datenschutz cert

Kurzgutachten zur Erteilung eines Datenschutz-Gütesiegels für das Produkt „ElsterOnline“

im Auftrag des Bayerischen Landesamtes für Steuern

datenschutz cert GmbH

Version 1.0

24. Juni 2010

datenschutz cert

Inhaltsverzeichnis

Kurzgutachten zur Erteilung eines Datenschutz-Gütesiegels für das Produkt „Elster-Online“

1. Zeitraum der Prüfung

Die Begutachtung erstreckte sich auf den Zeitraum von 27.01.2009 bis 10.05.2010 und beinhaltete eine konzeptionelle Analyse der vom Bayerischen Landesamt für Steuern und der secunet AG zur Verfügung gestellten Unterlagen sowie eine praktische Analyse durch Tests der online zur Verfügung gestellten Applikation.

2. Antragstellerin

Antragstellerin dieses Gutachtens:

Bayerisches Landesamt für Steuern
Referat IuK
Dienststelle München
80284 München

Gesamtverantwortlicher für die IT-Sicherheit des Produkts ELSTER und Projektleiter ist Herr Franz Widholm (Bayerisches Landesamt für Steuern). Ansprechpartner sind Michael Gebauer und Thomas Mohnhaupt (beide secunet AG).

3. Sachverständiger/Prüfstelle

Sachverständige dieses Gutachtens ist die Prüfstelle

datenschutz cert GmbH
Barkhausenstr. 2
27568 Bremerhaven

unter der Leitung von Herrn Dr. Sönke Maseberg (Technik) und Frau Dr. Irene Karper (Recht). Ansprechpartner für diese Begutachtung sind Frau Dr. Irene Karper (Recht) und Herr Dr. Sönke Maseberg (Technik) sowie Herr Thorsten Kamp (Technik).

4. Kurzbezeichnung des IT-Produktes

Gegenstand des Audits ist das Produkt

ElsterOnline Client Server Architektur (Stand: 10.05.2010).

ElsterOnline ist ein gemeinsames Projekt der deutschen Steuerverwaltung von Bund und Ländern, das die sichere elektronische Übermittlung zum Ziel hat. Betreiber des Verfahrens ELSTER (ELektronische STeuerERklärung) ist das Bayerische Landesamt für Steuern, welchem auch das Verfahrensmanagement obliegt. Das Bayerische Landesamt für Steuern wird für dieses Zertifizierungsverfahren von der secunet AG beraten.

Basis der elektronischen Übermittlung von Dokumenten an die Finanzverwaltungen der Länder ist § 150 i.V.m. § 87a Abgabenordnung (AO). § 87a Abs. 6 AO sieht vor, dass neben der „qualifizierten elektronischen Signatur“ im Sinne des Signaturgesetzes bis zum 31. Dezember 2011 auch ein „*anderes sicheres Verfahren*“ zugelassen werden kann.

Bei dem zu auditierenden Produkt handelt es sich um eine Client-Server-Architektur, die z.T. über öffentliche Kommunikationskanäle miteinander kommuniziert, um steuerrelevante Daten auszutauschen – bspw. zur Abgabe einer Steuererklärung. Das

Produkt wird dabei auch von Anwendern (Bürgern, Gewerbe) und der Finanzverwaltung im Lande Schleswig-Holstein eingesetzt und ist damit grundsätzlich auditierbar.

5. Beschreibung des IT-Produkts, Zweck und Einsatzbereich

Ein Anwender kann über die Client-Server-Architektur mit seinem ELSTER-(Web)Client mit seiner Finanzbehörde kommunizieren – beispielsweise für

- elektronische Steuererklärung,
- Umsatzsteuervoranmeldung,
- Lohnsteueranmeldung,
- Steuerkontoabfrage,
- Übermittlung von Lohnsteuerdaten (durch Unternehmen) oder
- Voranmeldungen von Steuern.

Anwender können Privatpersonen, aber auch juristische Personen sein.

Mitteilungen von der Finanzbehörde zurück sind z.B. Statusmitteilungen, Übertragungsprotokolle, Übermittlungsbestätigungen von Steuererklärungen oder Anfragen oder eine Bescheidkopie (z.B. zum Abgleich mit den Daten innerhalb einer Steuersoftware z.B. Steuersoftware von Drittanbietern, ElsterFormular) in elektronischer Form, die nicht rechtsverbindlich sind. Steuerbescheide hingegen dürfen rechtsverbindlich ausschließlich von der Finanzverwaltung nur in Papierform zugestellt werden (Verwaltungsakt).

ElsterOnline besteht aus folgenden Komponenten, vgl. auch Abbildung 1:

- ELSTER-Client (Client-Komponente):

  Der ELSTER-Client befindet sich auf Seiten des Anwenders (bspw. des Steuerbürgers) und ist

  - als Web-Client (ELSTER-WebClient) oder
  - als ELSTER-Client innerhalb einer Anwendung (z.B. ElsterFormular, Steuersoftware von Drittanbietern) ausgeprägt.

  Der ELSTER-Client wird auf einem lokalen Rechner betrieben.

  Zur kryptographischen Absicherung der Kommunikation steht dem Anwender eine der folgenden Varianten zur Verfügung:

  - Schlüssel und Zertifikate als Software-PSE auf der Festplatte des Clients (ELSTER-Basis);
  - Schlüssel und Zertifikate auf einem USB-Stick (ELSTER-Spezial);

--- Signaturerstellungseinheit (SSEE) inkl. Schlüssel und Zertifikate (ELSTER-Plus)[1].

--- ElsterOnline-Portal (Server-Komponente):

Das ElsterOnline-Portal wird in einem Rechenzentrum betrieben und besteht aus mehreren Serversystemen für

--- die Registrierung und Anmeldung inkl. Authentisierung,

--- CA (Certification Authority) und DIR (Verzeichnisdienst) sowie

--- Postfach-Funktionalität.

--- ELSTER Clearingstellen (Server-Komponente):

Die ELSTER Clearingstellen werden in zwei Rechenzentren (München und Düsseldorf) betrieben und bestehen aus mehreren Serversystemen, um eingegangene ELSTER-Daten für die weitere Verarbeitung aufzubereiten und an die sog. ELSTER-Kopfstellen der Finanzbehörde des jeweiligen Bundeslandes weiterzuleiten.

Anschließend erfolgt die weitere Datenverarbeitung unter Verantwortung der jeweiligen Finanzverwaltung des jeweiligen Bundeslandes in eigenen hoheitlichen Rechenzentren. Die ELSTER-Kopfstellen gehören daher nicht zum Auditgegenstand.

Die Schnittstelle zwischen den Clearingstellen und den Länderkopfstellen bilden Kryptogateways.

Die Serverkomponenten in den zwei Rechenzentren (München und Düsseldorf) (ElsterOnline-Portal und -Clearingstellen) weisen jeweils ein ISO 27001-Zertifikat auf der Basis von IT-Grundschutz vom Bundesamt für Sicherheit in der Informationstechnik (BSI) auf.[2]

Die ELSTER-Kopfstellen gehören nicht zum auditierten Produkt. Auch die bei ELSTER mögliche Abgabe einer „komprimierten Steuererklärung“ ist nicht Gegenstand des Audits.

6. Tools, die zur Herstellung des Produkts verwendet wurden

Das zu betrachtende Produkt ElsterOnline ist eine Ansammlung von Anwendungen, welche die Übermittlung von Daten an die Clearingstellen, das Datenclearing sowie das Bereitstellen von Informationen für den Anwender hat:

--- ElsterOnline-Portal in der Clearingstelle, Release 16.0 vom 01.12.2009;

--- Wiesel Authentifizierungs-/Signatur-Prüfungskomponente in der Clearingstelle, Release 16.0;

--- ElsterFormular (Clientsoftware mit ELSTER-Client ERiC Version 10.7.6.25787), Version 10.3.2.0;

[1] Zur Klarstellung: Es werden keine qualifizierten elektronischen Signaturen verwendet. Bei SigG-konformen SSEEs werden die Authentisierungszertifikate und zugehörigen Schlüssel verwendet.
[2] BSI-IGZ-0028-2008, gültig bis: 28.08.2010 und BSI-IGZ-0036-2008, gültig bis: 26.10.2011.

--- Ericlet/EMS (Client/Server), Version 2009.3.0;

--- ECC (Annahmeinstanz der Länderkopfstellen), Version 2009.2.2.

7. Modellierung des Datenflusses

Die Abbildung (Abbildung 1) illustriert die wesentlichen Komponenten und den Datenfluss.

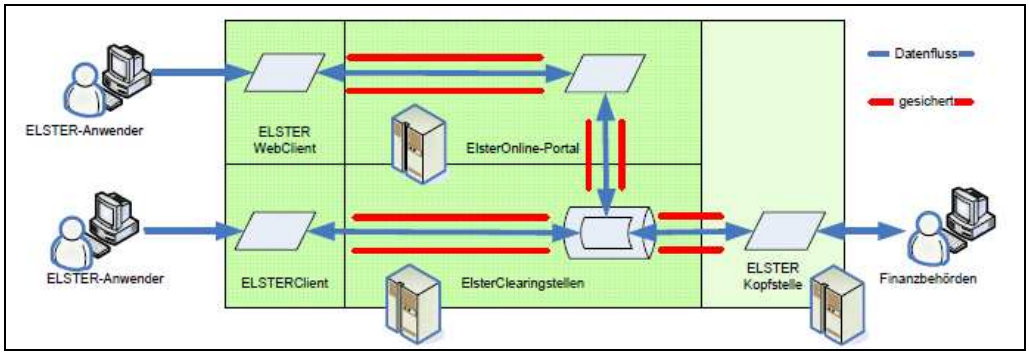

Abbildung 1: Komponenten

Die Erfassung und Verarbeitung von Daten im Rahmen der Nutzung des Produkts ElsterOnline unterteilt sich dabei in den Registriervorgang und den Nutzungsvorgang.

7.1 Registriervorgang

Der ELSTER-Anwender (dies ist eine natürliche oder juristische Person bzw. Organisation) muss sich zunächst registrieren lassen, um diesen Dienst nutzen zu können; die Registrierung läuft wie folgt ab:

--- Anmeldung mit Definition eines Kurznamens, Angabe von Name, Vorname, Geburtsdatum (nicht bei Organisationen), E-Mail-Adresse sowie Steuernummer des Steuersubjektes, zuständiges Finanzamt und Bundesland sowie Sicherheitsabfrage über das Internet.

Als Alternative zur Steuernummer kann die IdNr (lebenslange Steuer-ID) genutzt werden, sofern vom zuständigen Bundesland unterstützt.

Nicht zur Registrierung verwendet wird derzeit die Wirtschaftsidentifikationsnummer, die eTIN oder die Umsatzsteueridentifikation.

--- Anwender erhält eine Bestätigung per E-Mail zur Verifikation der E-Mail-Adresse.

--- Anwender ruft den mitgelieferten Link in der Bestätigungs-E-Mail auf und erhält eine Aktivierungs-ID (erster Passwortanteil) an die angegebene E-Mail-Adresse.

--- Die Finanzbehörde ermittelt anhand der übergebenen Daten (Identifikation über Name, Vorname, Geburtsdatum, Steuernummer oder IdNr.) die Postanschrift des Anwenders und versendet einen Aktivierungscode (zweiter Passwortanteil) per Post; dazu übermittelt ElsterOnline die Anmeldeda-

ten an die jeweilige Länderkopfstelle des steuerrechtlich zuständigen Bundeslandes des Registrierenden/Steuerpflichtigen.

In den Rechenzentren der Finanzbehörden wird die Steuernummer dann den dort gespeicherten Adressdaten zugeordnet; bei Verwendung der IdNr. erfolgt dies über eine Abfrage im Bundeszentralamt für Steuern (BZST) oder über die BZST-Datenbank. Die Adressverwaltung und -verifikation obliegt der jeweils zuständigen Finanzbehörde, nicht aber ELSTER.

Die Finanzbehörde nutzt hierfür andere Verfahren, die nicht Gegenstand dieses Audits sind. Das Produkt ElsterOnline verhindert für den Prozess der Registrierung mit IdNr. einen möglichen Missbrauch, da keine Adresseingabe in der Finanzbehörde erfolgt, indem während dieses Registrierungsprozesses eine ID-Recherche von einem internen Sicherheitssystem (Wiesel) auf die BZST-Datenbank bzw. BIMS-Datenbank durchgeführt wird. Die erhaltenen Adressdaten zu einer IdNr. werden über die Länderkopfstellen ausgeliefert. Damit werden die aktuellsten Adressdaten für die Registrierung dem postalischen Versand zugrundegelegt[3]. Die Adressdaten des BZST werden mit den Daten der Einwohnermeldeämter aktualisiert.

--- Nach Erhalt der Aktivierungs-ID und des Aktivierungscodes vervollständigt der Anwender seine Registrierung übers Internet:

  --- Identifikation über den mitgesendeten Link sowie Aktivierungs-ID und Aktivierungscode;

  --- bei ELSTER-Basis und ELSTER-Spezial: Erzeugung von zwei Schlüsselpaaren und Übermittlung der öffentlichen Schlüssel (Zertifikats-Request für Authentisierungs- und Verschlüsselungszertifikate) über das ElsterOnline-Portal zum ELSTER-Trustcenter;

  --- bei ELSTER-Plus: Übermittlung der Zertifikate (Authentisierungs- und Verschlüsselungszertifikat) der SSEE an das ElsterOnline-Portal; dabei gilt:

  Während des Registrierungsprozess' im ElsterOnline-Portal wird der Name nicht geprüft. Der Name wird hier ausschließlich zum Ansprechen des Kontoinhabers im Portal verwendet.

  Erst wenn eine Freischaltung zum Verfahren Steuerkonto-Abfrage erfolgt (dies ist erst auf Antrag und schriftlicher Genehmigung des Kontoinhabers möglich), wird der Name mit dem Namen aus dem Antrag auf Freischaltung abgeglichen.

--- Zertifikatserzeugung durch das ELSTER-Trustcenter und Übermittlung der signierten Zertifikate (Authentisierungs- und Verschlüsselungszertifikat) und Ablage in das vordefinierte PSE.

--- Diese Kommunikation ist über SSL abgesichert.

[3] Davon unabhängig ist die Angabe von Adressdaten des Benutzers in der jeweiligen Steuererklärung, die durchaus gewollt an eine dedizierte, vom Steuerpflichtigen angegebene Postadresse versendet werden kann.

7.2 Nutzungsvorgang

Für jede weitere Kommunikation zwischen Anwender und ElsterOnline – also den eigentlichen Kern der Datenerfassung und -verarbeitung – werden XML-Daten ausgetauscht – etwa zur Abgabe eines Formulares. Diese XML-Daten sind per SSL oder über eine Transportverschlüsselung auf Grundlage der ausgetauschten Authentisierungs- oder Verschlüsselungszertifikate abgesichert.

Für den Rückweg von der Finanzbehörde zu den ELSTER-Anwendern gilt: Rechtsgültige Bescheide der Finanzbehörde werden generell in Papierform versendet.

Elektronische Bescheid-Mitteilungen oder sonstige steuerliche Mitteilungen der Finanzbehörden werden bei allen ELSTER-Varianten (ELSTER-Basis, ELSTER-Spezial, ELSTER-Plus) elektronisch versendet und mit dem jeweiligen öffentlichen Verschlüsselungszertifikat des Anwenders verschlüsselt[4] in einer Bescheiddatenbank oder im privaten Bereich des Anwenders abgelegt. Damit kann ein Anwender mit seinem privaten Schlüssel die Bescheid-Mitteilungen oder sonstige steuerliche Mitteilungen entschlüsseln.

ELSTER-Plus bietet darüber hinaus die Steuerkontoabfrage über das ElsterOnline Portal und über die Clearingstelle an:[5]

--- Für die Steuerkontoabfrage über das ElsterOnline-Portal gilt: die Kontodaten werden jeweils mit dem Verschlüsselungszertifikat der SSEE des Anwenders verschlüsselt und für den Abruf in das jeweilige Postfach des Anwenders bereitgestellt.[6] Damit kann ein Anwender mit seiner SSEE die verschlüsselten Kontodaten entschlüsseln.

--- Für die Steuerkontoabfrage über die Clearingstelle gilt: Die Kontodaten werden online durch ein hybrides Verfahren mit einem generierten Session-Key in der Clearingstelle verschlüsselt. Damit kann ein Anwender die verschlüsselten Kontodaten entschlüsseln.

Für die eigentliche Finanzverwaltungs-interne Verarbeitung erfolgt eine Kommunikation zwischen der ELSTER Clearingstelle und den Finanzbehörden der Bundesländer via ELSTER-Kopfstelle. Diese Kommunikation erfolgt nicht über das Internet, sondern im zugangsgesicherten Behördennetz (DOI (Deutschland-Online Vorhaben "Infrastruktur" (DOI))-Netz, vormals TESTA) sowie zusätzlich verschlüsselt über Kryptoboxen.

Im Rahmen des technischen Betriebes von ElsterOnline fallen vor allem Protokolldaten auf Anwendungsebene an. Dies sind insbesondere Log-Daten sowie die IP-Adresse des anfragenden Rechners auf Portal bzw. Clearingstellen.

---

[4] Der private Schlüsselanteil des Anwenders für die Entschlüsselung liegt entweder in seinem Soft-PSE, im Sicherheitsstick oder in der Signaturkarte; der für die Verschlüsselung verwendete öffentliche Schlüssel ist auf dem Verschlüsselungszertifikat hinterlegt.

[5] Aufgrund unterschiedlicher technischer Systeme unterscheiden sich die beiden beschriebenen Wege für das Portal und für die Zustellung über die Clearingstelle.

[6] Im Postfach sind sämtliche ein- und ausgehenden Mitteilungen für den Anwender abgelegt.

Bei Verlängerung von Zertifikaten erfolgt eine Neu-Zertifizierung, wobei sich der Anwender mit seinem alten Zertifikat am ElsterOnline-Portal authentisiert.

Das Sperren eines Accounts ist möglich: Der Anwender kann dies online unter Verwendung der Sicherheitsabfrage durchführen oder indem der Anwender das für ihn zuständige Finanzamt kontaktiert und dies vornehmen lässt. Aus Archivierungsgründen erfolgt lediglich ein Sperren, kein Löschen des Accounts.[7]

Bei der Verwendung von ELSTER-Plus erfolgt zusätzlich die Validierung des zugehörigen Zertifikats über OCSP (Online Certificate Status Protocol) und CRL (Certificate Revocation List).

8. Version des Anforderungskatalogs, die der Prüfung zugrunde gelegt wurde

Version 1.2 vom 29.08.2005

9. Zusammenfassung der Prüfergebnisse

9.1 Zulässigkeit

Für die Auditierung des Produkts ElsterOnline waren zunächst die Bestimmungen des Steuerrechts, insbesondere der Abgabenordnung (AO), der „Verordnung zur elektronischen Übermittlung von Steuererklärungen und sonstigen für das Besteuerungsverfahren erforderlichen Daten" (StDÜV), der „Verordnung über den automatisierten Abruf von Steuerdaten“ (StDAV) sowie der Ministerialerlasse und Richtlinien zu berücksichtigen[8]. Ferner findet hinsichtlich der Einbindung der Webportal www.elsteronline.de und www.elster.de das Telemediengesetz (TMG) Anwendung. Neben den Landesdatenschutzgesetzen kommen außerdem ergänzend die Bestimmungen des Bundesdatenschutzgesetzes (BDSG) zur Anwendung, soweit das Produkt ElsterOnline auch von Bundesbehörden (z.B. Zollverwaltung) genutzt wird.

Es wurde geprüft und festgestellt, dass die Datenverarbeitung sowohl im Registrier- als auch im Nutzungsvorgang für die Primär- und Sekundärdaten den einschlägigen datenschutz-rechtlichen Anforderungen genügt und damit zulässig ist.

Die Auditoren sprechen die Auflage aus, einen eindeutigen Bezug zwischen dem Verwaltungsabkommen KONSENS und den in anderen Dokumenten fixierten oder zertifizierten technisch-organisatorischen Maßnahmen zum Datenschutz bei den Clearingstellen herzustellen oder den derzeit zwischen den Parteien erörterten Entwurf einer schriftlichen Regelung zu § 11 BDSG bzw. § 17 LDSG-S-H zu finalisieren.

Ein Hinweis zu qualifizierten elektronischen Signaturen: Grundsätzlich sind qualifizierte elektronische Signaturen nach Signaturgesetz ein Äquivalent zur händischen Unterschrift, so dass ein Anwender grundsätzlich sein Formular mit einer qualifizier-

[7] Derzeit ist der Löschzeitpunkt für den Account in Abstimmung mit den Bundesländern auf 10 Jahre nach Ablauf des Zertifikates festgelegt. Grundlage hierfür ist § 169 AO zur Festsetzungsfrist und § 171 AO zur Ablaufhemmung. Ein für den Benutzer verfügbarer Hinweis findet sich auf:
https://www.elsteronline.de/hilfe/eop/public/security/help_datasecurity.html#c103.

[8] Die generelle Automation in der Steuerverwaltung ist durch einen Erlass des Bundesministeriums der Finanzen vom 15.01.2007 reglementiert, abrufbar unter https://www.elster.de/download/bmf_schreiben_zur_stduev_15012007.pdf.

ten elektronischen Signatur versehen könnte und damit das Formular rechtsverbindlich unterschreiben würde. Dieser Weg ist bei diesem ELSTER-Verfahren gegenwärtig explizit ausgeschlossen und auch optional nicht möglich; selbst bei Verwendung von ELSTER-Plus wird das Authentisierungszertifikat und nicht das qualifizierte Zertifikat verwendet. § 87a Abs. 6 Abgabenordnung (AO) sieht vor, dass neben der „qualifizierten elektronischen Signatur" im Sinne des Signaturgesetzes bis zum 31. Dezember 2011 auch ein „*anderes sicheres Verfahren*" zugelassen werden kann. ElsterOnline realisiert dieses *andere sichere Verfahren*, welches gemäß Gesetz ausdrücklich eine Alternative zur qualifizierten elektronischen Signatur vorsieht.

9.2 Umsetzung der Betroffenenrechte

Das Auskunfts-, Berichtigungs- oder Löschrecht des Bürgers in Bezug auf seine über ElsterOnline verarbeiteten personenbezogenen Daten bleiben gegenüber der zuständigen Finanzbehörde im vollen Umfang bestehen; sie liegen in der Verantwortung dieser öffentlichen Stellen und damit außerhalb des ELSTER-Verfahrens.

Allerdings unterstützt ElsterOnline die Umsetzung der Betroffenenrechte, indem sich Personen bei allen Fragen zu ELSTER an das eigens eingerichtete Callcenter per E-Mail, Telefon oder Fax wenden können (vgl. https://www.elster.de/hotline.php). Über das Callcenter-Ticketing werden die Beschwerden dann dem jeweiligen betroffenen Bereich zur Bearbeitung zugewiesen.

Ferner ist das Verfahren ElsterOnline in einem datenschutzrechtlichen Verfahrensverzeichnis berücksichtigt, welches beim behördlichen Datenschutzbeauftragten des Bayerischen Landesamtes für Steuern geführt wird und für jeden Bürger einsehbar ist.

Weiterhin unterstützt ElsterOnline Anfragen von Steuerbürgern über den Frage- und Antwort-Avatar „Elias" und unterhält ein Anwender- und Entwicklerforum. Die Betroffenenrechte können insofern umfassend geltend gemacht werden.

9.3 Eingesetzte kryptographische Verfahren

Kryptographische Algorithmen „altern" in dem Sinne, dass sie im Laufe der Zeit schwächer werden. Aus diesem Grund werden von verschiedenen Stellen regelmäßig Listen von sicheren kryptographischen Algorithmen und Parametern veröffentlicht, etwa vom Bundesamt für Sicherheit in der Informationstechnik oder der Bundesnetzagentur. Im Bereich der Signaturen hat man die Probleme, die sich daraus ergeben, im Griff. Zu beachten ist jedoch, dass sich Daten, die mit kryptographischen Algorithmen und Parametern verschlüsselt sind, welche dem Stand der Technik entsprechen, in einigen Jahren ganz praktisch entschlüsseln lassen.

Dieses Problem ist jedoch unabhängig von der eingesetzten Verschlüsselung gegeben und betrifft grundsätzliche alle entsprechenden Anwendungen. Weiterhin ist zu berücksichtigen, dass auch alternative, nicht elektronische Übertragungswege keinen vollständigen, ewig gültigen Schutz gegen Offenbarung der Daten bieten. Daher ist bei Nutzung gegenwärtig aktueller Verschlüsselungsverfahren mindestens von einer vergleichbaren Sicherung der Vertraulichkeit der Daten bei Nutzung von ElsterOnline gegenüber anderen Kommunikationsmöglichkeiten mit den Steuerbehörden auszugehen.

Aktuell werden für die SSL-Absicherung, die Kryptoboxen und die drei Varianten ELSTER-Basis, ELSTER-Spezial und ELSTER-Plus verschiedene kryptographische Verfahren eingesetzt, die aktuell als hinreichend sicher erachtet werden. **Gleichwohl sprechen die Auditoren die Auflage aus, den jährlich erscheinenden Algorithmenkatalog sowie die Veröffentlichung von diesbezüglichen Informationen – etwa vom Bundesamt für Sicherheit in der Informationstechnik – gründlich zu beobachten und bei Bedarf sofort zu reagieren.**

9.4 Dokumentation

Für ElsterOnline liegt eine aussagefähige Produktdokumentation vor, die auch für den Anwender über das Internet-Angebot einsehbar ist.

9.5 Kommunikationssicherheit

Die Sicherheitsziele zur sicheren Datenübertragung umfassen die Registrierung, die Anmeldung, die Datenübermittlung und die Datenabholung.

Über verschiedene Mechanismen wird sichergestellt, dass die Authentizität der Nutzer hinreichend sichergestellt wird:

- zweigeteilter Registrierungsprozess – ein Teil wird via E-Mail zugestellt, der andere Teil über den Postweg abgesichert –;
- Verwendung von SSL-Verbindungen;
- die dabei verwendete Länge und Güte der Aktivierungs-ID und Aktivierungscodes werden als ausreichend erachtet;
- hinreichend sichere kryptographische Verfahren;
- Zugriffsschutz auf die privaten Schlüssel ist abhängig von den drei Varianten ELSTER-Basis, ELSTER-Spezial und ELSTER-Plus:
  - Bei ELSTER-Basis ist der Schlüssel softwarebasiert abgelegt und der Zugriff per Passwort geschützt.

    Das grundsätzliche Sicherheitsproblem liegt hier beim Benutzer: Er hat dafür Sorge zu tragen, dass sein PC „sauber“ ist, worauf der Anwender in der Dokumentation der Anwendung entsprechend hingewiesen wird (vgl. https://www.elsteronline.de/eportal/Sicherheit.tax).
- Bei ELSTER-Spezial gelten im Prinzip ähnliche Einschätzungen wie bei ELSTER-Basis, allerdings mit dem Unterschied, dass die Schlüssel nicht auf der Festplatte, sondern auf einem Smart Card Chip gelagert werden, welcher sich auf einem USB-Token befindet.
  - Die Güte des Sticks – das auf dem ELSTER-Stick laufende Betriebssystem STARCOS SPK 2.3 mit der digitalen Signaturanwendung StarCert V. 2.2 ist nach "ITSEC E4 hoch" zertifiziert – ist aus Sicht der Gutachter adäquat geprüft.
  - Die Güte des Nachfolgemodells „Sicherheitssticks“ StarSign USB Token mit dem Betriebsystem ‘native’ STARCOS® auf Basis von Java Card™ 2.2.1 ist nach FIPS 140-2 Level 3 und Common Criteria EAL 4+ als SSCD (Secure

Signature Creation Device) zertifiziert und ist aus Sicht der Gutachter adäquat geprüft.

--- Bei ELSTER-Plus ist bei der hier verwendeten Signaturkarte – insbesondere bei sicheren Signaturerstellungseinheiten gem. SigG/SigV – davon auszugehen, dass sie gegen hohes Angriffspotential geschützt sind, so dass es nicht möglich ist, auf die Schlüssel zuzugreifen.

--- Signaturerstellungseinheiten müssen gemäß Elster-Policy geprüft sein, so dass zugelassene Signaturerstellungseinheiten aus Sicht der Gutachter adäquat geprüft sind.

Die Auditoren haben auch geprüft, inwiefern die verwendeten Authentisierungsmechanismen geeignet sind – insb. im Hinblick auf die Ausführungen des E-Government-Handbuch des BSI:

--- Grundsätzlich ist in diesem Kontext die Registrierung von der Authentisierung zu trennen: Die Güte der Registrierung wurde in den obigen Punkten thematisiert, während die Authentisierung mit kryptographischen Verfahren und Zertifikaten als angemessen – auch in Bezug auf das E-Government-Handbuch des BSI – angesehen wird.

--- ELSTER nutzt E-Mail und Postversand, wodurch die Auditoren zu dem Ergebnis „Mittel“ für die Übergabe der Authentisierungs-Daten kommen, da beide Authentifizierungs-Datenteile zusammen benötigt werden. Die Identifizierung hängt damit am Aktivierungscode (Brief) und der Aktivierungs-ID (E-Mail).

Nach der Registrierung, wenn der Anwender ein Authentisierungszertifikat dem ElsterOnline-Portal bekannt gegeben hat, erfolgt eine gegenseitige Authentisierung, so dass ElsterOnline sicherstellt, auch mit dem korrekten Anwender zu kommunizieren und der Anwender sicherstellen kann, auch mit dem authentischen ElsterOnline-Portal zu kommunizieren.

Über die SSL-Verbindung wird eine vertrauliche, authentische und integere Verbindung gewährleistet. Zudem ist ein auf Public-Key-Kryptographie basierender Authentisierungsmechanismus sicher.

Die Datenübermittlung vom Anwender zu ElsterOnline ist per SSL oder über eine Transportverschlüsselung auf Grundlage der ausgetauschten Authentisierungszertifikate abgesichert.

Die Datenabholung – also das Abholen von Bescheiddaten – aus der Bescheiddatenbank in der Clearingstelle ist für alle Varianten (ELSTER-Basis, ELSTER-Spezial, ELSTER-Plus) wie folgt abgesichert:

Die Länderkopfstellen verschlüsseln die Daten mit dem Verschlüsselungszertifikat des Benutzers. Der zugehörige private Schlüssel ist im jeweiligen PSE des Anwenders gelagert, so dass sichergestellt ist, dass nur der Anwender diese Daten entschlüsseln kann.

ELSTER-Plus bietet darüber hinaus die Steuerkontoabfrage:

--- Für die Steuerkontoabfrage über das ElsterOnline-Portal gilt: die Kontodaten werden jeweils mit dem Verschlüsselungszertifikat der SSEE des Anwenders verschlüsselt und für den Abruf in das jeweilige Postfach des Anwenders bereitgestellt. Damit kann ein Anwender mit seiner SSEE die verschlüsselten Kontodaten entschlüsseln.

--- Für die Steuerkontoabfrage über die Clearingstelle gilt: Die Kontodaten werden online durch ein hybrides Verfahren mit einem generierten Session-Key in der Clearingstelle verschlüsselt. Damit kann ein Anwender die verschlüsselten Kontodaten entschlüsseln.

Wie zuvor erläutert, werden explizit keine qualifizierten elektronischen Signaturen verwendet, die eine Zuordnung und Nichtabstreitbarkeit gewährleisten würden. Die Zuordnungsfähigkeit und Nichtabstreitbarkeit obliegt damit auf der vorgesehenen Authentisierungsmethodik der zwei-geteilten Authentisierung, wovon eine per Post versendet wird. Damit wird ein adäquates Sicherheitsniveau erreicht.

Gleichwohl ist die Nichtabstreitbarkeit – juristisch gesehen – nicht gesichert: Während bei qualifizierten elektronischen Signaturen der Anscheinsbeweis dafür spricht, dass der Signaturschlüssel-Inhaber die Signatur erzeugt hat, muss hier individuell bewiesen werden, dass eine übermittelte Information tatsächlich vom behaupteten Absender stammt. Bei der Datenabholung – also dem Abholen von Bescheiddaten – aus dem Postfach ist zu berücksichtigen, dass Daten, die von den Steuerbürgern von der Clearingstelle abgeholt werden, nicht signiert sind, da Bescheide und Steuerkontodaten für die Steuerkontoabfrage keine rechtsgültigen Bescheide darstellen. Steuerbescheide dürfen rechtsverbindlich ausschließlich von der Finanzverwaltung nur in Papierform zugestellt werden (Verwaltungsakt).

Die eingehenden Steuerdaten werden in der Clearingstelle einheitlich mit einem Zeitstempel versehen; Ursprung der Zeit ist das DCF77 Signal. Die empfangenen Zeitsysteme stehen in einem geschützten Serverraum und sind Bestandteil der ISO 27001-Zertifizierung.

9.6 Sicherheit der eingesetzten Server-Systeme

Vorbemerkung: Auf den Serversystemen von ElsterOnline werden keine Steuerdaten gespeichert; die Daten werden temporär bis zur Verarbeitung vorgehalten. Normalerweise sind die Systeme so ausgelegt, dass die abgegebenen Daten sofort verarbeitet werden können und sich kein Datenstau bildet.[9]

Die Serverkomponenten werden in den beiden Rechenzentren in München und Düsseldorf betrieben. Für sie liegt ein ISO 27001-Zertifikat auf der Basis von IT-Grundschutz vom Bundesamt für Sicherheit in der Informationstechnik (BSI) vor. Die Zertifikate sind gültig und der Geltungsbereich umfasst die hier zu betrachtenden Serverkomponenten. Es wurde geprüft und festgestellt, dass die hier relevanten Serverkomponenten – insb. hinsichtlich des Schutzbedarfs für die Primär- und Sekun-

[9] Grund können Verbindungsabbrüche bzw. Anwendungsausfälle auf den nachgelagerten Systemen sein, die zwischen 1 und 24 Stunden dauern können.

därdaten – adäquat berücksichtigt sind, so dass über die gültigen Zertifikate sichergestellt ist, dass hinreichende Sicherheitsmaßnahmen umgesetzt werden.

10. Zusammenfassung

Aus den Bewertungen der beiden Datenart-Anforderungsprofile ergibt sich folgende Gesamtbewertung im Überblick:

Nr.	Anforderungsprofil	Bewertung / Kommentar
Datenart A: (Primärdaten)		
A1	Produktbeschreibung	verständlich und aussagekräftig, in vollem Umfang sichergestellt
A2	Datensparsamkeit, Pseudonyme	in adäquater Weise sichergestellt
A3	Zulässigkeit der Datenverarbeitung	Zulässig
A4	Authentizität der Nutzer	in vollem Umfang sichergestellt
A5	Authentizität des Servers	in vollem Umfang sichergestellt
A6	Vertraulichkeit der übertragenen Daten	in vollem Umfang sichergestellt
A7	Vertraulichkeit der auf dem Server gespeicherten Daten	in vollem Umfang sichergestellt
A8	Integrität der übertragenen Daten	in vollem Umfang sichergestellt
A9	Integrität der auf dem Server gespeicherten Daten	in vollem Umfang sichergestellt
A10	Verfügbarkeit der Daten	in vollem Umfang sichergestellt
A11	Revisionsfähigkeit	in vollem Umfang sichergestellt
A12	Betroffenenrechte	in vollem Umfang sichergestellt
Datenart B: (Sekundärdaten)		
B1	Produktbeschreibung	verständlich und aussagefähig, in vollem Umfang sichergestellt
B2	Zulässigkeit der Verarbeitung	Zulässig
B3	Vertraulichkeit der Protokolldaten	in vollem Umfang sichergestellt
B4	Integrität der Protokolldaten	in vollem Umfang sichergestellt
B5	Verfügbarkeit der Protokolldaten	in vollem Umfang sichergestellt
B6	Betroffenenrechte	In vollem Umfang sichergestellt

11. Beschreibung, wie das IT-Produkt den Datenschutz fördert

Das Produkt ElsterOnline enthält folgende datenschutz fördernde Funktionen:

Datenerfassung und -übermittlung konzentrieren sich auf die rechtlichen Anforderungen zum Zweck des Besteuerungsverfahrens und schöpfen das Maß der Datenverarbeitung damit ganz im Sinne der Datensparsamkeit im geringstmöglichen Maße aus.

Durch die Zweiteilung des Registriervorgangs bzw. der Passwortvergabe wird ein hohes Maß an Sicherheit erreicht.

Durch die Zertifizierung der Clearingstellen gemäß ISO 27001 wird die Umsetzung von technisch-organisatorischen Sicherheitsmaßnahmen nach dem aktuellen Stand der Technik belegt.

Die für die Verfahrensvariante ELSTER-Plus zugelassene Verwendung von Signaturkarten schöpft das derzeit größtmögliche Maß an Sicherheit und Vertraulichkeit der Daten aus.

Das Produkt entspricht den Anforderungen, da die verwendeten Lösungen die Umsetzung der gesetzlichen Vorgaben ermöglichen. Dies gilt insbesondere für die verständliche und aussagekräftige Produktdokumentation, aber auch für die Umsetzung technisch-organisatorischer Datenschutzmaßnahmen, die als angemessen betrachtet werden.

Aufgrund der potentiellen Angreifbarkeit der derzeit zumindest teilweise noch eingesetzten RSA 1024 Bit Schlüssel sprechen die Auditoren die **Auflage** aus, den jährlich erscheinenden Algorithmenkatalog sowie die Veröffentlichung von diesbezüglichen Informationen – etwa vom Bundesamt für Sicherheit in der Informationstechnik – gründlich zu beobachten und bei Bedarf sofort zu reagieren. Unter Beachtung dieser Auflage kann das Verfahren ElsterOnline als „anderes *sicheres* Verfahren“ im Sinne des § 87a Abs. 6 AO bewertet werden.

Darüber hinaus sprechen die Auditoren die **Auflage** aus, den Bezug auf die Kontrollrechte des Auftraggebers (Finanzverwaltungen) und die vom Auftragnehmer (Clearingstellen) zu treffenden technisch-organisatorischen Sicherheitsmaßnahmen in den bisherigen Dokumenten bzw. im Verwaltungsabkommen oder einer anderweitigen Regelung im Sinne des § 17 LDSG-SH bzw. § 11 BDSG zu konkretisieren.