Bereitstellung einer Public-Key-Infrastruktur (PKI) für INSIKA-Systeme

Claudia Klug[1], Uta Roßberg[2]

[1]Bundesdruckerei GmbH, Oranienstraße 91, 10969 Berlin
[2]D-TRUST GmbH, Kommandantenstraße 15, 10969 Berlin
claudia.klug@bdr.de, u.rossberg@d-trust.net

Zur Absicherung von Kassen- und Taxameterdaten gegen unzulässige Veränderungen können Smartcards mit Zertifikaten aus einer vertrauenswürdigen Public-Key-Infrastruktur (PKI) eingesetzt werden (INSIKA-Smartcard).

Die D-TRUST GmbH, ein Tochterunternehmen der Bundesdruckerei GmbH, betreibt ein akkreditiertes Trustcenter und liefert seit 2001 unter Anderem sichere Signaturerstellungseinheiten für die Erzeugung von qualifizierten elektronischen Signaturen an Wirtschaftsunternehmen und Behörden. Diese werden z.B. zur Beantragung von Ursprungszeugnissen, für elektronische Ausschreibungen, das elektronische Abfallbegleitscheinverfahren, das elektronische Gerichtspostfach oder dem Emissionshandel eingesetzt.

Als akkreditierter Zertifizierungsdiensteanbieter (ZDA) verfügt D-TRUST über etablierte und geprüfte Prozesse zur Erstellung und Ausgabe von Signaturkarten sowie dem Betrieb der dazu erforderlichen PKI-Systeme und Dienstleistungen. Die INSIKA-Smartcards wurden als neues Kartenprodukt in die Standardprozesse der D-TRUST GmbH in Zusammenarbeit mit der Physikalisch-Technischen Bundesanstalt aufgenommen und können für die INSIKA-Systeme im Taxameter geliefert werden.

1 Firmendarstellung

1.1 Bundesdruckerei GmbH (BDr)

Die Bundesdruckerei GmbH in Berlin entwickelt und liefert Systemlösungen und Dienstleistungen für die sichere Identifikation in der analogen und digitalen Welt und zählt weltweit zu den führenden Unternehmen in diesem Bereich.

Neben kompletten Pass- und Ausweissystemen bietet das Unternehmen Personaldokumente, Hochsicherheitskarten, Dokumentenprüfgeräte, Sicherheitssoftware, Trustcenter-Leistungen und eID-Services für nationale und internationale Kunden im hoheitlichen sowie privatwirtschaftlichen Markt an. Darüber hinaus fertigt die Bundesdruckerei Banknoten, Postwertzeichen und Steuerzeichen sowie elektronische Publikationen.

Als ganzheitlicher Systemanbieter unterstützt die Bundesdruckerei ihre Kunden entlang der gesamten Prozesskette: von der Erfassung, Verwaltung und Weiterleitung biografischer und biometrischer Daten über die Herstellung und Personalisierung modernster ID-Dokumente bis hin zu Systemen zur Ausgabe und Verifikation dieser Dokumente. Außerdem entwickelt sie die technische Infrastruktur, damit Bürger, Behörden und Unternehmen die elektronischen Komponenten der Dokumente in der digitalen Welt nutzen können.

Mit ihren Tochtergesellschaften BIS Bundesdruckerei International Services GmbH, D-TRUST GmbH, Maurer Electronics GmbH und iNCO Sp.z o.o. beschäftigt die Bundesdruckerei-Gruppe rund 2.000 Mitarbeiter weltweit.

1.2 D-TRUST – das Trustcenter der Bundesdruckerei

Über ihr akkreditiertes Trustcenter D-TRUST bietet die Bundesdruckerei Unternehmen und Behörden umfassende Beratung rund um die elektronische Signatur sowie die kompletten Dienstleistungen eines Trust-

PTB-Bericht IT-18
doi:10.7795/210.20130206a

centers an. Die Zertifizierungsstelle wurde Ende 1998 mit Sitz in Berlin gegründet. Mit hochqualifizierten Mitarbeitern und spezialisierten Partnern entwickelt D-TRUST neue Lösungen der Hochsicherheitstechnologie im Umfeld der elektronischen Signatur.

Das Trustcenter wurde in der geschützten Umgebung des hochsicheren Wertdruckgebäudes der Bundesdruckerei eingerichtet. Umfangreiche Eingangskontrollen, Überwachungsanlagen und Zutrittsprozeduren schließen den Zugang Unbefugter aus.

Auch die Verfügbarkeit und der Schutz vor Betriebsunterbrechungen werden permanent gewährleistet. Sensible Personendaten sind vor nicht autorisiertem Zugriff zuverlässig geschützt. Als eines der wenigen Trustcenter in Deutschland hat die D-TRUST GmbH das renommierte Zertifikat „Trusted Site Infrastructure – Level 3“ vom TüvIT erhalten: Dies entspricht der Note „sehr gut“ für die freiwillige Überprüfung der Gebäudesicherheit.

2 Trustcenter Leistungen

2.1 Public-Key-Infrastrukturen (PKI)

Public-Key-Infrastrukturen arbeiten immer mit dem Zusammenspiel von privatem und öffentlichem Schlüssel, die das Trustcenter einem Nutzer zuordnet. Während der private Schlüssel geheim bleibt, tritt der Nutzer mit dem öffentlichen Schlüssel nach außen in Erscheinung. Der öffentliche Schlüssel wird dazu vom Trustcenter mit einem Zertifikat versehen, das Informationen über den Nutzer enthält und ihm eindeutig zugeordnet werden kann.

Damit der Nutzer die volle Kontrolle über die Verwendung seines privaten Schlüssels hat, werden die privaten Schlüssel auf Smartcards generiert und gespeichert und können nicht ausgelesen oder kopiert werden.

Da eine Karte verloren oder gestohlen werden kann oder gegebenenfalls nicht mehr gebraucht wird, stellt das Trustcenter die Möglichkeit zur Sperrung der Karte zur Verfügung.

Die Zertifikate aller gesperrten Karten werden in Sperrlisten (Certificate Revocation Lists = CRLs) geführt und veröffentlicht. Der Empfänger einer signierten Nachricht kann so überprüfen, ob die Signatur zum Zeitpunkt der Erstellung gültig war.

2.2 Eigenschaften und Funktionsweise der Elektronischen Signatur

Die elektronische Signatur sichert elektronische Daten vor Manipulation (Datenintegrität) und ermöglicht die Zuordnung der Daten zu einer Person oder Organisation (Authentizität der Daten).

2.3 Datenintegrität

Bei der Signaturerzeugung wird von den Daten, die signiert werden sollen, mittels Signatursoftware ein so genannter Hash-Wert (eindeutiger Fingerabdruck der Daten) gebildet. Dieser Hash-Wert wird mit dem privaten Schlüssel verschlüsselt. Der verschlüsselte Hash-Wert stellt die elektronische Signatur dar. Diese passt genau zu diesen Daten. Wird in den Daten nur ein Bit geändert, so ist die Signatur nicht mehr für diese Daten gültig.

Bei der Prüfung der Signatur wird die Signatur mit dem frei verfügbaren öffentlichen Schlüssel entschlüsselt und somit der Hash-Wert der ursprünglichen Daten ermittelt. Zeitgleich wird zu den vorliegenden Daten noch einmal der Hash-Wert gebildet. Stimmen beide Hash-Werte überein, dann ist gewährleistet, dass die Daten keinerlei Veränderung erfahren haben.

2.4 Authentizität der Daten

Da die Signatur den öffentlichen Schlüssel enthält, der durch das Zertifikat dem Besitzer zugeordnet ist, kann der Empfänger einer Signatur auch die Existenz des Erzeugers und den Zertifikatsstatus beim Trustcenter überprüfen, das das Zertifikat ausgestellt hat.

Das Trustcenter stellt über geeignete Prozesse sicher, dass ein öffentlicher Schlüssel eindeutig einer Person oder Organisation zugeordnet werden kann. Diese Zuordnung wird mit einem Zertifikat, das den öffentlichen Schlüssel und Informationen zum Besitzer des Schlüsselpaares enthält, öffentlich gemacht. Verliert ein Besitzer die Kontrolle über seinen privaten Schlüssel, dann kann bzw. muss er sein Zertifikat sperren lassen. Damit wird für alle Beteiligten klar, dass sein Zertifikat ab diesem Zeitpunkt nicht mehr gültig ist und er sich für nach dem Sperrzeitpunkt erzeugte Signaturen nicht rechtfertigen muss.

3 INSIKA-Smartcards für Taxameter

Im Folgenden wird am Beispiel INSIKA-Smartcards für Taxameter beschrieben, welche Komponenten zum Einsatz kommen und wie der Antrags- und Ausgabeprozess für INSIKA-Smartcards umgesetzt wird.

Die Lieferung der INSIKA-Smartcards für den Wirkbetrieb wird durch D-TRUST, das akkreditierte Trustcenter der Bundesdruckerei GmbH, übernommen.

Dazu wurde der Standardantragsprozess für fortgeschrittene Signaturkarten um die Freigabe der Antragsdaten durch die Taxiaufsichtsbehörde erweitert und die Kartenvorpersonalisierung um das Aufbringen des INSIKA spezifischen Teils (ECC- & TIM-Package) zur sicheren Datenspeicherung auf den Smartcards ergänzt. Die Erstellung und Lieferung der INSIKA-Smartcard wird als D-TRUST Standardprozess für Signaturkarten realisiert.

3.1 Betriebsystem und Kartenprofil

Als Smartcard kommt zurzeit das Produkt der Firma Siemens mit dem Betriebssystem „CardOS V4.3B“ – und dem Infineon Chip SLE66CX642P mit 64 kB EEPROM oder SLE66CX322P mit 32 kB EEPROM zum Einsatz.

Um die Unversehrtheit der Karte vor der ersten Nutzung sicherstellen zu können, erhält der Nutzer für jede Karte einen PIN-Brief mit einer sogenannten Transport-PIN. Mit der Transport-PIN wird die Karte einmalig aktiviert.

3.2 Kartenlayout

Abbildung 1 zeigt eine INSIKA-Smartcard mit dem aktuellen Layout. Im Rahmen der optischen Personalisierung werden die Umsatzsteuer-Identifikationsnummer, die laufende Kartennummer und die Gültigkeitsdauer auf den Kartenkörper aufgedruckt.

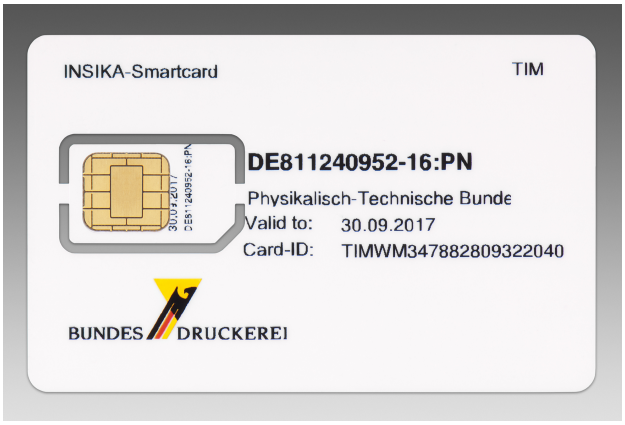

Abbildung 1: INSIKA-Smartcard

Der Kartenkörper wird im ID-1 Format ausgeliefert (Kreditkartenformat). Die Karte ist so perforiert, dass sie sich durch Herausbrechen in das ID-000 Format wandeln lässt. Dieses von SIM-Karten bekannte Format wird in den Sicherheitseinheiten für Taxameter verwendet.

4 PKI

Die D-TRUST GmbH liefert die personalisierten INSIKA-Smartcards mit einem X.509 Zertifikat aus einer bestehenden Class 2 CA Hierarchie (CA = Certification Authority).

4.1 CA-Hierarchie

Abbildung 2 zeigt die CA-Hierarchie. Die Class 2 CA unterliegt den Vorgaben der Zertifikatsrichtlinien der D-TRUST-Root PKI [1]. Class-2-Zertifikate sind hochwertig, aber nicht qualifizierte Zertifikate, die die Anforderungen von ETSI TS 102 042 erfüllen [2].

4.2 Namen

Die Zertifikate erhalten im Feld `DistinguishedName` die für die INSIKA-Anwendung erforderlichen Angaben zum Taxiunternehmen:

```
CN (CommonName) = <Umsatzsteuer-
   Identifikationsnummer> “-“ <laufende
   Nummer> “:PN“
O  (Organisation) = <Name des
   Taxiunternehmens>
C  (Country) = “DE“
```

Die Endung “`:PN`“ weißt darauf hin, dass es sich bei dem Namen um ein Pseudonym handelt. Im Trustcenter sind zu dem Pseudonym die persönlichen Daten des Karteninhabers hinterlegt und können bei einem berechtigten Anliegen offen gelegt werden.

4.3 Gültigkeit

Die Signaturzertifikate haben je nach Speicherplatz der Smartcards (32 oder 64 kB) eine Gültigkeitsdauer von zwei oder fünf Jahren. Die Prüfung der Zertifikatskette erfolgt nach dem Kettenmodell.

4.4 Veröffentlichung

Die Zertifikate werden bei der Erzeugung automatisch im LDAP-Verzeichnis unter `ldap://directory.d-trust.net` veröffentlicht. Dort werden auch die Sperrlisten (CRLs) veröffentlicht.

4.5 Sperrung

Die Zertifikate können vom Antragsteller telefonisch oder schriftlich gesperrt werden.

Bei der telefonischen Sperrung muss sich der Antragsteller mittels Sperrkennwort, das bei der Antragstellung vergeben wird, authentifizieren. Die Zertifikatssperrung erfolgt unmittelbar nach dem Anruf.

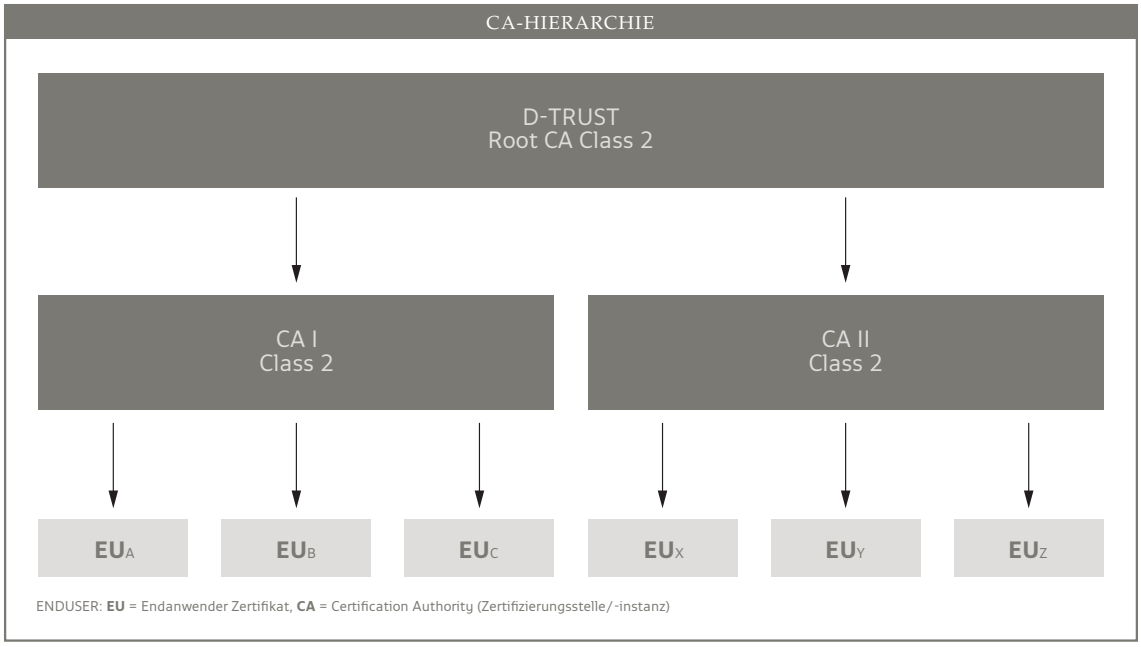

Abbildung 2: CA-Hierarchie (Quelle: Bundesdruckerei GmbH)

Bei der schriftlichen Sperrung sendet der Antragsteller einen persönlich unterschriebenen formlosen Antrag mit Namen, Umsatzsteuer-Identifikationsnummer und Antragsnummer an die D-TRUST GmbH. Die Sperrung erfolgt am ersten Werktag nach Posteingang des Sperrantrags.

5 Antragsprozess

Die Beantragung der INSIKA-Smartcard erfolgt über einen Weblink der D-TRUST GmbH. Der Taxiunternehmer füllt dazu online ein Antragsformular aus, das er am Ende ausdruckt und unterschreibt.

Im Rahmen der Beantragung werden die Personendaten, die Unternehmensdaten inklusive Umsatzsteuer-Identifikationsnummer und Rechnungsadresse abgefragt. Zudem werden die Daten der zuständigen Taxiaufsichtsbehörde zur Auswahl angezeigt.

Der Antragsteller wählt die zuständige Behörde aus und sendet den unterschriebenen Antrag an die Taxiaufsichtsbehörde.

5.1 Freigabe

Die Taxiaufsichtsbehörde prüft, ob der Antragsteller berechtigt ist und gibt den Antrag – im Fall der positiven Prüfung – frei. Anschließend sendet sie die freigegeben Antragsunterlagen an die D-TRUST GmbH.

5.2 Identifizierung

Die Identifizierung und Prüfung erfolgt auf mittlerer Stufe. Über eine Online-Abfrage wird geprüft, ob die Umsatzsteuer-Identifikationsnummer mit den Organisationsdaten übereinstimmt. Zudem wird geprüft, ob die Taxiaufsichtsbehörde den Antrag freigegeben hat.

5.3 Archivierung der Antragsunterlagen

Die Original-Antragsunterlagen werden nach der Prüfung gescannt und für die Zertifikatslaufzeit plus zehn Jahre archiviert. Die weitere Antragsbearbeitung erfolgt mit den elektronischen Daten.

5.4 Registrierung und Kartenpersonalisierung

Die Registrierung erfolgt mittels der geprüften Antragsdaten. Über die Pseudonymprüfung wird sichergestellt, dass der Name im CN eindeutig ist und nur einmal vergeben wird.

Im Rahmen der Vorpersonalisierung wurde bereits ein ECC-Schlüsselpaar auf der Karte erzeugt. Der öffentliche Schlüssel wird während der Registrierung ausgelesen und zusammen mit den Zertifikatsdaten an das zentrale Zertifikatsmanagement System der D-TRUST GmbH gesendet.

Das Zertifikat wird unmittelbar erzeugt und in die Karte eingebracht. Anschließend erfolgt die optische Personalisierung mit den antragsbezogenen Zertifikatsdaten.

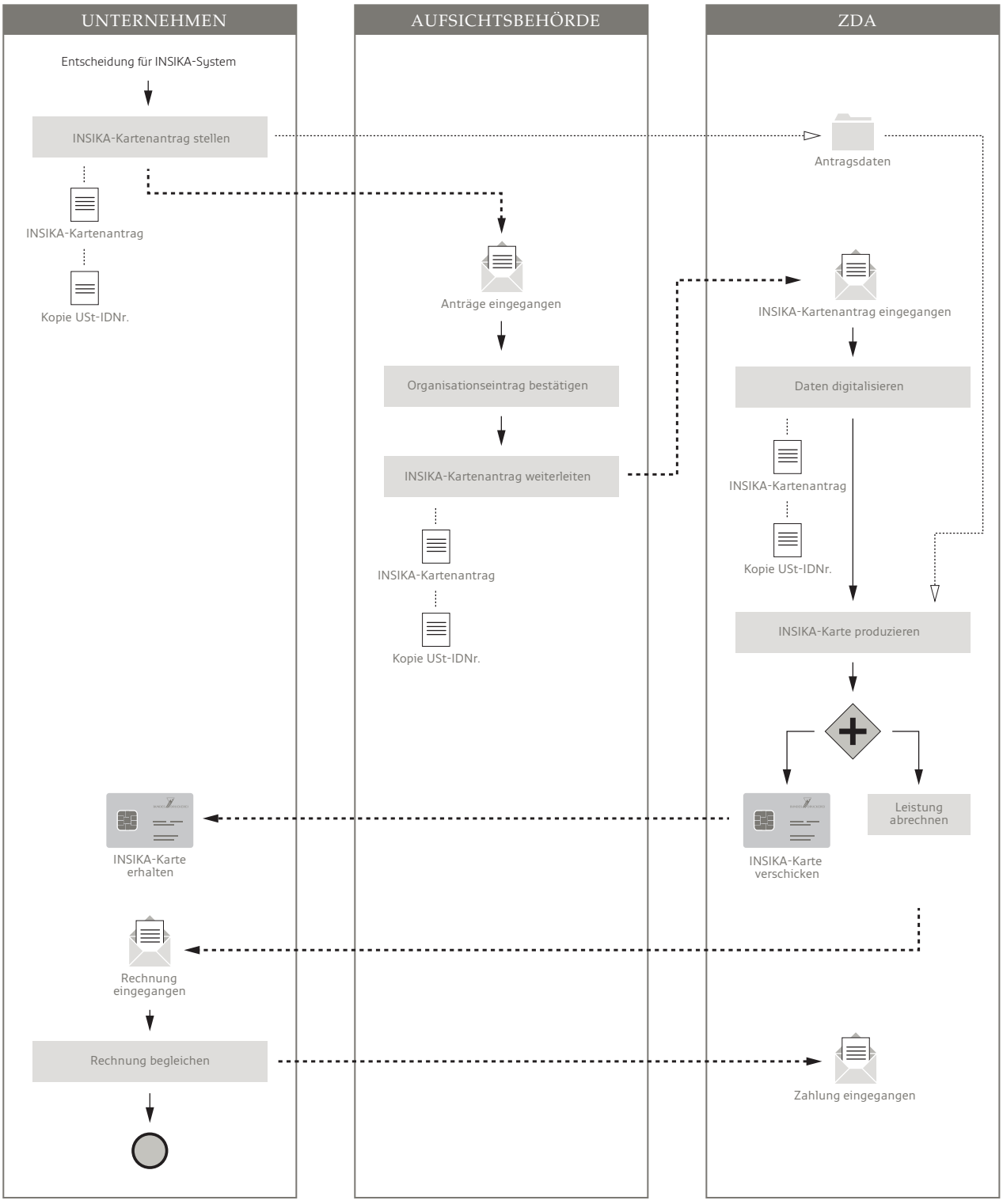

Abbildung 3: Antrags- und Ausgabeprozess INSIKA-Smartcard für Taxameter (Quelle: Bundesdruckerei GmbH)

5.5 Versand und Rechnungsstellung

Die INSIKA-Smartcards werden per Einschreiben an die Antragsteller versendet. Um Missbrauch der Karten zu vermeiden, wird der PIN-Brief zwei Tage nach Versand der Karte per Post an den Antragsteller gesendet. Die Rechnungsstellung erfolgt durch die Bundesdruckerei GmbH an den Antragsteller.

In der Abbildung 3 wird der komplette Prozess für die Ausgabe von INSIKA-Smartcard skizziert.

6 Ausblick

Die Ausgabe der INSIKA-Smartcards für Taxameter startete im 3. Quartal 2012. Eine Ausweitung der Lieferung von INSIKA-Smartcards, z. B. für Registrierkassen, kann problemlos analog umgesetzt werden.

In der ersten Phase sieht der oben beschriebene Antragsprozess und Freigabeprozess noch einen Papierantrag vor, dieser sollte mittelfristig auf einen rein elektronischen Prozess umgestellt werden.

Denkbar sind hierbei der Einsatz des neuen Personalausweises oder des elektronischen Aufenthaltstitels zur Beantragung der INSIKA-Smartcard durch den Unternehmer mittels eID-Funktion, sowie der Einsatz von qualifizierten Signaturkarten für den Freigabeprozess in der zuständigen Behörde.

Die Systeme für die elektronische Antragsprüfung, automatische Bearbeitung und elektronische Archivierung sind schon heute bei D-TRUST vorhanden.

Literatur

[1] D-TRUST GmbH. *Zertifikatsrichtlinie der D-TRUST-Root PKI*. Version 1.6. 13. Aug. 2012. URL: `https://www.d-trust.net/unternehmen/d-trust-cpcps/`.

[2] ETSI. *TS 102 042: Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates*. Version V2.1.2. European Telecommunications Standards Institute, Apr. 2010. URL: `http://www.etsi.org/`.