Digital signierte Wägeresultate

Neue Wege in der Sicherung eichfähiger Messwerte

U. Rauchschwalbe, Schenck Process GmbH,
Landwehrstrasse 55, D-64293 Darmstadt
A. Wiesmaier, C. Ludwig, J. Buchmann, TU-Darmstadt-CDC, Hochschulstrasse 10, D-64289 Darmstadt

1 Einleitung

In vielen Anwendungen werden heute Waagen im geschäftlichen Verkehr betrieben, d.h. das Ergebnis der Wägung ist Basis für eine mengenabhängige Berechnung von Waren oder Dienstleistungen. Der weite Bogen von Applikationen reicht dabei vom Verkauf von Wurst oder Gemüse im Einzelhandel, über die Abrechnung von Massengütern wie Kohle oder Erz bis hin zum Ermitteln von Transportkosten für Waren durch Speditionen oder Postbetriebe.

Waagen im geschäftlichen Verkehr unterliegen der Eichpflicht (z.B. dem deutschen Eichgesetz [3]). Sie benötigen eine Zulassung und unterliegen einer regelmäßigen Überwachung. Zu den Anforderungen der Eichgesetzgebung gehört neben der Zuverlässigkeit der Waage auch die Möglichkeit, dass sich der Kunde von der Richtigkeit der Wägung überzeugen kann. In den Fällen, in denen der Kunde der Wägung nicht direkt beiwohnt, führt dies in der Regel zu der Forderung einer eichfähigen Registrierung. Darunter versteht man, dass die Speicherung der Wägergebnisse durch ein Gerät ausgelöst und durchgeführt wird, das der Überwachung durch die Eichbehörde unterliegt.

Der Vorgang wird klar am Beispiel einer Kies lieferung auf eine Baustelle: Der Kies wird nach Gewicht abgerechnet, die Wägung erfolgt im Kieswerk, d.h. ohne Beisein des Warenempfängers. In der Regel erhält der Kunde einen Lieferschein, der von einem PC oder einem Warenwirtschaftssystem erzeugt wird - also von einem Gerät, das eben nicht der genannten Überwachung unterliegt. Als Konsequenz ergibt sich die Notwendigkeit einer Registrierung der erfassten Gewichte in der Waage selbst, und zwar in einer Weise, dass sich der Warenempfänger eindeutig von der Richtigkeit der Daten auf seinem Lieferschein überzeugen kann.

Klassisch wird diese Aufgabe gelöst durch die Installation eines Alibi-Druckers, der direkt an der Waage angeschlossen ist und der alle durchgeführten Wägungen abdruckt. Diese Lösung ist bei den Waagenbetreibern aber unbeliebt, denn die Geräte sind laut, müssen gewartet werden und kosten Platz und Geld. Die schon früher eingeführte Lösung des Alibi-Speichers legt die Wägeergebnisse für eine hinreichend lange Zeit in einem internen Speicher der Waage ab, z.B. einem EEPROM oder einer Speicherkarte. Gewöhnlich wird dabei eine Speicherdauer von 90 Tagen als hinreichend angesehen. Dadurch werden einige Probleme des Alibi-Druckers gelöst, aber auch neue produziert. Der Speicherplatz ist in den elektronischen Waagen in der Regel knapp, eine Aufrüstung des Waagenspeichers erhöht die Kosten. Bei vielen Geräten sind Anzeige und Tastatur so klein, dass das Auslesen der Werte kaum praktikabel ist.

In einem nächsten Schritt wurde der Alibi-Speicher in die angeschlossenen Rechnersysteme verlagert. Auch hier ist die Beseitigung bestehender Probleme mit dem Auftauchen neuer Schwierigkeiten verbunden. Die betroffenen Softwareteile auf dem Rechnersystem müssen ebenfalls zugelassen und unter behördliche Kontrolle gestellt werden. Die Anforderungen an eichfähige Software in ansonsten offenen Systemen sind mittlerweile vereinheitlicht und bekannt [9]. Die Absicherung der Software ist relativ aufwändig. Die Lösung ist an ein bestimmtes PC-Betriebssystem gebunden - in der Regel Windows.

Allen beschriebenen Verfahren gemeinsam ist das Handicap, dass der Kunde die Überprüfung seiner Daten nur am Ort der Waage vornehmen kann. Dieser Nachteil dürfte heute der Hauptgrund dafür sein, dass die Möglichkeit zur Überprüfung nur selten wahrgenommen wird. Eine Versendung der Daten zerstört den Kontext der eichfähigen Registrierung, was angesichts zunehmend globaler Handelsbeziehungen einen echten Nachteil darstellt. Diese Situation war Anlass, ein Verfahren zu entwickeln, das plattformunabhängig ist, kaum Betriebskosten verursacht und eine Verifikation der Daten auch am Standort des Warenempfängers erlaubt.

2 Ansatz

Grundidee ist, die Daten nicht in einem physikalischen Speicher abzulegen und dort für eine evtl. spätere Inspektion vorzuhalten, sondern vielmehr die Wiegedatensätze durch digitale Unterschriften zu intrinsisch eichfähigen Objekten zu machen, die keine Registrierung in einem zugelassenen Medium benötigen. Die signierten Datensätze können nach der Erzeugung in der Waage in beliebigen Medien gespeichert oder transportiert werden, die nicht der Eichpflicht unterliegen müssen. Die Überprüfung des Datensatzes auf Korrektheit kann prinzipiell an jedem beliebigen Ort erfolgen.

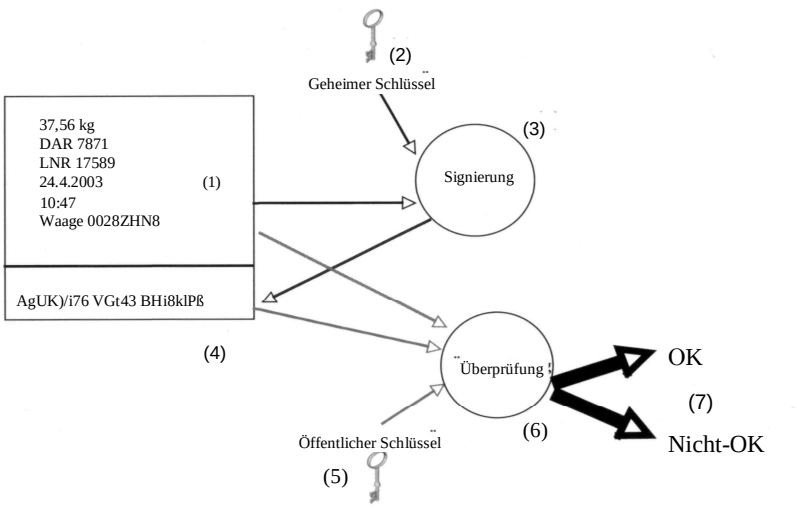


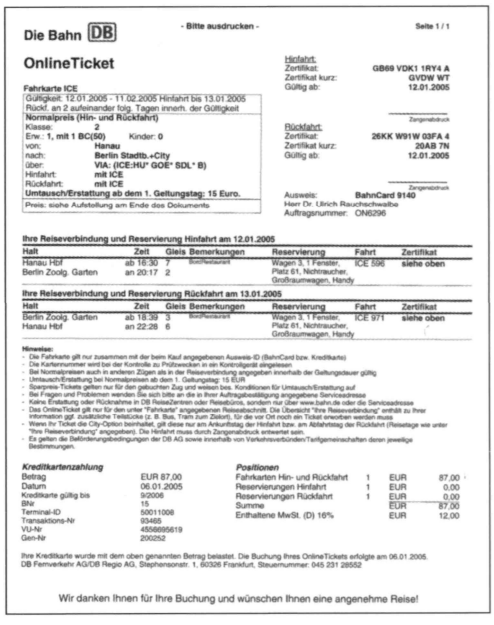
Abb. 1: Verfahren der digitalen Signatur

Ein digitales Signaturverfahren ist eine kryptographische Methode, mit welcher der Inhaber eines geheimen Signaturschlüssels unabstreitbar die Echtheit eines digitalen Dokumentes bestätigt. Zu jedem Signaturschlüssel gehört ein öffentlicher Verifikationsschlüssel, mit dem jeder überprüfen kann, ob eine Signatur tatsächlich aus einem vorgelegten Dokument und mit dem entsprechenden Signaturschlüssel berechnet wurde. Wurde das Dokument nach der Signaturerstellung in irgendeiner Weise verändert, so wird die Signatur bei dieser Prüfung als ungültig erkannt. Durch eine sogenannte Public Key Infrastructure kann der Verifikationsschlüssel nachvollziehbar mit der Identität einer natürlichen Person, mit der IP-Adresse eines Servers oder - in dem hier betrachteten Fall - mit einer Waage verbunden werden. Wenn die Verifikation eines Dokuments erfolgreich verläuft, so kann der Verifizierer sicher sein, dass das Dokument in dieser Form von der Person, von dem Webserver oder eben der Waage unterzeichnet wurde.

Abb.l verdeutlicht den prinzipiellen Ablauf. Der Wägedatensatz (1) wird in der Signierinstanz (3) bearbeitet. Dazu wird er mit dem geheimen Schlüssel (2) verrechnet, der nur der Waage bekannt ist. Ergebnis ist die digitale Signatur (4), die an den Klartext-Datensatz angehängt wird. Das Verfahren ist nicht umkehrbar, d.h. aus Datensatz und Signatur kann der Schlüssel nicht rekonstruiert werden, und damit kann auch kein verfälschter Datensatz mit einer gültigen Signatur ergänzt werden.

Mit Hilfe des öffentlichen Schlüssels, der - wie der Name sagt - jedermann frei zur Verfügung steht, kann ein Überprüfungsprogramm (6) eine Bewertung des Datensatzes durchführen. Jede Veränderung, insbesondere des Gewichtswerts, ist auf diese Weise unzweifelhaft zu detektieren. Da das Signierverfahren und seine Parameter ebenfalls öffentlich sind, kann die Überprüfung sogar ohne Hilfestellung von Waagenhersteller, Betreiber oder Zulassungsbehörde durchgeführt werden.

Digitale Signaturverfahren sind nicht zu verwechseln mit Verschlüsselungsverfahren, bei denen die Daten in unleserlicher Form (und damit für einen Angreifer unbenutzbar) übertragen und am Zielort entschlüsselt werden. In der kryptographischen Fachliteratur sind zahlreiche Signaturverfahren beschrieben, z. B., DSA, ECDSA [13], die nach aktuellem Stand der Forschung als sicher gelten.


Die Bahn DB - Bitte ausdrucken - Seite 1 / 1

OnlineTicket

Fahrkarte ICE
Gültigkeit: 12.01.2005 - 11.02.2005 Hinfahrt bis 13.01.2005
Rückf. an 2 aufeinander folg. Tagen innerh. der Gültigkeit
Normalpreis (Hin- und Rückfahrt)
Klasse: 2
Erw.: 1, mit 1 BC(50) Kinder: 0
von: Hanau
nach: Berlin Stadtb.+City
über: VIA: (ICE:HU* GOE* SDL* B)
Hinfahrt: mit ICE
Rückfahrt: mit ICE
Umtausch/Erstattung ab dem 1. Geltungstag: 15 Euro.
Preis: siehe Aufstellung am Ende des Dokuments

Hinfahrt:
Zertifikat: GB69 VDK1 1RY4 A
Zertifikat kurz: GVD9/ WT
Gültig ab: 12.01.2005
Zangenabdruck

Rückfahrt:
Zertifikat: 26KK W91W 03FA 4
Zertifikat kurz: 20AB 7N
Gültig ab: 12.01.2005
Zangenabdruck

Ausweis: BahnCard 9140
Herr Dr. Ulrich Rauchschwalbe
Auftragsnummer: ON6296

Ihre Reiseverbindung und Reservierung Hinfahrt am 12.01.2005

Halt	Zeit	Gleis	Bemerkungen	Reservierung	Fahrt	Zertifikat
Hanau Hbf	ab 16:30	7	Bordrestaurant	Wagen 3, 1 Fenster, Platz 61, Nichtraucher, Großraumwagen, Handy	ICE 596	siehe oben
Berlin Zoolg. Garten	an 20:17	2				

Ihre Reiseverbindung und Reservierung Rückfahrt am 13.01.2005

Halt	Zeit	Gleis	Bemerkungen	Reservierung	Fahrt	Zertifikat
Berlin Zoolg. Garten	ab 18:39	3	Bordrestaurant	Wagen 3, 1 Fenster, Platz 61, Nichtraucher, Großraumwagen, Handy	ICE 971	siehe oben
Hanau Hbf	an 22:28	6				

Hinweise:
- Die Fahrkarte gilt nur zusammen mit der beim Kauf angegebenen Ausweis-ID (BahnCard bzw. Kreditkarte)
- Die Kartennummer wird bei der Kontrolle zu Prüfzwecken in ein Kontrollgerät eingelesen
- Bei Normalpreisen auch in anderen Zügen als in der Reiseverbindung angegeben innerhalb der Geltungsdauer gültig
- Umtausch/Erstattung bei Normalpreisen ab dem 1. Geltungstag: 15 EUR
- Sparpreis-Tickets gelten nur für den gebuchten Zug und weisen bes. Konditionen für Umtausch/Erstattung auf
- Bei Fragen und Problemen wenden Sie sich bitte an die in Ihrer Auftragsbestätigung angegebene Serviceadresse
- Keine Erstattung oder Rücknahme in DB ReiseZentren oder Reisebüros, sondern nur über www.bahn.de oder die Serviceadresse
- Das OnlineTicket gilt nur für den unter "Fahrkarte" angegebenen Reiseabschnitt. Die Übersicht "Ihre Reiseverbindung" enthält zu Ihrer Information ggf. zusätzliche Textzeile (z. B. Bus, Train zum Zielort), für die vor Ort noch ein Ticket erworben werden muss
- Wenn Ihr Ticket die City-Option beinhaltet, gilt diese nur am Ankunftstag der Hinfahrt bzw. am Abfahrtstag der Rückfahrt (Reisetage wie unter "Ihre Reiseverbindung" angegeben). Die Hinfahrt muss durch Zangenabdruck entwertet sein.
- Es gelten die Beförderungsbedingungen der DB AG sowie innerhalb von Verkehrsverbünden/Tarifgemeinschaften deren jeweilige Bestimmungen.

Kreditkartenzahlung

Betrag	EUR 87,00
Datum	06.01.2005
Kreditkarte gültig bis	9/2006
BNr	15
Terminal-ID	50011008
Transaktions-Nr	93465
VU-Nr	4558695619
Gen-Nr	200252

Positionen

Fahrkarten Hin- und Rückfahrt	1	EUR	87,00
Reservierungen Hinfahrt	1	EUR	0,00
Reservierungen Rückfahrt	1	EUR	0,00
Summe		EUR	87,00
Enthaltene MwSt. (D) 16%		EUR	12,00

Ihre Kreditkarte wurde mit dem oben genannten Betrag belastet. Die Buchung Ihres OnlineTickets erfolgte am 06.01.2005.
DB Fernverkehr AG/DB Regio AG, Stephansonstr. 1, 60326 Frankfurt, Steuernummer: 045 231 28552

Wir danken Ihnen für Ihre Buchung und wünschen Ihnen eine angenehme Reise!

Abb. 2: Digital signierte Bahnfahrkarte (Zertifikat = Signatur)

Im Alltag begegnen uns digitale Signaturen bereits an vielen Stellen, z.B. bei online Bahnticktes (Abb. 2), bei online gebuchten und ausgedruckten Konzertkarten oder bei vom heimischen PC aus durchgeführten Bank-

3 Randbedingungen

geschäften. Neu war jedoch die Umsetzung auf Waagen, speziell unter dem Aspekt der notwendigen Bauartzulassung.

Für das Projekt gab es einige günstige Voraussetzungen. Moderne, effiziente Verfahren zur digitalen Signierung sind bekannt, frei verfügbar, und insbesondere frei von Lizenzgebühren. Die Direktive 1999/93/EC [4] der Europäischen Union, umgesetzt in Deutschland durch das Signaturgesetz [12], schafft eine internationale rechtliche Basis für den Einsatz solcher Verfahren. Mit dem Institut für Kryptographie und Computeralgebra an der TU-Darmstadt und der Firma FlexSecure waren Projektpartner verfügbar, die über umfassendes Wissen und breite Erfahrung in diesem Feld verfügen. Schenck Process hat als Ergänzung dazu die Erfahrungen im Bereich der Wägetechnik, des Eichrechts und der Zulassungsverfahren eingebracht. Die Physikalisch Technische Bundesanstalt (PTB), hat im Projekt SELMA [10] selbst Erfahrungen mit ähnlicher Technologie gesammelt - in diesem Projekt ging es um die Anwendung in Gas- und Wasserzählern.

Andere - eher technisch gelagerte - Randbedingungen waren weniger günstig für das Projekt: Typische elektronische Wägeindikatoren basieren auf Controllern, deren Leistungsfähigkeit um Größenordnungen geringer sind, als die von heute handelsüblichen PC's. Dies betrifft sowohl die Verarbeitungsleistung als auch den Speicherplatz. Es gibt zwar für die benötigten Algorithmen spezialisierte, preiswerte Krypto-Chips (z.B. aus Geldkarten bekannt), eine Änderung der Waagenhardware sollte aber auf jeden Fall vermieden werden. Trotz diesen Voraussetzungen sollte ein Signaturvorgang keinesfalls mehr als einige wenige Sekunden in Anspruch nehmen, damit die Waagenanwendung dadurch nicht gestört wird. Mit dem Konzept, eichfähige Daten durch digitale Signaturen zu sichern, wird zulassungstechnisches Neuland betreten. Keine Regelungen - national oder international - existieren zu diesem Thema. Deshalb war es nicht verwunderlich, dass eine Reihe von technischen Bedenken durch die Zulassungsbehörde (PTB) und durch die Eichbehörden geäußert wurden. Die Punkte mussten intensiv diskutiert und gemeinsam gangbare Wege gefunden werden.

4 Signatur

Um initialisiert zu werden, wird die Waage beim Hersteller an einen Rechner angeschlossen, der ausschließlich für die Trustcenter-Software (FlexiTRUST [2]) reserviert ist. Hier erhält die Waage das Kommando zur Generierung des Schlüsselpaars. Wie in Abb. 3 zu sehen ist, antwortet die Waage mit ihrem (eben erzeugten) öffentlichen Schlüssel. Dieser wird zusammen mit Zusatzdaten (Datum, Uhrzeit, Seriennummer der Waage) im X.509-Format [5] zertifiziert und in einem öffentlich zugänglichen LDAP-Verzeichnis [1] publiziert.

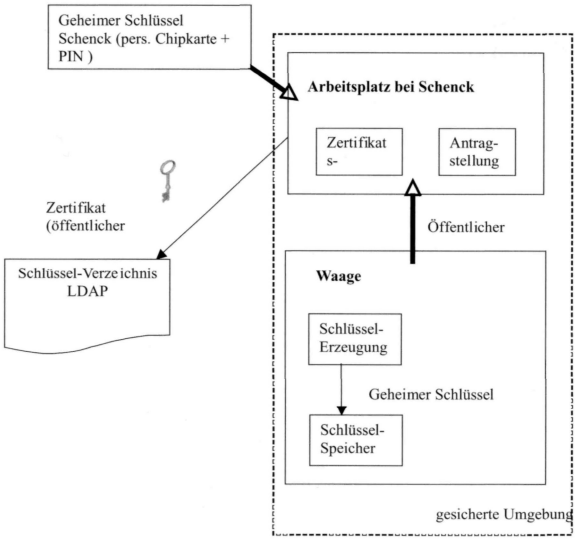


Abb. 3: Schlüsselerzeugung und Zertifizierung

Eine Wägung - und damit die Generierung eines signierten Datensatzes - kann auf unterschiedliche Weisen ausgelöst werden:

- Durch Tastendruck am Gerät
- Durch ein externes Signal, etwa das Überfahren einer Induktionsschleife
- Durch ein EDV-Kommando (seriell oder Feldbus)

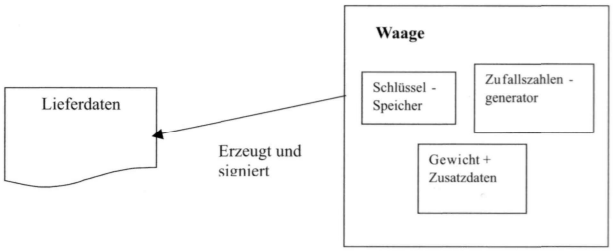
Die eigentliche Signaturberechnung (dargestellt in Abb. 4) nach der Wägung dauert ca. 1 Sekunde und ist damit für den Bediener nicht als Verzögerung wahrnehmbar. Ergebnis der Berechnung ist die digitale Signatur, im konkreten Fall zwei je 160 Bit lange Strings. Diese werden der besseren Lesbarkeit wegen als zwei jeweils 40-stellige ASCII-codierte Hexadezimalzahlen dargestellt (1 Zeichen je 4Bit). Die Signatur wird zusammen mit den vollständigen Wiegedaten ausgegeben. Neben der eventuellen Klartextausgabe der Wiegedaten für den Warenempfänger werden die Daten direkt in einer komprimierten Version ausgegeben, um bei einem späteren Kopieren der Daten in ein Verifikationsprogramm Fehler z.B. durch hinzugefügte Zeilenumbrüche oder Leerzeichen zu vermeiden. Im Hintergrund werden zugleich Vorberechnung für weitere Signaturen ausgeführt. Nach 5-10 Sekunden (je nach Systemlast) ist das System bereit für den nächsten Wägevorgang.

Es ist zu jeder Zeit möglich, redundante Informationen (z.B. zur Fehlerkorrektur) hinzuzufügen, oder die Daten umzukodieren. Die einzige Bedingung ist, dass die Originaldaten aus dem modifizierten Datensatz rekonstruiert werden können, damit die Signatur weiterhin verifiziert werden kann. Denn nur anhand des vollständigen Datensatzes, der neben dem Gewicht noch

- Datum / Uhrzeit
- Seriennummer der Waage
- Laufende Nummer der Wägung
- Status
- Begleitenden Text (z.B. Kennzeichen)

und die Signatur enthält, kann später dessen Integrität überprüft werden. Das folgende Beispiel zeigt einen

Abb. 4: Bildung der Signatur



Datensatz inkl. komprimierter Ausgabe und Signatur.

Seriennummer Waage:	0022E6HV
Waagennummer:	1
Bruttogewicht:	11,72t
Taragewicht:	0,00t
Status:	0E80
Datum:	2005-01-18
Uhrzeit:	10:06
Laufende Nummer:	13
Text:	DA-R7871

Komprimierter Datensatz:
0022E6HV-l-ll,72t-0,00t-0E80-2005-01-18-10:06-13-DA-R7871
62D21D16E6C28C64B75C3FDFD78C8EC35C1C70A2217F
5CEAC8F34960DB3B02EACE466DEDECC53F

Tabelle 1: Signierter Datensatz

5 Verifikation

Das Signaturverfahren und die verwendeten Kurvenparameter sind öffentlich. Alle Zertifikate sind über das Internet verfügbar. Damit ist es jedem möglich, die Überprüfung der signierten Datensätze gemäß den entsprechenden Standards selbst zu implementieren und durchzuführen. Abb. 5 zeigt den allgemeinen Ablauf der Verifikation.

Es existieren aber auch vorgefertigte, für Laien einfacher benutzbare Lösungen: Schenck Process wird in seinem

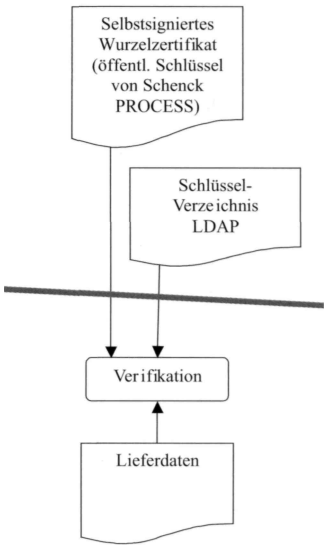


Abb. 5: Verifikation

Internetbereich ein Programm zur Verfügung stellen, mit dem die Daten interaktiv überprüft werden können. Die signierten Daten werden in eine Eingabemaske eingegeben. Das System hat Zugriff auf die Zertifikate und kann eine Korrektheitsaussage machen. Wegen der Gefahr von Eingabefehlern (speziell bei der Signatur) ist dieses Verfahren nur geeignet, wenn der Kunde wenige Signaturen prüfen will.

Eine andere Möglichkeit der Verifikation wäre ein eigenes zu diesem Zweck erstelltes Verifikationsprogramm, das beim Kunden läuft. Dieses erlaubt einerseits die manuelle Eingabe der Daten wie im oben beschrieben Web-Service. Es hat aber auch eine Datenschnittstelle, mit welcher der komprimierte Datensatz eingelesen und verarbeitet werden kann. Weil die Zertifikate per Internet bezogen und dann lokal gespeichert werden können, ist bei dieser Lösung kein permanenter Internetzugang notwendig.

6 Ausblick

Eine befristete Zulassung zur Erprobung des Systems ist im Gange. Sie gibt allen beteiligten Parteien (Hersteller, Zulassungsbehörde, Eichbehörden) die Möglichkeit Erfahrungen mit dem neuen System auf einer geregelten gesetzlichen Grundlage zu sammeln.

Mit absehbaren leistungsfähigeren Waagenhardwaren können die Berechnungen beschleunigt werden. Dadurch werden sogar bei längeren Schlüsseln (192 Bit) deutlich kürzere Bearbeitungszeiten erwartet. Angesichts der immer weiteren Verbreitung der PCs im Bereich der eichfähigen Wägetechnik erscheint auch die Übertragung des Verfahrens auf die offene PC-Architektur interessant.

References

1 S. Boeyen, T. Howes, and P. Richard. Internet X.509 Public Key Infrastructure LDAPv2 Schema. IETF RFC 2587, June 1999. www.ietf.org/rfc/rfc2587.txt.

2 Department of Cryptography and Computeralgebra (CDC). FlexiPKI Homepage, www.cdc.informatik.tu-darmstadt.de/research/pki.html.

3 Gesetz über das Mess- und Eichwesen (EichG). BGBl. 11969, S. 759, zuletzt geändert durch Art. 115 der Verordnung v. 25.11.2003, BGBl. I 2003, S. 2304, bundesrecht.juris.de/eichg/index.html.

4 European Union Parliament and Council. Directive 1999/93/EC of the European Parliament and of the Council of 13. December 1999 on a Community Framework for Electronic Signatures. Official Journal of the European Communities, L13:12-20, Januar 2000. http://europa.eu.int/eur-lex/pri/en/oj/dat/2000/l_013/l_01320000119en00%120020.pdf.

5 ITU-T. Information Technology — Open Systems Interconnection — The Directory: Authentication Framework, August 1997. www.itu.int/rec/recommendation.asp?type=folders&lang=e&parent=T-%REC-X.509.

6 D. Johnson, A. Menezes, and S. Vanstone. The Elliptic Curve Digital Signature Algorithm (ECDSA). International Journal of Information Security, pages 36-63, August 2001. Version von 1999: citeseer.ist.psu.edu/johnson99elliptic.html.

7 LiDIA-Group. LiDIA - A library for computational number theory. TU Darmstadt, 2004. www.informatik.tu-darmstadt.de/TI/LiDIA/Welcome.html.

8 National Institute of Standards and Technology. FIPS PUB 140-1. http://csrc.nist.gov/publications/fips/fipsl40-l/fipsl401.pdf, 1994.

9 Physikalisch-Technische Bundesanstalt (PTB). Leitfaden zur Prüfung von Software (Waagen). www.welmec.org/publications/2-3ge.pdf, Juni 2002.

10 SELMA: Sicherer Elektronischer Messdatenaustausch. www.selma-project.de/.

11 Shamus Software Ltd. Multiprecision Integer and Rational Arithmetic C/C++ Library. http ://indigo .ie/ ~ mscott/.

12 Gesetz über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften (SigG). BGBl. I 2001, S. 876, zuletzt geändert durch Art. 3 Absatz 9 des Gesetzes v. 7.7.2005, BGBl. I 2005, S. 2013, http://bundesrecht.juris.de/bundesrecht/sigg_2001/gesamt.pdf.

13 Nigel Smart. Cryptography: An Introduction. Mcgraw-Hill College, 2004.

Autoren

Dr. Ulrich Rauchschwalbe arbeitet als Produktmanager bei der Schenck Process GmbH. Er betreut dort neben den Wägeelektroniken der DISOMAT Familie auch die Wägesensoren.

Prof. Dr. Johannes Buchmann ist Leiter des Fachgebietes Theoretische Informatik an der TU-Darmstadt. Das Fachgebiet erforscht Kryptographie und Computeralgebra.

Dr. Christoph Ludwig ist wissenschaftlicher Mitarbeiter bei Prof. Buchmann. Neben seinem Schwerpunkt Gitterkryptographie beschäftigt er sich u.a. mit performanten kryptographischen Implementierungen in Embedded Systems und auf Smart Cards.

Dipl.-Inform. Alex Wiesmaier ist wissenschaftlicher Mitarbeiter bei Prof. Buchmann. In seinem Schwerpunkt IT-Sicherheit beschäftigt sich u.a. mit angewandter Sicherheit und Public Key Infrastrukturen.