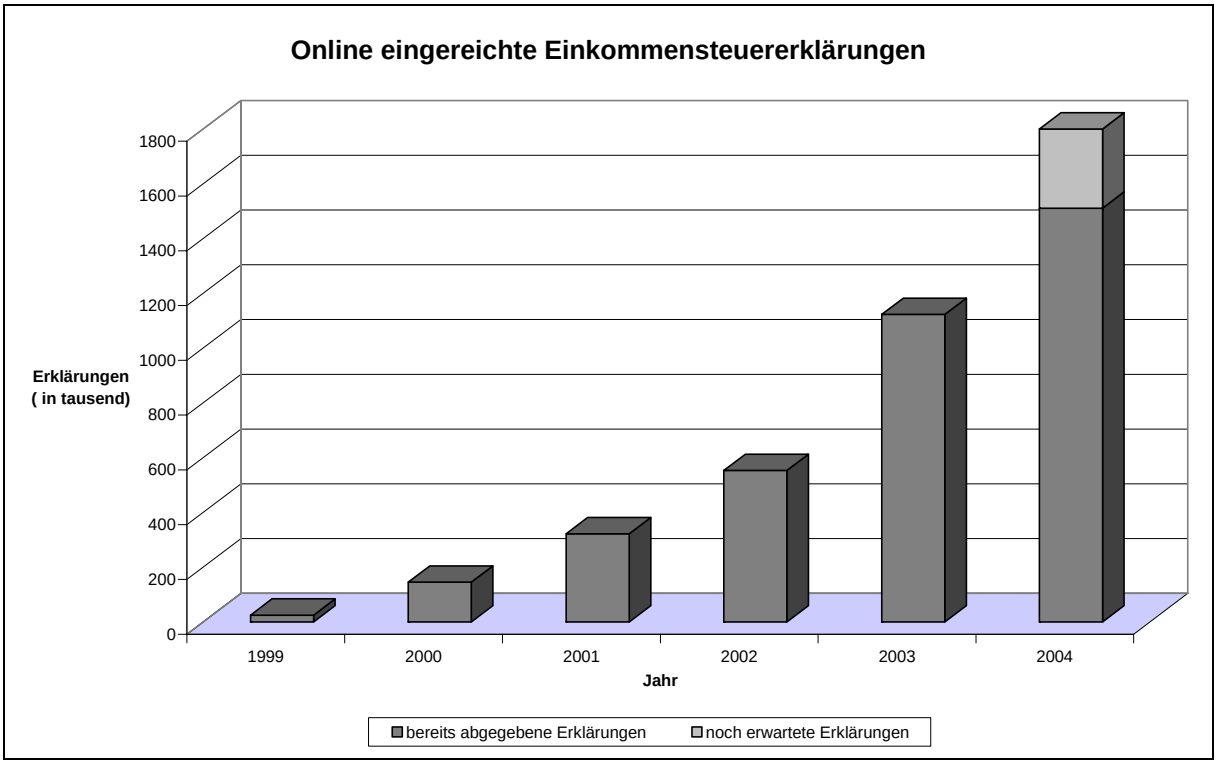

Abbildung 1: Anzahl eingereichter Online-Erklärungen;
Quelle: Angaben der Finanzverwaltung

[5] Nach Angaben des RZF NRW ist die Quote der Nutzung von Elster durch Steuerpflichtige, die fachliche Beratung in Anspruch genommen haben, nur halb so groß wie bei allen Steuerpflichtigen zusammen (vgl. Teil 6). Vgl. auch Jahr-Weidauer (2004).

Die Zielgruppe für eine elektronische Einkommensteuererklärung hat einen großen Umfang. Nach einer Internet-Trendstudie würden knapp neun von zehn Bürgern (88 %) ihre Amtsgeschäfte online erledigen[6]. Laut einer Befragung unter Steuerpflichtigen der Zeitschrift Capital nehmen mehr als 70 % der Bürger Hilfen bei der Erstellung ihrer Erklärung in Anspruch[7]. Würden nur diejenigen, die ihre Erklärung mit Hilfe von Software (incl. ELSTER) erstellen, die Möglichkeiten der elektronischen Einreichung nutzen, so könnten bereits 22 % der Erklärungen online eingehen (vgl. Abbildung 2). Bei einer vollständigen Einbeziehung von Steuerberatern und Lohnsteuerhilfevereinen würde der Anteil auf ca. 65 % steigen.

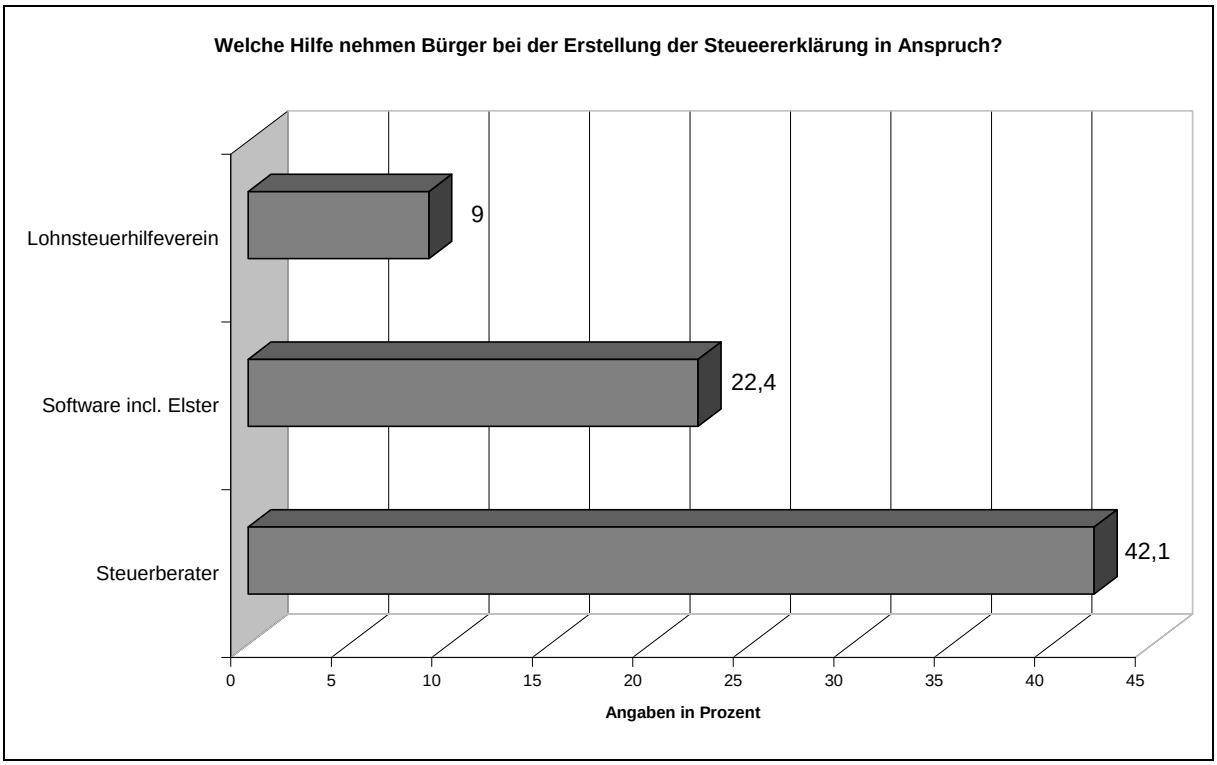

Abbildung 2: Hilfen bei der Erstellung der Einkommensteuererklärung; Quelle: www.capital.de/finanzamt - Europressedienst

Die Quote von 5,6 % (in den ersten drei Quartalen 2004 bzw. voraussichtlich 6,7 % im Gesamtjahr) Online-Erklärungen ist etwa im Vergleich zu den USA sehr niedrig; dort werden knapp 40 % aller Erklärungen online eingereicht[8]. Die wichtigsten Gründe hierfür vermuten wir darin, dass in den USA auch

[6] Vgl. Mummert Consulting (2003).

[7] Vgl. Hoffmann/Votsmeier (2004).

[8] Vgl. www.irs.gov.

professionelle Berater die Erklärung ihrer Mandanten elektronisch einreichen und dass die Möglichkeiten der papierlosen Einreichung größer sind. So wird in den USA neben der elektronischen Abgabe der Erklärung über das Internet auch die Eingabe der Erklärungsdaten in Webformulare unterstützt und sogar die Abgabe über das Telefon (vgl. Abbildung 3).

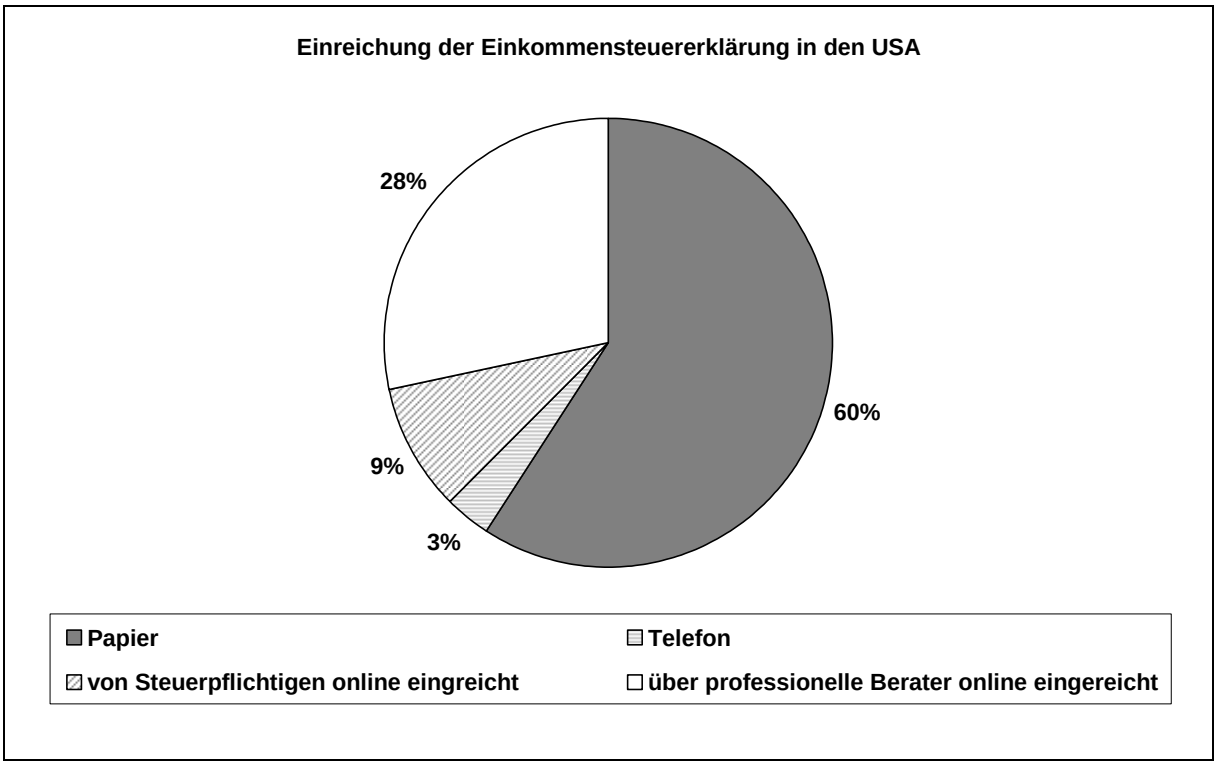

Abbildung 3: Abgabe der Einkommensteuererklärung in den USA;
Quelle: www.irs.gov (eigene Berechnungen)

Bei der Eingabe über Webformulare benötigt der Bürger nicht einmal ein Programm zur Erstellung einer Erklärung; die Eingabe erfolgt mit dem Webbrowser direkt in entsprechende Webseiten der Finanzverwaltung. Bei der Abgabe der Erklärung über das Telefon müssen Erklärungsdaten mittels Telefontastenangabe durchgegeben werden. Die Steuerpflichtigen identifizieren sich mittels einer durch die Finanzverwaltung mitgeteilten Nummer.

3 Bestandteile von ELSTER

Das Projekt ELSTER umfasst mehrere Programmteile, die die elektronische Kommunikation mit dem Finanzamt ermöglichen oder unterstützen. Wichtigster Bestandteil der ELSTER-Programme ist der so genannte ElsterClient. ElsterClient ist ein Baustein sowohl der kostenlosen Software der Finanzverwaltung (ElsterFormular) als auch von kommerziellen Steuerverwaltungsprogrammen. Er fungiert als Schnittstelle zwischen Anwender und Finanzverwaltung, indem er die Kommunikation zwischen dem Computer des Steuerpflichtigen und den Rechnern der Finanzverwaltung ermöglicht. Neben der Verschlüsselung für den Versand beinhaltet ElsterClient auch eine Plausibilitätsprüfung der zu sendenden Daten sowie eine Updatefunktion, über die das Programm selbständig auf aktuellem Stand bleibt.

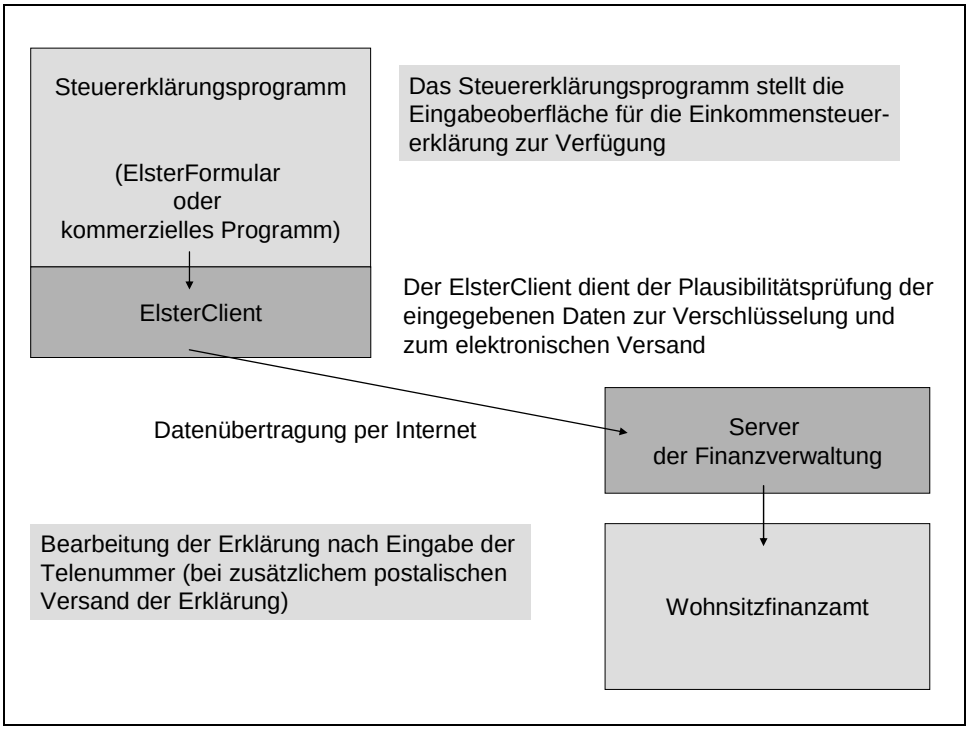

Abbildung 4: Ablauf der Steuererklärung mit dem ELSTER-Programm

Will ein Steuerpflichtiger die Möglichkeit zur digitalen Steuererklärung nutzen, so braucht er derzeit entweder das Programm ElsterFormular oder ein kommerzielles Steuerverwaltungsprogramm, welches den Programmbaustein ElsterClient beinhaltet. ElsterFormular kann auf der Webseite der Finanzverwaltung unter

www.elster.de herunter geladen werden oder ist auf der offiziellen ELSTER-CD der Verwaltung enthalten, die kostenlos u.a. bei den Finanzämtern erhältlich ist[9]. Das Programm der Finanzverwaltung und andere am Markt verfügbare Steuerprogramme beinhalten eine Eingabeoberfläche für den Steuerpflichtigen. Dabei werden die offiziellen Formulare der Finanzverwaltung auf dem Monitor zum Ausfüllen abgebildet. ElsterFormular bietet die offiziellen von den Papiervordrucken bekannten Erläuterungen zu den einzelnen Feldern, kommerzielle und auch frei verfügbare Steuerprogramme geben darüber hinaus ausführlichere Hilfen oder unterstützen durch gezielte Fragestellungen den Erklärenden bei der Erstellung der Einkommensteuererklärung. Die fertige Einkommensteuererklärung kann online versandt oder bei kommerziellen Produkten alternativ ausgedruckt werden. Bei Abgabe der Online-Erklärung ist in der Regel noch zusätzlich der Ausdruck einer komprimierten Einkommensteuererklärung erforderlich, die für die spätere Zuordnung eine vom Programm generierte Telenummer enthält. Diese komprimierte Erklärung ist zu unterschreiben, da nur unterschriebene oder digital signierte Erklärungen (bei denen der Ausdruck entfällt, siehe Teil 4.2) die Voraussetzungen des § 25 EStG erfüllen. Zusammen mit derzeit noch unentbehrlichen Belegen (u.a. Lohnsteuerkarte, Spendenquittungen, Bescheinigungen der Kreditinstitute zu vermögenswirksamen Leistungen oder zur Kapitalertragsteuer, Bilanzen, Gewinn- und Verlustrechnungen) wird die unterschriebene Kurzfassung der Steuererklärung per Post an das zuständige Finanzamt geschickt. Dort kann der Sachbearbeiter die online übermittelte Erklärung durch Eingabe der Telenummer abrufen und die Erklärung weiter bearbeiten[10]. Nur die online eingereichte Erklärung, die zu der individuellen Telenummer des zugehörigen Ausdrucks passt, wird bearbeitet. Irrtümlich online übersandte Erklärungen gelangen somit nicht in die Bearbeitung. Ein Vorteil für den Erklärenden ist, dass eine mögliche Steuererstattung schneller erfolgen kann, da digital eingereichte Einkommensteuererklärungen bevorzugt bearbeitet werden sollen. Der endgültige Steuerbescheid geht dem Erklärenden weiterhin per Post zu.

---

[9] Für den Veranlagungszeitraum 2004 wird versuchsweise für sechs Finanzämter in NRW die ElsterFormular-CD dem Bürger mit den Erklärungsvordrucken zugesandt. Aber auch die Steuerpflichtigen, die bereits in der Vergangenheit die elektronische Erklärung nutzten, erhalten die CD zugeschickt.

[10] Vgl. o.V. (2002).

Zusätzlich besteht die Möglichkeit der elektronischen Bescheiddatenabholung. ElsterFormular kann dann die Abweichungen zwischen Erklärung und Bescheid darstellen. Einige kommerzielle Programme unterstützen die Erstellung eines Einspruchs gegen den Steuerbescheid, der dann allerdings auf herkömmlichem Wege erfolgen muss.

Unterstützt werden von ElsterFormular derzeit die Betriebssysteme Windows 98/ME, Windows NT 4.0, Windows 2000 und Windows XP sowie Windows 95 (ohne Support). Nur für ElsterClient ist auch eine Ausdehnung auf andere Betriebssysteme vorgesehen, so dass unabhängige Softwareentwickler diesen in ihre Programme einbinden können. Ob auch das Erklärungsprogramm ElsterFormular für andere Plattformen neben dem Betriebssystem Windows umgesetzt wird, ist derzeit offen. Insbesondere zur Unterstützung der Open-Source-Bewegung könnte hier eine Version beispielsweise für Linux aus wirtschaftspolitischen Gesichtpunkten sinnvoll sein[11].

In Nordrhein-Westfalen und Bremen läuft derzeit ein Barcode-Pilotprojekt. Damit kann der Steuerpflichtige auf den digitalen Versand der mit ElsterFormular erstellten Erklärung verzichten und stattdessen die Erklärungsdaten in einer Kurzform ausdrucken. Daneben wird ein Barcode generiert und ausgedruckt. Das Scannen dieser Barcodeanlage beim zuständigen Finanzamt ersetzt die langwierige und fehlerträchtige Eingabe der Erklärungsdaten. Allerdings erfordert auch das Einlesen der Barcodes in den Finanzämtern Zeit und eine entsprechende Ausstattung. Hier gilt es zu prüfen, ob Kosten und Nutzen in einer sinnvollen Relation zueinander stehen, insbesondere wenn berücksichtigt wird, dass für das Massenverfahren der Barcode wohl nur für eine Übergangszeit Bedeutung haben wird. Auch ist das Pilotprojekt auf das Programm ElsterFormular beschränkt. Rückblickend wäre es im Übrigen wohl sinnvoll gewesen, mit diesem Verfahren zu beginnen und die elektronische Übermittlung der Steuererklärung in einem zweiten Schritt einzuführen.

Private Anbieter (z.B. www.steuerfuchs.de) ermöglichen daneben die Eingabe der Erklärungsdaten über das Internet und ihre digitale Übermittlung an die

---

[11] Für Linux existiert bereits eine kommerzielle Version.

Finanzbehörden. Nachdem der Steuerpflichtige die Erklärung online auf den Webseiten dieser Anbieter ausgefüllt hat, wird ihm der Ausdruck der komprimierten Erklärung zugeschickt, die er unterschreibt und zusammen mit seinen Belegen an das Finanzamt sendet. Der Vorteil dieses Angebots ist, dass der Steuerpflichtige eine einfache Beratung durch die Programmsteuerung der Webseite erhält und durch gezielte Fragestellungen unterstützt wird. Diese Angebote sind kostenpflichtig.

4 Medienbrüche und Maßnahmen zu ihrer Vermeidung

4.1 Verzicht auf Belege in Papierform zur Vermeidung von Medienbrüchen

Derzeit enthält das elektronische Einkommensteuererklärungsverfahren noch mehrere Medienbrüche: Die komprimierte Steuererklärung ist zu unterschreiben, damit die Steuererklärung Rechtskraft erhält, und bestimmte Belege (Lohnsteuerkarte, Spendenbescheinigungen etc.) sind in Papierform beizufügen. Für den Steuerpflichtigen und für die Finanzverwaltung wird die elektronische Einkommensteuererklärung erst dann zu wesentlichen Vorteilen führen, wenn *jeder* dieser Medienbrüche überwunden ist. Eine Vermeidung von Medienbrüchen bedeutet, dass der Steuerpflichtige endgültig auf den postalischen Versand von Unterlagen verzichten kann. Auf Seiten der Finanzverwaltung würde die manuelle Verteilung eingehender Erklärungen auf die Bearbeiter entfallen, die Poststellen würden entlastet, und nach Bearbeitung würde die Archivierung einen späteren Zugriff einfacher und kostengünstiger ermöglichen.

Das derzeitige Belegsystem der Lohnsteuerkarte ist mit erheblichem Aufwand sowohl für die beteiligten Verwaltungen als auch für den Erklärenden verbunden. Die Lohnsteuerkarte ist vom Arbeitnehmer bei seiner Gemeinde zu beantragen. Dann muss die Karte dem Arbeitgeber vorgelegt werden, der auf dieser Grundlage die abzuführende Lohnsteuer errechnet. Bestimmte unterjährige Änderungen der steuerlichen Verhältnisse sind von den Einwohnermeldeämtern auf der Lohnsteuerkarte einzutragen. Vom Arbeitgeber wird die Lohnsteuerkarte nach Ablauf des Jahres einschließlich einer Lohnsteuerbescheinigung an den Arbeitnehmer zurückgesandt. Dieser leitet die Lohnsteuerkarte mit seiner Einkommensteuererklärung an sein Finanzamt weiter.

Dieses Belegsystem soll durch die „digitale Lohnsteuerkarte“ (ElsterLohn) ersetzt werden. Dem Arbeitnehmer soll keine Lohnsteuerkarte mehr zugeschickt werden, sondern zusammen mit dem elektronischen Steuerbescheid für das Vorjahr soll ihm eine elektronische Steuerabzugsbescheinigung zugehen, die er wiederum online an seinen Arbeitgeber weiterleiten kann. Der Arbeitgeber soll mit Hilfe der Steuerabzugsbescheinigung die vom Arbeitslohn abzuziehende Lohnsteuer

ermitteln und eine elektronische Lohnsteueranmeldung beim zuständigen Finanzamt vornehmen können. Nach Ablauf des Jahres soll der Arbeitgeber die Lohnsteuerbescheinigung elektronisch an das Finanzamt und (postalisch oder auch elektronisch) an den Arbeitnehmer senden. Dadurch sollen die bisher notwendigen elf Arbeitsgänge[12] auf sechs reduziert werden. Abbildung 5 zeigt die Verfahrensstruktur:

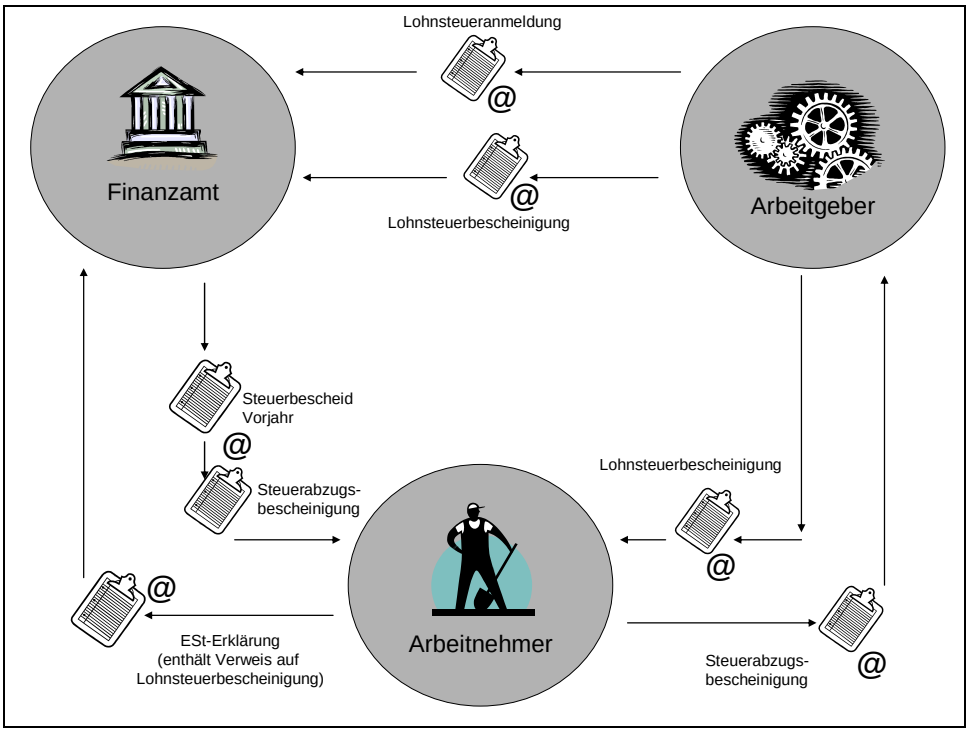

Abbildung 5: Vollelektronisches Lohnsteuer-/Einkommensteuerverfahren; in Anlehnung an BMF (Fn. 12).

Nach der Pilotierung mit etwas mehr als einer Million Arbeitnehmern im Jahre 2004 wird ab dem 1.1.2005 flächendeckend und gesetzlich verpflichtend die erste Stufe für eine solche „digitale Lohnsteuerkarte" beginnen, die bereits die Übermittlung der Bescheinigungsdaten zwischen Arbeitgeber und Finanzamt erlaubt. Die Identifikation des Arbeitnehmers erfolgt hierbei über einen Bezeichner (eTIN), der aus Namen und Geburtsdatum des Arbeitnehmers generiert wird. Erhebliche Einsparungen für den Arbeitgeber entstehen bereits durch den Wegfall der Lohnsteuerkartenrücksendung an die Arbeitnehmer einschießlich Verbinden von Lohnsteuerbescheinigung und Lohnsteuerkarte bzw. Ausfüllen der Rückseite

[12] Vgl. BMF (2003).

der Lohnsteuerkarte. Der Arbeitnehmer erhält einen Ausdruck seiner Lohnsteuerbescheinigungsdaten einschließlich seiner eTIN. Wird die Steuererklärung auf herkömmlichem Weg abgegeben, muss diese Bescheinigung der Steuererklärung beigefügt werden. Bei elektronisch übermittelten Erklärungen sind dagegen nur noch die Daten in die Anlage N einzugeben und die eTIN in das Formular einzutragen; eine Übersendung der Bescheinigung entfällt.

Für die Eingabe der Erklärung sind in ElsterFormular die offiziellen Formulare der Finanzverwaltung nachgebildet, damit die Umstellung auf die elektronische Erklärung leichter fällt. Dadurch reicht der zur Verfügung stehende Platz häufig nicht aus. Bei der herkömmlichen Erklärung löst der Steuerpflichtige dieses Problem durch Nebenrechnungen, die der eigentlichen Erklärung angefügt werden. Bei der elektronischen Erklärung führt diese Vorgehensweise aber zu neuen Belegen und entsprechenden Medienbrüchen. Hier bietet es sich an, Kommentarfelder variabler Größe anzubieten, die es erlauben, Nebenrechnungen und Erklärungen zu einzelnen Feldern auf elektronischem Wege beizufügen.

Um sämtliche Medienbrüche zu vermeiden, sind auch für andere Belege Verbesserungen des Status quo notwendig. Für Spendenquittungen sind etwa folgende Verfahren denkbar, wobei sich die Grundgedanken auf sämtliche Belege übertragen lassen:

- Der Spendenempfänger meldet Spenden unter Verknüpfung mit bestimmten Ordnungsmerkmalen, die den Spender eindeutig identifizieren, beim Finanzamt. Dieses Ordnungsmerkmal und die Höhe der Spende könnten dem Steuerpflichtigen quittiert werden, so dass er diese Daten in die Steuererklärung eingeben kann.
- Der Beleg könnte in eingescannter Form akzeptiert werden.
- Auf den Beleg könnte im Regelfall verzichtet werden; nur bei einer genaueren Prüfung der Erklärung könnte der Beleg dann verlangt werden.

Alternativ könnte die Einführung der elektronischen Steuererklärung dazu genutzt werden, die steuerliche Abzugsfähigkeit von Spenden zu überdenken. Als Ersatz kommen neben der Streichung dieser Steuerbegünstigung etwa die direkte Subvention des Spenders oder - verwaltungstechnisch wohl einfacher - eine

Subvention des Spendenaufkommens allein beim Empfänger in Betracht. Hier ist allerdings ein genauerer Vergleich der Vor- und Nachteile der einzelnen Varianten notwendig.

4.2 Ersatz der Unterschrift durch digitale Signaturen

4.2.1 Signaturkarte

Notwendige Bedingung für die Rechtskraft einer Steuererklärung ist die Unterschrift des Erklärenden bzw. seines Vertreters, so dass in der Ursprungsversion von ELSTER zusätzlich eine komprimierte Steuererklärung als papiergebundenes Dokument postalisch an das Finanzamt geschickt werden muss. Die Vermeidung von Medienbrüchen erfordert daher unter Anderem den Ersatz der papiergebundenen Unterschrift durch eine digitale Signatur[13].

Rechtlicher Ausgangspunkt für die digitale Signatur bilden § 150 Abs. 6 AO i.V.m. § 87a Abs. 6 AO, die die Möglichkeit einräumen, die Steuererklärung sowohl elektronisch zu speichern als auch per Datenfernübertragung zu verschicken. Nach § 87a Abs. 3, 6 AO sind Daten, die allein elektronisch übermittelt werden, mit einer digitalen Signatur zu versehen.

Technisch läuft der Prozess der signierten elektronischen Datenübermittlung in einem zweistufigen Verfahren ab. Zunächst werden die Daten mit ElsterFormular erfasst. Dann werden die erfassten Daten einer Plausibilitätsprüfung unterzogen, digital signiert (elektronisch unterschrieben) und einschließlich der Signatur an die Finanzverwaltung gesendet. Die digitale Übermittlung der Daten entspricht somit einem rechtsverbindlichen Unterschreiben der Steuererklärung. Die hierfür notwendige Signaturkarte und der darauf gespeicherte Schlüssel werden durch sog. Trust Center generiert.

Dabei übernimmt ein Trust Center mehre Aufgaben: Es nimmt erstens die eindeutige Identifikation des Chipkartenbesitzers vor, indem es der Person ein eindeutiges Schlüsselpaar zuordnet, um anderen Personen oder Institutionen zu belegen, dass der Chipkarteninhaber diejenige Person ist, für die sie sich ausgibt

[13] Für die einzelnen Anforderungen an die digitale Signatur vgl. § 7 StDÜV.

(elektronischer Identitätsnachweis). Zweitens generiert das Trust Center den für die Identifikation nötigen Schlüssel in einer sicheren Umgebung.

Die Kosten für die Karte sowie für die Ausstellung und Generierung des auf der Karte gespeicherten Schlüssels belaufen sich auf ca. 45 Euro. Als Trustcenter fungieren etwa die Deutsche Post oder einige Banken, die ihren Kunden zusätzlich die Möglichkeit des Online-Bankings mittels digitaler Signatur bieten. Für das Einlesen der digitalen Signaturkarte wird weiterhin ein Lesegerät benötigt, das derzeit ca. 50 € kostet.

Die digitale Signatur vermeidet Medienbrüche freilich nur für das Steuerformular selbst; die Belegproblematik wird dadurch nicht gelöst. Damit sind die Anreize für die Steuerpflichtigen, Geld und Zeit in die notwendige Technik und das erforderliche Wissen zu investieren, entsprechend niedriger[14].

4.2.2 Softwarelösung als Alternative zur Signaturkarte

Ab 2005 wird in Nordrhein-Westfalen, Bayern und Sachsen ein Pilotprojekt gestartet, das eine digitale Signierung der elektronischen Einkommensteuererklärung ohne Signaturkarte ermöglichen soll. Der Steuerpflichtige muss sich dazu auf einem Web-Portal der Finanzverwaltung registrieren und erhält daraufhin auf dem Postweg einen individuellen Identifikationsschlüssel. Mit Hilfe dieses Schlüssels kann er - wiederum auf dem Web-Portal der Finanzverwaltung - seine eigentliche, individuell generierte digitale Signatur erhalten.

Im Unterschied zur Signaturkarte kann dieser Schlüssel auf einem Datenträger der eigenen Wahl (z.B. USB-Stick) für die spätere Verwendung gespeichert werden, so dass keine Ergänzungen der Hardware notwendig werden. Mit Hilfe des gespeicherten Schlüssels soll der Steuerpflichtige dann seine künftigen elektronischen Steuererklärungen rechtsverbindlich signieren können. Im Erfolgsfall ist eine bundesweite Einführung für das Jahr 2006 geplant, was wohl die Verbreitungsgeschwindigkeit der Signaturkarte reduzieren wird.

---

[14] Eine Übersicht über die Bundesländer, die eine vollständig digitale Übermittlung unterstützen, ist unter https://www.elster.de/ssl/main-pro-sig-01.htm zu finden. Für die geringe Akzeptanz sei

5 Sicherheitsrisiken der elektronischen Einkommensteuererklärung

5.1 Darstellung der allgemeinen Sicherheitsproblematik

Durch den Systemwechsel zur elektronischen Datenerfassung und -übermittlung entstehen neue Sicherheitsrisiken sowohl auf Seiten der Erklärenden wie auch auf Seiten der Finanzverwaltung[15].

Als Vergleichsmaßstab für Risiken wird hier der Sicherheitsstandard der herkömmlichen papiergebundenen Erklärung herangezogen[16]. Untersucht wird der Fall, dass der Steuerpflichtige seine Daten via ElsterFormular eingibt; auf kommerzielle Programme wird im Folgenden nicht eingegangen.

5.2 Generelle Sicherheitsanforderungen an die Online-Erklärung

Sicherheitsrisiken treten an verschiedenen Stellen des Prozesses der elektronischen Erklärung auf. Für die online eingereichte Erklärung muss sichergestellt sein, dass die folgenden Anforderungen erfüllt werden[17]:

- Vertraulichkeit (Keine unbefugte dritte Person darf Zugriff auf den Inhalt der Daten bekommen),
- Integrität (Unbefugte Änderungen der Daten sollen verhindert werden bzw. eine Manipulation soll sofort entdeckt werden),
- Authentizität (Daten können zweifelsfrei einer Person zugeordnet werden),
- Nichtabstreitbarkeit (Dem Sender darf es nicht möglich sein, die Daten nachträglich zu ändern, wohingegen der Empfänger der Daten den Empfang nicht abstreiten kann).

Diese Anforderungen sollen durch kryptografische Verfahren erfüllt werden. Für die Nutzung des ELSTER-Angebotes ist zudem die Verfügbarkeit der von der

---

exemplarisch auf Berlin hingewiesen, wo nur vier Personen auf die komprimierte Steuererklärung verzichtet und ihre Erklärung digital signiert haben. Vgl. Senatsverwaltung für Finanzen (2004).

[15] Exemplarisch sei hier nur auf die in der vergangenen Zeit aufgetauchten Bedrohungen hingewiesen, vgl. o.V. (2004a). Umfassender werden die denkbaren Sicherheitsrisiken bei Hundsdoerfer/Siegmund (2003) beschrieben.

[16] Vgl. Hundsdoerfer/Siegmund (2003).

[17] Vgl Bundesamt für Sicherheit in der Informationstechnik (2003), Abschnitt 3.7, Kryptokonzept. Görtz geht auch auf die Verfügbarkeit ein. Vgl. Görtz/Stolp (1999), S. 43.

Finanzverwaltung eingesetzten Hardware relevant. Es muss für den Erklärenden weitestgehend sichergestellt sein, dass er auf die zur Verfügung gestellten Kommunikationswege zugreifen kann. Die Verfügbarkeit des Webauftritts und damit auch die Downloadmöglichkeit von ElsterFormular soll durch den umfangreichen Schutz des Webservers u.a. durch Firewalls und durch redundante Systeme gesichert werden. Damit sollen insbesondere DDoS-Attacken verhindert werden.

5.3 Sicherheitsmaßnahmen während der Kommunikation zwischen Client und Webserver

Einen schematischen Überblick über Authentifizierung, Verschlüsselung und Datenfluss bei der elektronischen Kommunikation zwischen Steuerpflichtigen und Finanzverwaltung gibt die folgende Abbildung 6:

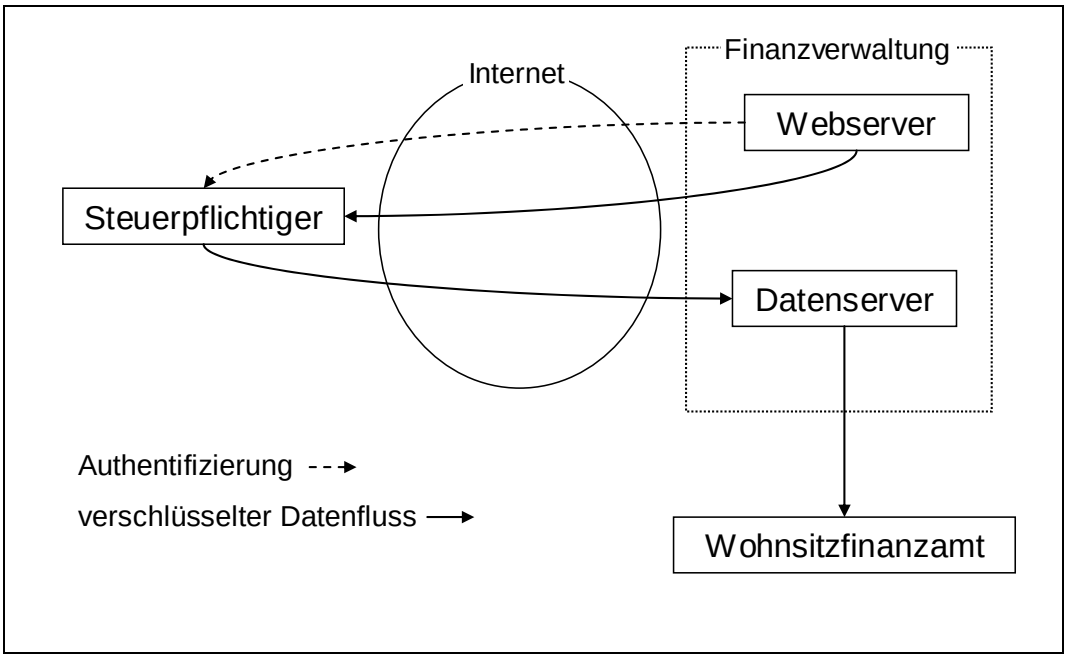

Abbildung 6: Schematische Darstellung des Datenflusses

5.3.1 Authentifizierung

Beim Download der Software ist von größter Bedeutung, dass der Anwender tatsächlich eine von der Finanzverwaltung zur Verfügung gestellte aktuelle Version von ElsterFormular erhält. Angreifer könnten versuchen, dem potentiellen Nutzer eine manipulierte Version zu übermitteln, um persönliche Daten auszuspähen. Dies könnte zum einen durch eine Modifizierung der Downloaddaten geschehen als

auch durch eine bereits modifiziert angebotene Version von ElsterFormular. Die Aktualität dieser Problematik zeigt das Ausspähen von Bankkunden, um mit Hilfe gefälschter Web-Seiten („Phishing“) an PIN-/TAN-Nummern etc. zu gelangen.

Demnach muss sichergestellt werden, dass der Anwender sich auf der Homepage der Finanzverwaltung und nicht auf einer gefälschten Webseite befindet und dass die übertragenen Daten (hier ElsterFormular) nicht von Dritten manipuliert werden. Ein SSL-Zertifikat soll sicherstellen, dass der Internetnutzer sich auf der richtigen Seite befindet. Der Webserver der Verwaltung authentifiziert sich über ein digitales Zertifikat (ISO X.509 Standard) unter Verwendung des https-Protokolls. Der Internet-Browser macht auch Angaben[18] über das benutzte Zertifikat[19] (Schloss-Symbol in der Statusleiste des Browsers).

Ein Authentifizierungsverfahren durch Zertifikate ist freilich nur in dem Grade sicher, wie auch die Zertifizierungsstelle sicher ist. Im Internetauftritt von ELSTER findet sich die Behauptung: „Das Zertifikat garantiert Ihnen, dass Sie tatsächlich mit www.elsterformular.de verbunden sind“. Dass jedoch auch ein solches Authentifizierungsverfahren mit Sicherheitsrisiken durch menschliche Fehlentscheidungen behaftet ist, zeigt der Fall von falsch ausgestellten Zertifikaten durch das Unternehmen verisign[20].

5.3.2 Verschlüsselung

Nach der Authentifizierung des ELSTER-Servers wird der Datentransfer einschließlich Download der Software über das https-Protokoll abgewickelt. Die Verwendung des SSL-Protokolls soll die Vertraulichkeit und die Integrität der Daten gewährleisten. Dadurch soll das bewusste Verändern der Downloaddaten verhindert werden.

---

[18] Die durch das Zertifikat bereitgestellten Informationen sind im dem ISO Standard X.509 festgelegt. Man kann hier erfahren, wer z.B. Antragsteller der Zertifikates ist (i.d.F. die Finanzverwaltung), welches Verschlüsselungsverfahren eingesetzt wird, wie lange das Zertifikat gültig ist und wer das Zertifikat ausgestellt hat.

[19] Nähere Information lassen sich auf Seiten des Elster-Projekts unter https://www.elster.de/ssl/elfo/main-anw-form-main-01-lk-sich.htm finden. Elster benutzt dabei Zertifikate der Firma verisign.

[20] Vgl. hierzu o.V. (2001).

Symmetrische Verschlüsselungsverfahren benutzen sowohl für die Ver- als auch für die Entschlüsselung der Daten denselben Schlüssel. Im Gegensatz dazu verwenden asymmetrische Verfahren zwei unterschiedliche Schlüssel. Der öffentliche, für jeden zugängliche Schlüssel wird für die Verschlüsselung eingesetzt. Hingegen ist der private Schlüssel für die Entschlüsselung nur dem Empfänger der Daten bekannt. SSL bedient sich sowohl symmetrischer als auch asymmetrischer Kodierungsschlüssel. Über ein Public-Key-Verfahren wird zunächst eine gesicherte Verbindung zwischen WebServer und Anwender unter Verwendung eines asymmetrischen Schlüssels (1024 Bit) aufgebaut. Wiederum über diese sichere Verbindung wird der symmetrische Schlüssel ausgetauscht (128 Bit), welcher für die Kodierung der jeweiligen Daten verantwortlich ist[21]. Letzterer Schlüssel wird anhand von Zufallszahlen erzeugt und dient als Session Key, der nur für die jeweilige Sitzung verwendet werden kann und am Ende der Sitzung wieder gelöscht wird. Die Integrität der Daten wird über eine schlüsselabhängige kryptografische Hashfunktion (MAC) erreicht. Diese garantiert, dass eine mögliche unbefugte Änderung der Daten sofort wahrgenommen und zurückgewiesen wird. Auf die oben genannten Verfahren wird auch zurückgegriffen, wenn die Updatefunktion von ElsterFormular bzw. ElsterClient genutzt wird.

5.4 Sicherheitsrisiken während der Dateneingabe per ElsterFormular

Nachdem der Benutzer ElsterFormular auf seinen Rechner geladen hat, besteht darüber hinaus die Möglichkeit, mit Hilfe des ElsterByteCodeChecker und eines Fingerprints[22] die Integrität der Software zu prüfen. Diese Integritätsprüfung ist dazu geeignet, die Software sowohl auf eventuelle technische Übertragungsfehler zu überprüfen, als auch Modifikation durch einen Angreifer aufzudecken, wenngleich derartige Modifikationen bereits wirksam durch die gesicherte Übertragung ausgeschlossen sein sollten.

Nach der Installation kann der Anwender seine persönlichen Steuerdaten eingeben und auf seinem lokalen Computer speichern. Hier besteht u.E. die größte Sicherheitslücke. Verschlüsselungsverfahren bei Download und Versendung der

---

[21] Im Detail wird nicht der symmetrische Schlüssel ausgetauscht, sondern nur die relevanten Informationen, um diesen Schlüssel auf beiden Seiten berechnen zu können, werden gesandt.

Daten nützen wenig, wenn auf dem Computer des Erklärenden Keylogger, Trojaner, Würmer oder andere Malware[23] die Privatsphäre ausspionieren. Die schnelle Verbreitung der in den letzten Monaten aufgetauchten Schädlinge zeigt, dass hier noch große Sicherheitsdefizite bestehen[24]. Auf den Internetseiten des Projektes ist ein rudimentärer Benutzerleidfaden zu finden, der darstellt, welche Bedrohungen in einer ungesicherten Computerumgebung bestehen, und der die dafür notwendigen Gegenmaßnahmen hervorhebt. Jedoch richten sich diese Hinweise eher an den technisch versierten Anwender als an den Durchschnittsbenutzer[25].

Zwar ist das Risiko gering, dass die persönlichen Steuerdaten durch einen Angreifer verfälscht werden, da diese derzeit noch mit den Daten der komprimierten Erklärung abgeglichen werden können. Jedoch ist bereits das Ausspionieren privater Daten als Sicherheitsrisiko anzusehen. Die Gefahrenlage verschärft sich, sobald auf die komprimierte Steuererklärung zugunsten der digitalen Signaturkarte komplett verzichtet wird. Dabei könnte von der Finanzverwaltung für die Sicherheit am Computer des Steuerpflichtigen noch mehr getan werden. Zum einen wäre eine Art „Online-Check" möglich, der überprüft, ob auf dem Computer sämtliche Sicherheitspatches für das jeweilige Betriebssystem installiert sind. Zum anderen finden sich nur wenige und teilweise sehr technisch gehaltene Informationen bezüglich dieses Themas auf den Seiten von ELSTER. Ergänzende Angebote (wie z.B. Freeware-Programme zum Aufspüren von Trojanern und Viren sowie weiterführende Informationen zu potentiellen Sicherheitsrisiken) sind hier u.E. wünschenswert.

5.5 Sicherheitsmaßnahmen während der Kommunikation zwischen Client und Server der Finanzverwaltung

Nachdem der Benutzer seine Daten eingegeben hat, erfolgt die eigentliche Übertragung der Daten an das jeweilige Rechenzentrum der Finanzverwaltung. Die

---

[22] Die Prüfsumme des Fingerprints ist zur Kontrolle auf den Seiten von Elster zu finden.

[23] Abkürzung für malicious software.

[24] Vgl. Fn. 15.

[25] Vgl. Benutzerleitfaden zu Elster: https://www.elster.de/ssl/download/Benutzerleitfaden_Elster_SIG.pdf.

hierbei auftretenden Sicherheitsrisiken sind analog zu jenen, die auch bei dem Download von ElsterFormular entstehen. Die Vertraulichkeit und Integrität der Daten wird über ein hybrides Verschlüsselungsverfahren unter Verwendung symmetrischer und asymmetrischer Schlüssel erzeugt[26]. Die dabei eingesetzten Verschlüsselungsverfahren sind 3DES[27] und RSA. Der DES[28] gehört wohl zu den bekannten symmetrischen Verschlüsselungsverfahren. Aufgrund des symmetrischen Verfahrens muss der Schlüssel über einen sicheren Kanal ausgetauscht werden, was einen Nachteil darstellt. Vorteile symmetrischer Verfahren sind die einfache Schlüsselerzeugung, die Schnelligkeit (hoher Datendurchsatz) sowie die Sicherheit bei relativ kurzer Schlüssellänge. Die ursprüngliche Länge des DES betrug 56 Bit, jedoch wurde dieses Verfahren schnell zu unsicher[29]. Als Nachfolger zum DES etablierte sich als derzeitiger Standard der 3DES in der Form einer dreifach hintereinander geschalteten Verschlüsselung. In der Praxis hat sich derzeit dieses Verfahren mit einer Schlüssellänge von 112 Bit durchgesetzt[30]. RSA gehört zu den asymmetrischen Kryptografieverfahren. Der Nachrichtenempfänger erzeugt hierbei zwei Schlüssel: Der öffentliche Schlüssel (public key) ist nur für die Verschlüsselung der Nachricht vorgesehen und kann dem Sender ohne weitere Maßnahmen unverschlüsselt zugesandt werden. Entschlüsselt werden kann die Nachricht über den zweiten (privaten) Schlüssel, der im alleinigen Besitz des Empfängers der Nachricht verbleibt. Vorteil solcher Verfahren ist die Tatsache, dass der öffentliche Schlüssel über einen unsicheren Kanal übertragen werden kann bzw. für jeden verfügbar ist[31]. Nachteilig ist, dass die Schlüsselerzeugung sehr komplex ist, das Verfahren im Allgemeinen langsam und dass es größeren Erfolg versprechende Angriffsstrategien gibt als das reine Ausprobieren sämtlicher Schlüssel. Folglich

---

[26] Auch wenn dieses Verfahren sehr dem Verfahren unter Verwendung von SSL ähnelt, sind jedoch im Detail beide Mechanismen unterschiedlich, weshalb bei SSL nicht von einem hybriden Verfahren gesprochen werden kann. Für die Detailunterschiede vgl. Eckert (2003), S. 589 - 601.

[27] 3DES basiert auf dem DES.

[28] Der Data Encryption Standard (DES) wurde Anfang der 70 Jahre von IBM entwickelt.

[29] Bereits 1997 gelang es, durch eine vollständige Schlüsselsuche den DES zu überwinden.

[30] Bei einer Schlüssellänge von 112 Bit würde eine Attacke mit dem Ziel der vollständigen Schlüsselsuche mit derzeit verfügbarer Hard- und Software etwa 10^9 Jahre dauern. Das Alter des Universums wird auf 10^{10} Jahre geschätzt. Vgl. Eckert (2003), S. 249 - 258.

[31] Dieser Vorteil wird von den digitalen Zertifikaten ausgenutzt.

müssen solche Schlüssel verhältnismäßig länger sein, um einen vergleichbaren Schutz zu bieten wie symmetrische Schlüssel. Ferner muss sichergestellt werden, dass der öffentliche Schlüssel auch wirklich der Person zugeordnet ist, mit welcher man kommunizieren will.

Bei der Übermittlung der relevanten Steuerdaten wird nun durch Anwendung des Hybridverfahrens erreicht, dass sowohl die Vorteile von symmetrischen als auch von asymmetrischen Verfahren genutzt werden können. Mit Hilfe des Public-Key Verfahrens wird der eigentliche Schlüssel, welcher die Daten des Anwenders verschlüsselt, kodiert. Somit kann zum einen ein unsicherer Kanal wie das Internet genutzt werden. Zum anderen muss nicht auf die Sicherheit und die Schnelligkeit der symmetrischen Verschlüsselung verzichtet werden. Für die Nichtabstreitbarkeit des Versands der Erklärung bietet dieses Verfahren allein noch keine Lösung, so dass derzeit neben dem digitalen Versand im Regelfall noch der zusätzliche Versand der komprimierten Steuererklärung notwendig ist.[32]

Bezüglich der Sicherheitsrisiken und -maßnahmen bei den Rechenzentren der Finanzverwaltung kann grundsätzlich auf den Anfang dieses Abschnitts verwiesen werden, in dem die Problematik anhand des WebServers erläutert wurde. Vertraulichkeit und Verfügbarkeit werden hier auch durch ein mehrschichtiges Verfahren aus Firewalls, Paketfiltern etc. gewährleistet. Zudem ist das Rechenzentrum nicht direkt an das Internet angeschlossen, sondern erhält die Daten über eine Clearingstelle[33].

Insgesamt können die unternommenen Bemühungen, die Sicherheit der Daten*übertragung* zu gewährleisten, als vorbildlich bezeichnet werden. Nachholbedarf besteht u.E. bei der Unterstützung der Nutzer, auf ihren Computern Sicherheit zu gewährleisten.

---

[32] Für die digitale Signatur vgl. Abschnitt 3.2.

[33] Vgl. Hundsdoerfer/Siegmund (2003).

5.6 Sicherheitsrisiken der digitalen Signatur

Anforderungen an die digitale Signatur ergeben sich direkt aus der Funktion einer herkömmlichen handschriftlichen Unterschrift. Die Anforderungen sind im Einzelnen[34]:

- **Identifikation:** Die Unterschrift gibt eindeutig Auskunft über die Person des Unterzeichners.
- **Echtheit:** Die Unterschrift bezeugt, dass das Dokument dem Aussteller vorgelegen hat und von ihm anerkannt wurde.
- **Abschluss:** Die Unterschrift erklärt den Text für sachlich richtig und inhaltlich vollständig.
- **Warnung:** Durch die Notwendigkeit, dass eine Unterschrift geleistet werden muss, wird dem Verfasser die rechtliche Bedeutung des Dokumentes aufgezeigt.

Die Echtheit der digitalen Signatur wird durch diverse Sicherheitsmaßnahmen garantiert, so dass eine Fälschung der Signatur schwierig ist. Zu den Maßnahmen gehören u.a. eine PIN-Nummer für die Chipkarte, Verschlüsselungsmechanismen, die den eigentlichen Schlüssel auf der Chipkarte schützen, und elektrotechnische Verfahren, die verhindern, dass der Inhalt der Karte mit einem Kartenleser dupliziert werden kann.

Die Übertragung und Signierung der elektronischen Steuererklärung mit einer digitalen Signatur funktioniert wie folgt: Ist die Dateneingabe in ElsterFormular abgeschlossen, werden die lokal gespeicherten Daten an den ElsterOnlineManager (EOM) übergeben. Dieser sendet die eingegeben Informationen an den ElsterServer, der eine Plausibilitätsprüfung der steuerrelevanten Aspekte vornimmt. Nach Prüfung der Daten werden diese zurück an den EOM gesendet und dort nochmals für den Benutzer angezeigt. Aufgrund eines Sandbox-Verfahrens[35] sind die Daten nun gesichert, da sie von außen nicht mehr verändert werden können. Im letzten Schritt werden die gesicherten Daten durch Zugriff auf die Signaturkarte

---

[34] Vgl. Eckert (2003), S. 307.

[35] Dies ist ein Verfahren, das Prozesse voneinander abschottet, um den Zugriff von außen zu verhindern.

des Steuerpflichtigen signiert, wobei dem Steuerpflichtigen die rechtliche Bedeutung dieser Aktion mitgeteilt wird. Den Daten wird das auf der Chipkarte gespeicherte Benutzerzertifikat beigelegt. Der ElsterServer ist an eine Datenbank gekoppelt, die Zugriff auf sämtliche ausgestellten Signaturen hat. Bei Einsendung der Daten wird die benutzte Signatur kontrolliert, und die Steuerdaten werden, sofern die Prüfung keine Fehler ergeben hat, auf dem Server der Finanzverwaltung zur Weiterverarbeitung abgelegt. Im Anschluss an den Vorgang können die signierten Daten noch lokal gespeichert werden. Rechtlich ist die Steuererklärung dem Finanzamt mit dem Zeitpunkt der Speicherung auf dem Server zugegangen[36].

Theoretische Sicherheitsrisiken treten sowohl bei der eigentlichen Datenübermittlung als auch bei dem Verifizierungsverfahren auf. Sicherheitsrisiken bei dem Verifizierungsprozess bestehen hauptsächlich darin, dass von Malware der Versuch unternommen werden kann, den digitalen Schlüssel auszulesen, zu duplizieren und danach für andere Verwendungszwecke zu missbrauchen. Für die Sicherungsmaßnahmen bzgl. der Datenübermittlung kann auf Abschnitt 5.3 verwiesen werden. Analog zur komprimierten Steuererklärung ist die größte Schwachstelle in der ungesicherten Computerumgebung zu sehen. Sowohl das Verifizierungsverfahren für die Erstellung der Chipkarte als auch die eigentliche digitale Signierung sind bezogen auf den Zweck als sicher einzustufen. Durch die Nutzung der digitalen Signatur treten keine wesentlich neuen Sicherheitsrisiken auf[37]. Im Gegenteil: Die digitale Signatur ist insgesamt als sicherer anzusehen als die herkömmliche Unterschrift[38]. Der Signaturprozess erfordert zum einen den Besitz der Chipkarte und zum anderen die geheime PIN-Nummer, um auf die Signatur zuzugreifen. Demnach wird die Fälschung der Unterschrift im Vergleich zum herkömmlichen Verfahren erheblich erschwert, sofern nicht die PIN-Nummer zusammen mit der Chipkarte aufbewahrt wird. Somit ist auch hier wie bei der elektronischen Datenübertragung der Steuererklärung das größte Gefahrenpotential in ungesicherten Heimcomputern der Nutzer zu sehen.

---

[36] Vgl. § 87a Abs. 1 S. 2 AO; zudem Wünsch (2004), § 87a, Rz. 27, 33.

[37] Verwiesen sei hier auf die theoretische Möglichkeit, Chipkarten zu duplizieren bzw. eine erfolgreiche Attacke gegen einen Signaturschlüssel durchzuführen.

[38] Vgl. Rossnagel (2002), S. 282.

Auch die Alternative zur Signaturkarte, die oben dargestellte Softwarelösung, ist nicht ohne Sicherheitsrisiken. Hier kann auf die zuletzt häufiger aufgetretenen Bedrohungen in Form von „Trojanern“ hingewiesen werden, die auch die elektronische Signatur ausspähen könnten[39]. Welche Risiken aber im Einzelnen hier auftreten werden, wird von der genauen Ausgestaltung des Verfahrens abhängen.

[39] Vgl. Bachfeld (2004).

6 Zum ELSTER-Einsatz bei Steuerberatern

Wie oben dargestellt, ist die Beteiligung von Steuerdienstleistern (Steuerberatern und Lohnsteuerhilfevereinen) am ELSTER-Verfahren derzeit gering. Um Gründe hierfür zu untersuchen, sollen zunächst die Möglichkeiten der Steuerberater (und Lohnsteuerhilfevereine), ihre Mandanten bei der Einkommensteuererklärung zu unterstützen, dargestellt werden:

- Im herkömmlichen Verfahren wird dem Finanzamt - durch den Steuerpflichtigen oder den Berater - allein eine papiergebundene Steuererklärung zugeschickt. Dabei kann sich die Leistung des Beraters in einer Beratung erschöpfen; regelmäßig übernimmt der Steuerdienstleister aber auch das Ausfüllen des Formulars. Dies kann manuell oder mit Hilfe von Software (DATEV oder andere Anbieter) erfolgen.
- Eine elektronische Einkommensteuererklärung könnte dem Finanzamt vom Steuerpflichtigen oder vom Berater übersandt werden. Der Berater könnte für die Dateneingabe und -übertragung ELSTER (ElsterFormular und ElsterClient) oder andere Software einsetzen. Sowohl die DATEV e.G. als auch andere Softwareanbieter ermöglichen Beratern die elektronische Übermittlung von Einkommensteuererklärungen an das Finanzamt. Dabei wird zwar auch der ElsterClient eingesetzt, doch andere Schnittstellen sind stärker verbreitet. So erfolgt die elektronische Übermittlung der Einkommensteuererklärung durch die DATEV e.G. noch mit Hilfe eines proprietären Verfahrens. Ab dem Veranlagungszeitraum 2004 ist jedoch ein vollständiger Umstieg der DATEV e.G. auf das ELSTER-Verfahren geplant.

Über die Gründe, warum Steuerdienstleister Einkommensteuererklärungen weiterhin allein auf dem Postweg an die Finanzämter übermitteln, sind nur Vermutungen möglich. Gegen die elektronische Einkommensteuererklärung könnte aus Sicht der Berater sprechen:

- Wenn von der - wie dargestellt wenig verbreiteten - digitalen Signatur abgesehen wird, muss der Steuerpflichtige auch bei elektronischer Übermittlung der Einkommensteuererklärung noch eine Unterschrift (unter die komprimierte Erklärung) leisten. Aus diesem Grund bringt die

elektronische Einkommensteuererklärung für die Arbeitsorganisation des Beraters kaum Vorteile.

- Software für die Eingabe der Steuerdaten - samt Möglichkeit der Speicherung - ist bei Steuerberatern regelmäßig vorhanden. Damit entfällt der Vorteil der kostenlosen ElsterFormular-Software. Auch die Ausfüllhilfen werden hier vermutlich kaum benötigt.
- Die Möglichkeit einer elektronischen Bescheidkontrolle bringt für Steuerberater wegen ihrer Erfahrungen bei der Bescheidkontrolle und wegen der Einbindung der Bescheidkontrolle in die Betriebsorganisation wenig bis nichts.
- Bei elektronischer Übermittlung der Einkommensteuererklärung mit Hilfe der DATEV entstehen dem Steuerberater zusätzliche Kosten im Vergleich zum Selbstausdruck des herkömmlichen papiergebundenen Einkommensteuerformulars.

Viele Steuerberater nutzen bereits die Möglichkeit, Umsatzsteuervoranmeldungen und Lohnsteueranmeldungen ihrer Mandanten auf elektronischem Weg zu übermitteln. Dies zeigt, dass der Berufsstand die Vorteile der elektronischen Kommunikation sehr wohl nutzt. Solche Vorteile scheinen viele Berater aber derzeit für die elektronische Einkommensteuererklärung nicht zu sehen.

7 Fazit und Ausblick

Zwar kann für die digitale Steuererklärung in Deutschland künftig mit Steigerungen der Teilnehmerzahlen gerechnet werden. Jedoch deutet die im internationalen Vergleich relativ geringe Nutzungsquote stark darauf hin, dass derzeit die Steuerpflichtigen die Vorteile der elektronisch übermittelten Steuererklärung als gering einschätzen. Derzeit bietet die elektronische Übermittlung der Einkommensteuererklärung mit ELSTER den Steuerpflichtigen als Vorteile eine schnellere Bearbeitung der Einkommensteuererklärung beim Finanzamt, die Möglichkeit der elektronischen Bescheiddatenabholung und - sofern die Daten auf dem Computer des Steuerpflichtigen noch gespeichert und verfügbar sind - die Übernahme von Vorjahresdaten bei der nächsten Einkommensteuererklärung. Echte Vorteile bietet die elektronische Einkommensteuererklärung aber vor allem den Finanzbehörden, bei denen die zeitraubende und teure Eingabe der Erklärungsdaten entfällt. Für die bisher im internationalen Vergleich eher geringe Akzeptanz von ELSTER bei den Steuerpflichtigen spielen Sicherheitsbedenken vermutlich kaum eine Rolle: Online-Banking wird weit stärker (von ca. 11 Mio. der 34,4 Mio. Bürger in Deutschland) genutzt[40], obwohl die für ELSTER angewandten Sicherheitsmaßnahmen als wirksamer zu beurteilen sind als die im Online-Banking eingesetzten Maßnahmen. Die größte Sicherheitslücke der elektronischen Steuererklärung wird - wie auch beim Online-Banking - regelmäßig ein ungeschützter Computer des Nutzers sein.

Das zentrale Problem von ELSTER liegt derzeit darin, dass Medienbrüche noch nicht vollständig vermieden werden. Selbst wenn der Steuerpflichtige bereits die Möglichkeiten der digitalen Signatur nutzen sollte, sind weiterhin Belege (Spendenbescheinigungen, teilweise noch die Lohnsteuerkarte) in Papierform an das Finanzamt zu senden. Ohne digitale Signatur muss zusätzlich eine komprimierte Einkommensteuererklärung in Papierform unterschrieben und versendet werden. An der Vermeidung von Medienbrüchen wird freilich gearbeitet, sowohl bezüglich der Signatur als auch der Lohnsteuerkarte.

---

[40] Vgl. van Eimeren/Gerhard/Frees (2003), S. 347.

Um die Nutzungsquote zu steigern, könnten den Steuerpflichtigen beim Einsatz von ELSTER weitere Vorteile geboten werden. So könnten etwa die Bearbeitungszeiten elektronisch eingereichter Steuererklärungen noch weiter verkürzt werden, was den Steuerpflichtigen kommuniziert werden müsste[41]. Auch könnte dem ELSTER-Nutzer Einblick in sein „Steuerkonto" oder in den Bearbeitungsstatus seiner Erklärung gegeben werden. Die Finanzverwaltung könnte dem ELSTER-Nutzer Statistiken oder Berechnungshilfen zur Verfügung stellen, die ihm die Höhe der Steuerzahlungen und sein zu versteuerndes Einkommen im Zeitablauf verdeutlichen und ihm Durchschnitts- und Grenzsteuersatz mitteilen. Darüber hinaus ist eine Funktion denkbar, welche dem Steuerpflichtigen mögliche Veranlagungsszenarien im Sinne einer rudimentären Beratungsfunktion an die Hand stellt (z.B. Variation beim Verlustvortrag/Rücktrag). Während Gewinnspiele als Anreizmechanismen für die Nutzung von ELSTER bereits von der Finanzverwaltung eingesetzt werden[42], wird die Möglichkeit eines Steuererlasses von z.B. 10 € bei erstmaliger Einreichung einer digitalen Steuererklärung bisher nicht genutzt.

Hilfreich für die Verbreitung von ELSTER wäre auch eine besser koordinierte Einführung des E-Governments. Die Akzeptanz einer digitalen Signaturkarte könnte massiv gesteigert werden, wenn der Bürger mit dieser ein breites Angebot von Verwaltungsdienstleistungen in Anspruch nehmen könnte. Zudem wäre vorstellbar, dass eine digitale Signaturkarte auch die herkömmliche EC-Karte sowie die Krankenversicherungskarte enthält, da diese weit verbreitet sind[43]. Dann könnten auch Krankenkassen als Trust Center fungieren und bei Ausstellung einer neuen Versicherungskarte zugleich eine digitale Signaturfunktion anbieten. Da - wie speziell bei ELSTER ersichtlich - die Vorteile vor allem auf der Seite der Behörden liegen, könnten für einen begrenzten Zeitraum die Kosten der Steuerpflichtigen für

---

[41] Finanztest bestätigt anhand eines durchgeführten Tests, dass in den meisten Bundesländern die elektronische Steuererklärung deutlich schneller bearbeitet wird als die papiergebundene. Jedoch wird auch angemerkt, dass zum einem in einigen Bundesländern die Bearbeitungszeit der Elster-Erklärung erheblich länger dauert als jene der papiergebundenen und zum anderen die Grenze von sechs Wochen als akzeptable Bearbeitungszeit von einigen Finanzämtern bei der Bearbeitung der Elster-Erklärung deutlich überschritten wird. Vgl. o.V. (2004b).

[42] Vgl. Wilkens (2004).

[43] Dabei auftretende Datenschutzprobleme könnten technisch gelöst werden.

die Signaturkarte und die notwendige Hardware vom Staat subventioniert werden. So könnte das Projekt ELSTER in ein E-Government-System eingebettet werden.

Literaturverzeichnis

Bachfeld, Daniel (2004): Trojaner klauen Bank-Kunden PINs und TANs, in: Heise Online News, 09.09.2004, elektronisch veröffentlicht unter der URL http://www.heise.de/newsticker/meldung/50793.

BMF (2003): Endstufe: Vollelektronisches Lohnsteuer-/Einkommensteuerverfahren, 11.03.2003, Berlin.

Bundesamt für Sicherheit in der Informationstechnik (2003): IT-Grundschutzhandbuch, 5. Ergänzungslieferung, 2003.

Eckert, Claudia (2003): IT-Sicherheit - Konzept, Verfahren, Protokolle -, 2. Auflage, München 2003.

Eimeren, Birgit van; Gerhard, Heinz; Frees, Beate (2003): Internetverbreitung in Deutschland: Unerwartet hoher Zuwachs, in: Media Perspektiven, Jg. 7, Heft 8, 2003, S. 338 - 358, elektronisch veröffentlicht unter der URL http://www.daserste.de/service/ardonl03.pdf.

Görtz, Horst; Stolp, Jutta (1999): Informationssicherheit in Unternehmen - Sicherheitskonzepte und -lösungen in der Praxis -, 1. Auflage, München 1999.

Hoffmann, Marie-Luise; Votsmeier, Volker (2004): Vorsicht Finanzamt, in: Capital, Jg. 43, Heft 11, 2004, S. 86 - 101.

Hundsdoerfer, Jochen; Siegmund, Olaf (2003): Elster: Vorteile, Nachteile und IT-Sicherheitsrisiken der elektronischen Einkommensteuererklärung, in: Der Betrieb, Jg. 56, Heft 46, 2003, S. 2460 - 2466.

Jahr-Weidauer (2004): Steuererklärung am PC wird in Berlin immer beliebter, in: Die Welt Online, 26.1.2004, elektronisch veröffentlicht unter der URL http://www.welt.de/data/2004/01/26/228661.html.

Mummert Consulting (2003): Bürger gehen den Behörden ins Netz, in: Presseinformation, 18.03.2003, elektronisch veröffentlicht unter der URL http://217.111.5.68/presse/mummertpress/do_news.phtml?aid=58.

o.V. (2001): Gefahr durch gefälschte MS-Zertifikate, in: tecchannel Online, 23.03.2001, elektronisch veröffentlicht unter der URL http://www.tecchannel.de/news/20010323/thema20010323-3979.html.

o.V. (2002): Steuererklärung per Internet - Die elektronische Steuererklärung ist auf dem Vormarsch, in: Der Steuerzahler, Jg. 53, Heft 7, 2002, S. 133.

o.V. (2004a): Neuer Wurm schaltet Computer aus, in: Financial Times Deutschland Online, 03.05.2004.

o.V. (2004b): Es könnte überall flott gehen, in: Finanztest, o. Jg., Heft 10, 2004, S. 62 - 65.

Röhrs, Heinz-Peter (2002): Auf dem Weg zur papierlosen Steuererklärung, in: Gabriel, Roland; Hoppe, Uwe (Hrsg.): Electronic Business, Heidelberg 2002, S. 447 -475.

Rossnagel, Alexander (2002): Der elektronische Ausweis - Notwendige und mögliche Identifizierung im E-Government -, in: Datenschutz und Datensicherheit (DuD), Jg. 26, Heft 5, 2002, S. 281 - 285.

Senatsverwaltung für Finanzen (2004): Elektronische Steuererklärung mit Elster, in: Pressemitteilung, 05.05.2004, elektronisch veröffentlicht unter der URL http://www.berlinews.de/archiv-2004/2131.shtml.

Wilkens, Andreas (2004): Finanzämter werben für Online-Steuererklärung, in: Heise online News, 09.02.2004, elektronisch veröffentlicht unter der URL http://www.heise.de/newsticker/meldung/44439.

Wünsch, Doris (2004) in: Pahlke, Armin; Koening, Ulrich, Kommentar zur Abgabenordnung, Stand März 2004.

Verzeichnis der Arbeitsberichte

Lange, Jörg: Sicherheit als notwendige Eigenschaft computergestützter Informationssysteme – Rechtliche Rahmenbedingungen und gesellschaftliche Aspekte, Arbeitsbericht Nr. 1 des Instituts für Sicherheit im E-Business, Bochum 2003

Hundsdoerfer, Jochen; Siegmund Olaf: ELSTER – Vorteile, Nachteile und IT-Sicherheitsrisiken der elektronischen Einkommensteuererklärung, Arbeitsbericht Nr. 2 des Instituts für Sicherheit im E-Business, Bochum 2003

Gabriel, Roland; Gersch, Martin; Rüdiger, Klaus (Hrsg.): Sicherheit im E-Business – Eröffnungsworkshop des Instituts für Sicherheit im E-Business, Arbeitsbericht Nr. 3 des Instituts für Sicherheit im E-Business, Bochum 2003

Lange, Jörg: Sicherheit als materielle Gestaltungsanforderung an computergestützte Informationssysteme, Arbeitsbericht Nr. 4 des Instituts für Sicherheit im E-Business, Bochum 2004

Gabriel, Roland; Rüdiger, Klaus; Neuber, Susanne (Hrsg.): „IT-Sicherheit als Managementaufgabe" – Workshop des Instituts für Sicherheit im E-Business, Arbeitsbericht Nr. 5 des Instituts für Sicherheit im E-Business, Bochum 2004

Hechtner, Frank; Hundsdoerfer, Jochen; Siegmund, Olaf: Wann wird sich die elektronische Einkommensteuererklärung durchsetzen? - Zum Sicherheits- und Entwicklungsstand von ELSTER, Arbeitsbericht Nr. 6 des Instituts für Sicherheit im E-Business, Bochum 2004

Sie können die Arbeitsberichte gegen eine Schutzgebühr von 15 Euro pro Bericht bestellen:

Institut für Sicherheit im E-Business
Ruhr-Universität Bochum
Fakultät für Wirtschaftswissenschaft
Gebäude GC 3/29
D-44780 Bochum

Tel.: +49 (0)234 – 32 25325
Fax: +49 (0)234 – 32 14350
iseb@ruhr-uni-bochum.de
http://www.iseb.ruhr-uni-bochum.de

Stand: November 2004