Sicherheit moderner Frankiersysteme

Gerrit Bleumer, Heinrich Krüger-Gebhard

Francotyp-Postalia AG&Co, g.bleumer@francotyp.com,
Rohde & Schwarz SIT GmbH, Heinrich.Krueger-Gebhard@sit.rohde-schwarz.com

Zusammenfassung

In den USA und mit Abwandlungen auch in Kanada wird seit 1996 ein technisches Programm in die Praxis umgesetzt, das den Markt von mechanischen auf elektronische Lösungen umstellen sowie Manipulation und den Mißbrauch von Frankiersystemen signifikant eindämmen soll. Dieses Programm (Information Based Indicia Program IBIP) umfasst sowohl stand-alone Frankiermaschinen als auch PC-Frankierlösungen und schreibt für beide den Einsatz starker Authentisierungstechniken auf der Basis von Public-Key Kryptographie vor. Inzwischen haben erste europäische Postbehörden, z.B. die DPAG, ähnliche Frankiersysteme spezifiziert. Unsere Firmen entwickeln gemeinsam die Software für ein manipulationsgeschütztes kryptographisches Hardwaremodul (Postal Security Device), wie es von den Postbehörden der USA und Kanada gefordert wird.

Wir zeigen am Beispiel des US Frankiersystemmarkts, wie Public Key Kryptographie eingesetzt werden kann, um den gesamten Lebenszyklus der kryptographischen Module von der Fertigung über die Einbettung in das jeweilige Hostsystem (Frankiermaschine) und den anschließenden weltweiten Vertrieb bis zum üblicherweise mehrere Jahre währenden Gebrauch beim Endkunden zu schützen. Die Herausforderung der Gesamtlösung liegt darin, die postalischen Vorgaben aller Zielländer zu erfüllen, dennoch ein für alle Länder einheitliches und sicheres logistisches Vertriebskonzept aufzubauen, und dennoch die Kosten zu begrenzen.

1 Technischer Überblick

Trotz moderner elektronischer Kommunikationssysteme wie Email und Fax spielt das Versenden von materiellen Poststücken noch immer eine zentrale Rolle im privaten und wirtschaftlichen Leben. In den Aufsätzen [Tygar_96] und [Pintsov_98] und offiziellen Geschäftsberichten der US Post werden dazu die folgenden Informationen gegeben:

- Die US-Postbehörde (US Postal Service, USPS) stellt jährlich etwa 197 Milliarden Poststücke zu (Stand 1998).
- Ungefähr 80 % der Briefpost wird dabei von computergestützten Systemen versendet.
- In den USA existieren ca. 1,5 Millionen Frankiermaschinen, über die jährlich Post mit einem Portowert von insgesamt ca. 20 Milliarden Dollar versendet wird.

In Deutschland wurden nach Angaben der Deutschen Post 1998 etwa 20 Milliarden Briefe und 4,5 Milliarden Pakete zugestellt, bei einer jährlichen Wachstumsrate von 4 bis 6 %.

Die betrügerische Verwendung von Frankiermaschinen ist für die Postbehörden ein signifikantes Problem:

- 1996 waren in den USA ca. 82.000 Frankiermaschinen als gestohlen gemeldet.
- Die USPS schätzt, daß ihr pro Jahr ca. 100 Millionen Dollar Verlust durch gestohlene und/oder manipulierte Frankiermaschinen entsteht.

Bisher werden Frankiermaschinen mit traditionellen Techniken wie Siegeln etc. geschützt. Gedruckt wird üblicherweise mit weniger zugänglichen Druckfarben, etwa fluoreszierender Tinte. Der Frankierabdruck selbst (engl.: indicium) enthält Angaben über den Portowert, Ort und Datum des Drucks, ggf. Werbelogos, den Hersteller der Frankiermaschine und weitere Informationen (siehe Abbildung 1).

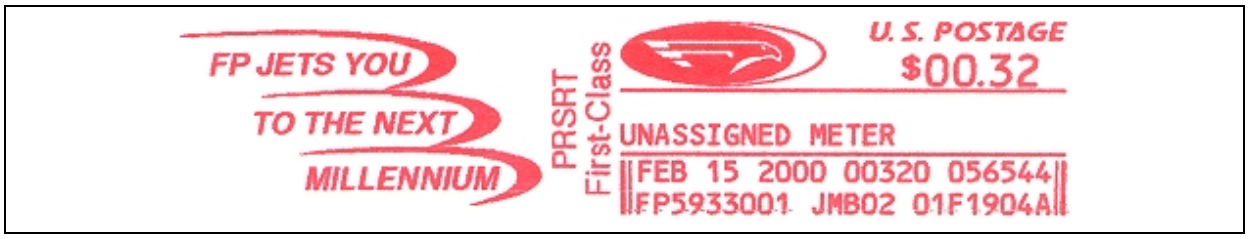

Abbildung 1: Beispiel eines konventionellen Frankierabdrucks

Die bisherigen Verfahren bieten relativ geringen Schutz gegen die folgenden Angriffs-Szenarien:

- Mechanische Manipulation von Frankiermaschinen so dass kostenlose Frankierabdrücke erzeugt werden können (Manipulation interner Zählerstände),
- Fälschen gültiger Frankierabdrücke (Selbstgemachte Stempel und Stempelfarbe),
- Benutzung einer Frankiermaschine durch nicht autorisierte Personen,
- Diebstahl von Frankiermaschine.

In den USA und Kanada wurden daher seit Mitte der 90er Jahre Verfahren entwickelt, die eine erheblich größere Sicherheit vor betrügerischem Mißbrauch von Frankiersystemen bieten. Jede neu in den Markt gestellt Frankiermaschine muß mit einem kryptographischen Hardwaremodul (Postal Security Device, PSD) ausgerüstet sein, das manipulationsgeschützten permanenten Speicher, RAM und Prozessor besitzt und gemäß [FIPS 140-1_94] evaluiert ist. Wir skizzieren seine Arbeitsweise grob:

- Das PSD kann sich über eine Modemverbindung mit einem Datenzentrum gegenseitig kryptographisch stark authentisieren. Sofern der Kunde zuvor ein Guthaben bei diesem Datenzentrum aufgebaut hat, kann das PSD seiner Frankiermaschine daraufhin Portowerte vom Datenzentrum in den manipulationsgeschützten Speicher des PSDs laden.
- Das PSD erzeugt bei Bedarf die Daten für einen Frankierabdruck. Dabei verringert es seinen intern gehaltenen Portowert um den Wert des aktuell erzeugten Frankierabdrucks. Aus historischen Gründen wird der Portowert jedes PSD intern von drei Registern gehalten, dem „ascending register“ (AR), dem „descending register“ (DR) und dem „total settings register“ (TS). Das total settings register hält die Summe aller Portowerte, die das PSD seit Fertigung vom Datenzentrum geladen hat. Das ascending register hält die Summe der Werte aller seit Fertigung erzeugten Frankierabdrücke, und das descending register hält den zu jedem Zeitpunkt im PSD verbliebenen Portowert. Die Redundanz der drei postalischen Register ist durch folgende Gleichung beschrieben: AR + DR = TS.
- Die Frankiermaschine kodiert die Daten des Frankierabdrucks in einen 2-dimensionalen Barcode
- PDF417 http://www.pdf417.com/ oder
- DataMatrix http://www.rvsi.com/cimatrix/DataMatrix.html.

- Diese Daten können in Briefverteilzentren mit preiswerten Scannern eingelesen und automatisch verarbeitet werden.
- Das ECDSA-Signaturverfahren (elliptic curve digital signature algorithm) [ANSIX9.62_98] und [Johnson_99] bietet nach heutigem Wissensstand bei Signaturlängen von 160-200-bit eine vergleichbare oder höhere Sicherheit als 1024-bit-RSA. Der Standardisierungs-Prozess für ECDSA ist sowohl bei [ANSIX9.62_98] als auch bei [IEEEP1363_99] in der Endphase.

In den Frankierabdruck werden weitere Daten einbezogen, etwa eine Identifikation der Frankiermaschine, eine Zählvariable sowie der aktuelle Stand der Postregister der Frankiermaschine. Der gesamte Frankierabdruck einschließlich einer digitalen Signatur wird als Barcode kodiert — ein Teil der Informationen wird außerdem in menschenlesbarer Form gedruckt.

Dadurch wird unter anderem folgendes erreicht:

- Das Fälschen von Frankierabdrücken ist praktisch unmöglich, da ohne Kenntnis des für eine Frankiermaschine registrierten Signierschlüssels keine gültige Signatur erzeugt werden kann.
- Das mehrfache Kopieren eines gültigen Frankierabdrucks kann anhand des konstanten Zählerstandes schnell erkannt werden.
- Wenn eine Frankiermaschine gestohlen und nicht sofort telefonisch vom Kunden gesperrt wird, so führt dies nicht ohne weiteres zu einem Verlust für die jeweilige Postbehörde. Gegen ein Abfrankieren der verbliebenen Portowerte kann sich der Kunde schützen, indem er bei Inbetriebnahme seiner Maschine einen Passwortschutz aktiviert.

In den folgenden Abschnitten wird das verwendete kryptographische Hardwaremodul genauer beschrieben.

2 Das Sicherheitsmodul (Postal Security Device)

Kernstück der beschriebenen Techniken ist ein Sicherheitsmodul (postal security device, *PSD*), das in die Frankiermaschine eingebaut wird und das ein sicheres Laden und Verwalten von Portowerten auch in einer vom Benutzer—und nicht von einer Postbehörde—kontrollierten Umgebung ermöglicht. Francotyp-Postalia fertigt für diesen Zweck spezielle kryptographische Hardwaremodule etwa von der Größe einer Zigarettenschachtel, die in Epoxit-Harz eingegossene auslesegeschützte Speicher und Micro-Controller (ARM7) für die kryptographischen Funktionen enthalten.

Der weltweit bekannteste Standard für Sicherheitsmodule dieser Art ist [FIPS140-1_94] der amerikanischen Standardisierungsbehörde NIST (National Institute of Standards and Technology). Dieser Standard beschreibt vier Sicherheitsstufen. Die niedrigste Stufe 1 kann auch von softwarebasierten Systemen erreicht werden. Die USPS verlangt, dass PSDs in Frankiermaschinen auf Stufe 3 mit einigen Zusatzanforderungen evaluiert werden müssen („Level 3+“). Einen regelmäßig aktualisierten Überblick über erfolgreich evaluierte kryptographische Hardwaremodule veröffentlicht das NIST unter http://csrc.nist.gov/encryption.

Die Zertifizierung erfolgt durch ein NIST-akkreditiertes Testlabor. Mit diesem Labor besteht schon während der Entwicklungs-Phase regelmäßiger Kontakt. Im folgenden beschreiben wir einige Elemente des Zertifizierungsprozesses etwas genauer — weitere Informationen findet man bei Smith, Weingart und anderen [Smith1_99, Smith2_99], die den Zertifizierungsprozess am Beispiel des Crypto-Coprocessor *IBM 4758* beschreiben, das erste Sicherheitsmodul, das eine Evaluierung der Stufe 4 erreicht hat.

2.1 Manipulationssichere Ummantelung

Das PSD muss vollständig umgeben sein von einer nicht ablösbaren und undurchsichtigen Hülle, die aktiv auf Manipulationsversuche reagieren kann. Manipulationsversuche durch Anbohren, Feilen, Sägen oder chemische Auflösung müssen erkannt werden. Außerdem wird gefordert, dass Temperatur- und Spannungsschwankungen erkannt werden (Environment Failure Protection). Bei einem Manipulationsversuch müssen alle sicherheitsrelevanten Parameter gelöscht (auf Null gesetzt) werden. Die postalischen Register hingegen dürfen nicht gelöscht werden, damit bei einer späteren Untersuchung unter anderem geklärt werden kann, welche Auswirkungen mögliche Betrugsversuche auf das Datenzentrum gehabt haben, das dieses PSD mit Portowerten versorgt hat. Außerdem müssen PSDs ausreichend robust sein gegen „linear and differential timing and power attacks“.

Die Zertifizierungslabore verfügen über Ausrüstung (zum Beispiel Präzisionsfräsen, Bohrer im $^{1}/_{10}$-mm-Bereich, chemisches Labor), um alle relevanten Angriffe selbst durchzuführen und auszuwerten.

Für das Erreichen dieser Anforderungen wird die Platine des PSD mit einer 7 mm dicken, von Serpentinenkontakten durchzogenen Schicht aus Epoxit-Harz umgossen. Auf der Platine sind Spannungs- und Temperatursensoren sowie eine Batterie untergebracht, um das Löschen der sicherheitsrelevanten Parameter auch bei Abfall der äußeren Spannung zu gewährleisten.

2.2 Software, Schnittstellen

Für das PSD muß eine Sicherheitspolitik aufgestellt werden. Der Lebenszyklus des PSD muß in Form eines endlichen Automaten spezifiziert werden. Die wesentlichen Teile der PSD-Software müssen in einer Hochsprache geschrieben sein — in unserem Fall C++. Diese Software muss so dokumentiert sein, dass ihr Zusammenhang mit dem Finite-State-Machine Modell klar und eindeutig ersichtlich ist und zum Testen der Software herangezogen werden kann.

Nach außen muss das Modul eine Anzahl von abgrenzbaren Diensten bieten, für die eine rollen-basierte Autorisierung gefordert wird.

In unserem Fall sind wesentliche Dienste — etwa das Laden von Portowerten etc. — durch Public-Key Methoden gesichert. Das ließ sich nicht immer einfach auf die passwort-orientierten Vorstellungen aus [FIPS140-1_94] abbilden.

2.3 Validierung kryptographischer Algorithmen

Der Standard [FIPS-140-1_94] verlangt spezielle Konformanz-Testreihen für die Implementierung von offiziellen FIPS-Algorithmen — z. Zt. sind dies DES, Triple-DES, AES, RSA Signieren und ECDSS (Elliptic Curve Digital Signature Standard). Für uns ergaben sich daraus Konformanztests für die Implementierungen von DES, Triple-DES und SHA-1.

Die Testbeschreibungen umfassen jeweils einige hundert Seiten und sind nicht immer eindeutig, so dass es einige Iterationen kostete, um zu einer akzeptierten Implementierung der Testrahmen zu kommen — besser wäre wenn das NIST die Testrahmen selber stellte. Für die mindestens eben so wesentlichen Public-Key Algorithmen —RSA, Diffie-Hellman, ECDSA — gibt es bislang überhaupt keine speziellen Anforderungen (RSA in Vorbereitung).

3 Zweidimensionale Barcodes

Traditionelle Barcodes werden seit Jahrzehnten zur Kennzeichnung von Einzelhandelsartikeln, Transportstücken, Medikamenten, Bibliotheksbüchern, etc. eingesetzt. Solche Barcodes heißen eindimensional, da die Information nur in einer Dimension kodiert ist.

Abbildung 2: Beispiel eines eindimensionalen Barcodes

Größere Datenmengen können zum Beispiel in zweidimensionalen (2D) Barcodes kodiert werden. Zwei weit verbreitete 2D-Barcodes sind PDF417 (PDF417 steht für „Portable Data File“, nicht zu verwechseln mit Adobes „Portable Document Format“) und DataMatrix.

2D-Barcodes erreichen erheblich höhere Informationsdichten als traditionelle Barcodes: Ein häufig verwendeter 2D-Barcode im Bereich Transport, Logistik und Gesundheitswesen ist PDF 417, erfunden 1991 von Ynjiun Wang bei Symbol Technologies http://www.symbol.com/. Ein PDF417 Abdruck kann maximal 2000 8-bit Zeichen enthalten. Ein typischer Abdruck ist 3-4 square inch groß und erzielt eine typische Datendichte von 100 bis 300 Byte per square inch (entspricht 15,5 bis 46,5 Byte je cm^2).

Abbildung 3: Beispiel eines PDF417 2D-Barcodes

Besonders bei der Produktion von elektronischen Bauteilen, wo weniger Platz für den Abdruck zur Verfügung steht, kommt häufig der DataMatrix ECC-200 zum Einsatz. Er wurde 1995 bei RVSI entwickelt (http://www.rvsi.com/). Ein Abdruck kann maximal 2335 8-bit Zeichen enthalten und erzielt eine typische Datendichte von 5000 Byte per square inch (entspricht 775 Byte je cm^2). Ein Beispiel eines DataMatrix Barcodes zeigt Abbildung 4.

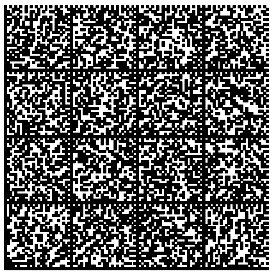

Abbildung 4: Beispiel eines DataMatrix ECC-200 2D-Barcodes

Durch Fehlerkorrekturverfahren kann bei beiden 2D-Barcodes erreicht werden, dass noch Abdrücke gelesen werden können, von denen bis zu 40% der Fläche unlesbar sind. (Technische Angaben gemäß Russ Adams Bar Code Homepage [Adams_01])

Die USPS unterstützt als Bestandteil des Frankierabdrucks die 2D-Barcodes *PDF417*, *DataMatrix* und andere, die kanadische Post die Barcodes *DataMatrix* und *Aztec*. Gedruckt wird mit einer Auflösung von mindestens 200 dpi. Die Lesefehlerrate muss unter 0,5 % liegen.

4 Postalische Transaktionen und die Struktur des Frankierabdrucks

4.1 Portoladen, Postalische Register

Die wesentlichen finanziellen Transaktionen einer Frankiermaschine sind das sichere Portoladen (postage value download) und das Erzeugen von Frankierabdrücken.

Das Portoladen geschieht in folgenden Schritten:

- Der Kunde zahlt einen Geldbetrag ein auf ein Konto, das entweder dem Frankiersystembetreiber oder der Postbehörde gehört. Die Bank benachrichtigt den Frankiersystembetreibers über der erfolgten Einzahlung.
- Der Hersteller erhöht daraufhin den Kontostand eines speziellen Portokontos des Kunden. Gleichzeitig wird ggf. der entsprechende Betrag auf ein Konto der Postbehörde eingezahlt.
- Der Kunde stellt nun durch Knopfdruck an der Frankiermaschine eine Modemverbindung zu dem Sicherheitsmodul der betreffenden Frankiermaschine her und führt das Portoladen durch.
- Es findet eine gegenseitige Authentisierung statt; gleichzeitig werden Sitzungsschlüssel für die Authentisierung von Nachrichten sowie zum Verschlüsseln von Daten vereinbart.
- Schließlich wird der gewünschte Portowert dem Kundenkonto im Datenzentrum belastet und gleichzeitig im PSD gutgeschrieben. Dies geschieht durch entsprechende Inkrementierung des Total Settings Register (TS) und des Descending Register (DR).

4.2 Frankierabdruck USA

Abbildung 5 zeigt die Struktur und die enthaltenen Daten eines Frankierabdrucks, wie er von der USPS für das IBI-Programm gefordert wird [PCIBI-C_99].).

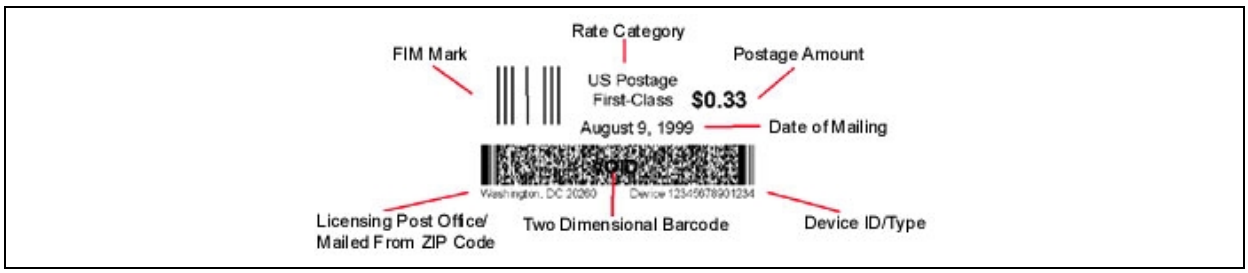

Abbildung 5: Beispiel eines Frankierabdrucks gemäß IBI-Programm

Gemäß IBI-Programm enthält der Barcode-Teil des Frankierabdrucks die folgenden Daten:

Barcode-Daten, USA

Feld	Indicium Version	Algorithmus-OID	Zertifikats- Serien-Nummer	Geräte-ID (PSD)	Ascending Register (AR)	Portowert	Frankier-Datum	Ursprungs-ZIP	(unspezifiziert)	Software ID	Descending Register (DR)	Porto-Kategorie	Signatur (ECDSA)	(unspezifiziert)
Länge [Bytes]	1	1	4	8	5	3	4	4	5	6	4	4	42	?
	49												42	

Abbildung 6: Dateninhalt eines Indicium nach IBI-Programm

Ein Teil dieser Daten wird auch in menschenlesbarer Form aufgedruckt. Die Signatur erstreckt sich über die grau markierten Daten— die signierten Daten erlauben die eindeutige Identifikation des PSD sowie des einzelnen Frankiervorgangs (durch den Wert des ascending register (AR)).

Der (geheime) Signierschlüssel wird im Sicherheitsmodul erzeugt. Der zugehörige Verifizierschlüssel wird von der Frankiersystembetreiber zertifiziert. Der Signierschlüssel hat eine Lebensdauer von drei Jahren.

Das Zertifikat des Verifizierschlüssels wird an die postalische Infrastruktur übertragen. Die Postverteilzentren müssen auf die Zertifikate aller Sicherheitsmodule zugreifen können, denn ein Poststück kann grundsätzlich von jeder im Markt befindlichen Frankiermaschine freigemacht worden sein.

4.3 Frankierabdruck, Kanada

Gemäß der kanadischen Spezifikation für elektronische Frankiermaschinen [CPC_00] enthält der Barcode-Teil des Frankierabdrucks die folgenden Daten:

	Barcode-Daten, Kanada														
Feld	Country Code	Indicium Kenner	Algorithmus-OID	Zählnummer	Frankier-Datum	Absende-Datum	Ascending Register (AR)	Descending Register (DR)	Porto-Kategorie	Portowert	Zertifikats- Serien-Nummer	Zertifikats-Gültigkeitsende	MAC über die lesbaren Daten	Signatur (ECDSA)	Public ECDSA Key	Signature der Hersteller-CA
Länge [Bytes]	2	1	1	3	2	1	5	4	2	3	4	2	5	42	22	42/ 48
	2	33												112 max		

Abbildung 7: Dateninhalt eines Indicium nach kanadischer Spezifikation

Ein Teil dieser Daten wird auch in menschenlesbarer Form aufgedruckt. Die Signatur erstreckt sich die in Abbildung 7 grau markierten Datenfelder sowie 31 Padding-Bytes. Unterschiede zum IBI-Programm der USPS:

- Der Signierschlüssel wird mit dem zugehörigen (öffentlichen) Verifizierschlüssel vor jedem Portoladen neu erzeugt.
- Der Verifizierschlüssel wird — zusammen mit einem Datensatz, der das PSD sowie den momentanen Stand der Postregister eindeutig beschreibt — an die Frankiersystembetreiber übermittelt.
- Der Frankiersystembetreiber signiert den Verifizierschlüssel und die genannten Daten mit seinem Signierschlüssel. Ein von der Postbehörde signiertes Zertifikat für den zugehörigen Verifizierschlüssel ist frei verfügbar.

Bei diesem Verfahren muss jedes Postverteilzentrum lediglich über das Zertifikat des Frankiersystembetreibers verfügen; in den USA hingegen muss für jedes PSD ein eigenes Zertifikat vorhanden sein.

5 Infrastruktur des Frankiersystembetreibers

Hinsichtlich der Sicherheit moderner Frankiersysteme verlassen sich die Postbehörden der USA und Kanadas in erster Linie auf den Manipulationsschutz unabhängig evaluierter kryptographischer Hardwaremodule. Stünden nicht enorme Kosten dagegen, würden die Postbehörden einen durchgehenden Ende-zu-Ende Schutz von der Bank bis zum PSD in jeder Frankiermaschine einfordern und zwar so, daß auch in den Datenzentren der Frankiersystembetreiber die Kundendatenbanken durch entsprechende FIPS140-1 evaluierte kryptographische Hardwaremodule eingesetzt werden. Ganz bewußt und aufgrund einschlägiger Erfahrung vertrauen die Postbehörden den Datenzentren der Frankiersystembetreiber nicht wirklich, sondern erfordern sauber dokumentierte Systemabläufe und führen regelmäßige Inspektionen vor Ort durch. Noch stärker misstrauen die Postbehörden den Unterauftragnehmern und den Kunden der Frankiersystembetreiber; sicher mit Recht, denn diese sind nur den Betreibern bekannt, nicht den Postbehörden.

Üblicherweise betreibt jeder Frankiersystembetreiber ein eigenes Datenzentrum für seine Frankiermaschinen und bietet speziell auf seine Maschinen abgestimmte Zusatzdienste an. Das Datenzentrum versorgt die elektronischen Frankiermaschinen mit Portokontingenten, auditiert sie in regelmäßigen Zeitabständen und bietet weitere Zusatzdienste, wie z.B. das Abfragen der Kundenkontenstände oder Bestellen neuer Druckköpfe, Farbbänder, Werbeklischees, etc.

5.1 Sicherheit als Kostenfaktor

Die Postbehörde muss vermeiden, dass sich das elektronische Porto im Datenzentrum eines Frankiersystembetreibers oder in einer Frankiermaschine erhöht, ohne dass vorher eine Einzahlung in derselben Höhe vorausgeht. Dieses Schutzziel der finanziellen Integrität ist von einem Frankiersystembetreiber durch eine geeignete Spezifikation, Dokumentation und Implementierung seines Frankiersystems zu beantworten. Um die postalische Zulassung zu bekommen, muß die Postbehörde „überzeugt“ werden, daß das vorgeschlagene Frankiersystem nach dem Stand der Technik entwickelt wurde und ein hinreichend geringes Betrugsrisiko verbleibt. Dieser Überzeugungsprozeß ist wenig formalisiert, er orientiert sich teilweise an Sicherheitsstandards aus dem Bankenbereich und bleibt letztlich ein wirtschaftspolitischer Verhandlungsprozeß, bei dem sich die Postbehörde von hohen Sicherheitsforderungen und der Frankiersystembetreiber von kostengünstigen Sicherheitsangeboten ausgehend aufeinander zubewegen, bis eine für beide Seiten gerade noch erträgliche Lösung gefunden ist. Dabei treibt beide das Bemühen um ein kurzes time-to-market und die Postbehörde zusätzlich das Bemühen, alle Frankiersystembetreiber im Wettbewerb zu halten.

Gegenüber dem Endkunden wird die Forderung nach finanzieller Integrität durch das PSD gelöst. — Dem Datenzentrum selbst kann jedoch auch nicht bedingungslos vertraut werden. Ein Systemadministrator hat üblicherweise Zugriffsrechte auf alle Tabellen seines Datenbanksystems und könnte dafür sorgen, dass bestimmte Konten gelegentlich aufgefüllt werden, ohne dass eine entsprechende Einzahlung erfolgt ist. Die USPS hat seit Auflegung ihrer IBIP Spezifikation die Sicherheitsanforderungen immer wieder erhöht, um den bekannt gewordenen Missbrauchsfällen zu begegnen. Dazu gehört, dass verschiedene Transaktionen innerhalb des Datenzentrums des Frankiersystembetreibers ebenfalls durch kryptographische Module geschützt werden sollen.

Die USPS inspiziert darüber hinaus die Fertigung und den Vertrieb der PSDs aller Frankiersystembetreiber sowie das Schlüssel-Management ihrer Frankiersysteme. Dies führt zu erhöhten Kosten, denen kein Nutzen für den Endkunden oder den Frankiersystembetreiber gegenübersteht: Ein typisches Problem in einem stark regulierten Markt-Segment.

5.2 Weltweite Infrastruktur

Ein weltweit agierender Frankiersystembetreiber unterhält typischerweise eine Public-Key Infrastruktur mit folgenden Hierarchie-Ebenen:

- Die Stamm-Niederlassung des Frankiersystembetreibers oder ein beauftragtes Trust Center dient typischerweise als Wurzel-CA (Certification Authority).
- Die Datenzentren der Niederlassungen in den verschiedenen nationalen Zielmärkten dienen als CA für das betreffende Land.
- Die unterste Hierarchiestufe bilden die PSDs.

Die PSDs müssen während ihrer gesamten Lebensdauer lückenlos verfolgt werden. Dies umfasst:

- Die kryptographische Initialisierung gleich nach der Herstellung,
- den Vertriebsweg ins Zielland und zum Kunden,
- die (evtl. wiederholte) Zuordnung zu neuen Kunden bzw. Leasing-Partnern,
- den normalen Frankierbetrieb,
- die dokumentierte Außerbetriebnahme.

Zum Schutz vor Manipulation, Diebstahl von PSDs sowie dem Einschleusen unauthorisierter PSDs werden ähnliche organisatorische Maßnahmen eingesetzt, wie zur Verteilung von Kreditkarten.

5.3 Prä-Initialisierung von PSDs

Damit PSDs bereits während des Transports zur Produktionsstätte ihres späteren Hosts—hier einer Frankiermaschine—und von dort zum Kunden sicher verfolgt werden können, wird direkt nach der Produktion ihre eindeutige und fälschungssichere kryptographische Identität vom PSD Hersteller registriert, wobei der PSD Hersteller wiederum von der (Francotyp-Postalia) Wurzel-CA zertifiziert ist. Hier werden Standardverfahren nach X.509 benutzt. Diese Prä-Initialisierung ist ein sicherheits-kritischer Prozess, weil diese erste Übertragung von public keys und public-key Zertifikaten nicht kryptographisch, sondern nur durch organisatorische Maßnahmen geschützt werden kann.

Wie in der Einführung zu Kapitel 5 beschrieben misstraut die USPS den Frankiersystembetreibern, besonders ihren Unterauftragnehmern und in verschärfter Weise PSD-Herstellern,

die keine US-Unternehmen sind. Sie besteht in jedem Fall auf Inspektionen der PSD-Fertigung. Um den Aufwand und die Kosten solcher Inspektionen, die voll zu Lasten des Frankiersystembetreibers gehen, gering zu halten, entschärft Francotyp-Postalia das inhärente Sicherheitsproblem der Prä-Initialisierung durch eine Sichtkontrolle jeder Frankiermaschine, die in den US-Markt gestellt werden soll, und eine Nachinitialisierung des eingebetteten PSDs. Sichtkontrolle und Nachinitialisierung geschehen bei Francotyp-Postalia US in den USA unter stichprobenweiser Aufsicht der USPS. Dabei generiert sich jedes PSD ein weiteres Signierschlüsselpaar und läßt es vom Datenzentrum seines Ziellandes (im Beispiel USA) zertifizieren. Die Rolle der Wurzel-CA wird im nächsten Unterkapitel betrachtet.

Die Nachinitialisierung im Zielland ist nur für mittlere Stückzahlen praktikabel, weil die bereits zuvor kundenfertig verpackten Kartons geöffnet werden müssen, um das in seine Frankiermaschine eingebettete PSD über eine vorbereitete Schnittstelle an den Nachinitialisierungsrechner anzuschliessen. Dieser Prozess kann bei größeren Stückzahlen leicht zum Flaschenhals werden. Daher hat Francotyp-Postalia ein kryptographisches Verfahren entwickelt, das die inhärente Unsicherheit des Prä-Initialisierungsprozesses entschärft, ohne dass im Zielland eine Kommunikationsverbindung zu jedem PSD aufgebaut werden muß, bevor es mit seiner Frankiermaschine zum Kunden ausgeliefert wird.

Es funktioniert so, daß der Verifizierschlüssel eines PSDs z.B. mittels einer Speicherchipkarte in einer Känguruhtasche am Karton seiner Frankiermaschine befestigt wird, bevor der Karton die Frankiermaschinenfertigung verläßt. Kommt eine Lieferung bei Frankotyp-Postalia im Zielland an, so wird eine individuelle und gleichverteilt zufällig erzeugte BoxID erzeugt. Der Verifizierschlüssel und die dafür erzeugte BoxID werden in einer Datenbank registriert, der Verifizierschlüssel auf der Speicherchipkarte wird zuverlässig gelöscht und durch die BoxID ersetzt. Sobald der Kunde seine Frankiermaschine ausgepackt und angeschlossen hat, führt er die Speicherchipkarte in das Lesegerät seiner Frankiermaschine ein, die Frankiermaschine wählt sich zum Datenzentrum bei der Tochter von Francotyp-Postalia ein und sendet nun als erstes eine Signatur der BoxID. Das Datenzentrum prüft, ob diese Signatur gültig ist gegen den Verifizierschlüssel, den es zuvor für diese BoxID registriert hat.

Dieses Verfahren vereitelt die bekannten man-in-the-middle Attacken bei der Prä-Initialsierung, weil der Angreifer seine Frankiermaschine am Datenzentrum des Ziellandes nicht erfolgreich registrieren lassen kann, selbst wenn er den gesamten Prä-Initialisierungsprozess beim PSD-Hersteller unterwandert hat und sämtliche geheimen Signierschlüssel aller ausgelieferten PSDs kennt.

5.4 Vertrauensbereich der Wurzel-CA

Die USPS verlangt, dass der Betrieb der Datenzentren von Frankiersystembetreibern im US-Markt nicht von übergeordneten Wurzel-CAs der Betreiber abhängen soll. In diesem Fall könnte der Zertifizierschlüssel des Betreibers außerhalb der USA kompromittiert werden und dadurch Dienste für US Kunden beeinträchtigt werden.

In unserem konkreten Fall hält das Datenzentrum USA zu jedem Zeitpunkt zwei unabhängige öffentliche Schlüssel bereit, die von der Root-CA zertifiziert sind (Lebensdauer 6 – 12 Jahre). Einer der Schlüssel ist aktiv, der andere dient als Ersatzschlüssel. Wenn ein neues PSD registriert wird, so erhält es Zertifikate beider Schlüssel.

Das PSD verifiziert jedes der beiden Zertifikate genau einmal in seinem Lebenszyklus und kann anschließend nur noch mit dem Datenzentrum der USA kommunizieren. Sobald die Registrierung erfolgreich abgeschlossen ist, verhält sich das Datenzentrum USA zu dem neu registrierten PSD wie eine Wurzel-CA.

6 Postalische Infrastruktur USA

Die Postbehörden der USA und Kanadas betreiben Public-Key Infrastrukturen, mit denen die Public-Key-Infrastrukturen der Frankiersystembetreiber interoperieren müssen. Die postalische Public-Key Infrastruktur dient dazu, die Prüfschlüssel aller registrierten Frankiermaschinen aller Frankiersystembetreiber einzusammeln, zu zertifizieren, sicher zu verwalten (inkl. Aktualisierung und Sperrung), und sie allen Postverteilzentren zeitnah zur Verifizierung von Frankierabdrücken bereitzustellen.

Im Endausbau der Postverteilzentren wird ein vollständiges und automatisches Screening aller Frankierabdrücke erfolgen müssen, um die individuellen Signaturen zu verifizieren. In der Anlaufphase des IBI-Programms, in der das Aufkommen der neuen IBI Frankierabdrücke noch sehr begrenzt ist, werden kostengünstigere Mechanismen eingesetzt, wie Stichprobenkontrolle, Handscanner und/oder Überprüfung von Poststücken, die bei konventioneller Behandlung verdächtig auffallen.

7 Kryptographische Mechanismen

In unserem PSD kommen u.a. die folgenden kryptographischen Algorithmen und Standards zur Anwendung:

- Für Signaturen und Authentisierung innerhalb der PKI des Frankiersystembetreibers wird das RSA-Verfahren mit SHA-1 gemäß PKCS #1 und [IEEEP1363_99] verwendet. Die Schlüssellänge beträgt für das PSD 1024 Bits, für alle anderen Instanzen 2048 Bits.
- Für die Authentisierung zwischen PSD und Frankiersystembetreiber wird X.509 *three-way-authentication* in Verbindung mit RSA-Signierschlüsseln verwendet.
- Zertifikats-Requests werden nach PKCS #10 formatiert.
- Für den Austausch von Sitzungsschlüsseln zwischen dem PSD und Datenzentrum wird Diffie-Hellman gemäß [ANSIX9.42_98] verwendet.
- Für die Integrität der zwischen PSD und Datenzentrum übertragenen Daten wird SHA-1 und HMAC gemäß RFC 2104 verwendet.
- Für die Verschlüsselung von Datenfeldern während einer Verbindung zwischen PSD und Datenzentrum wird Triple-DES verwendet. Tatsächlich werden nur wenige Daten verschlüsselt — die für das PSD entscheidenden kryptographischen Dienste sind Authentisierung und Datenintegrität.

Für das Signieren der Barcode-Daten wird der ECDSA gemäß [ANSIX9.62_98] verwendet. [PCIBI-C_99] und [CPC_00] enthalten jeweils eine Liste zulässiger Kurven aus [ANSIX9.42_98]. Wir verwenden eine Kurve über $GF(2^{163})$ mit zufällig erzeugten Punkten (Schlüssellänge 163 Bits; Signaturlänge 42 Bytes). Die nebenstehende Tabelle gibt einen vergleichenden Überblick, in welchem Jahr man für verschiedene kryptographische Verfahren welche Schlüssellänge planen sollte, um gegen schlüsselbezogenes Brechen sicher zu sein.

Schlüssellängen vergleichbarer Sicherheit [Lenstra_99]			
Jahr	Äquivalente Schlüssel-Längen [Bits]		
	Symm. Algorithmen	RSA, DH, ElGamal	ECC
1982	56	417	
1990	63	622	
2000	70	952	132
2010	78	1369	160
2020	86	1881	188

Abbildung 8: Vergleich empfohlener Schlüssellängen

8 Ausblick: PC Frankier-Systeme

In den USA und Kanada sind auch sogenannte PC Frankiersysteme spezifiziert worden, mit denen Privatpersonen oder kleine Firmen Frankierabdrücke auf einem PC-Drucker erzeugen können. Hierfür werden ebenfalls 2D Barcodes und digitale Signaturen verwendet. Das Portoladen erfolgt in diesem Fall via Internet. Die Firma E-stamp verwendete ein PSD in Form eines kryptographisch aufgerüsteten Dongles am PC. Die Firma *stamps.com* bietet eine online-Lösung an, die auf spezielle Hardware beim Kunden ganz verzichtet. Hier sind die individuellen PSDs in Form eines online Datenbanksystems bei *stamps.com* realisiert. Beide Systeme sind von der USPS zugelassen, allerdings mit Auflagen, die für viele Benutzer nicht akzeptabel sind.

Während Frankiermaschinen mit fluoreszierender Tinte drucken, die einen gewissen Schutz vor schlichtem Kopieren bietet, sind Frankierabdrücke aus Laserdruckern oder Tintenstrahldruckern einfach zu reproduzieren. Die IBIP Spezifikation für PC Frankiersysteme sieht daher vor, im Frankierabdruck eine Reihe weiterer Merkmale aufzunehmen und unterschreiben zu lassen, die ein Kopieren von Frankierabdrücken weniger attraktiv machen. So wird z.B. eine knappe Gültigkeitsdauer definiert. Diese muss zusammen mit der Postleitzahl des Empfängers im Frankierabdruck enthalten sein und vom PSD unterschrieben werden.

Das Kopieren eines gültigen Frankierabdrucks ist dann nutzlos: Poststücke mit kopiertem Abdruck können immer nur an den gleichen Empfänger gesendet werden. Durch den Zeitstempel kann dies nur innerhalb eines kleinen Zeitfensters geschehen.

Für Kunden bedeutet dies aber, dass ein Brief innerhalb von 24 Stunden nach Erzeugen des Frankierabdrucks abgeschickt werden muss. Außerdem verlangt die USPS, dass nur solche Empfängeradressen angegeben werden dürfen, die in einem von der USPS vierteljährlich bereitgestellten Adressverzeichnis enthalten sind (AMS CD ROM). Auslandsadressen sind überhaupt nicht enthalten. Durch die hohe Mobilität in den USA sind diese Restriktionen für Kunden unbequem.

Hier zeigt sich, dass der Interessenkonflikt zwischen Sicherheitsbedürfnis der Postbehörden und Wirtschaftlichkeitsbedürfnis der Frankiersystembetreiber bei PC Frankiersystemen verschärft auftritt. Die Risiken für die jeweilige Postbehörde sind größer, weil die Frankierab-

drücke leichter zu reproduzieren sind und weil die Datenzentren der Frankiersystembetreiber am Internet betrieben werden müssen, was weitere Angriffsszenarien ermöglicht.

Technisch gesehen müßte die Integrität der Kundenkonten auf Applikationsschicht (im Sinne von ISO7498) gesichert werden — das ist bis heute in fast keinem Datenzentrum im kommerziellen Bereich realisiert. In [Bleumer_00] wurde gezeigt, wie in einem Frankiersystem die Integrität von elektronischem Porto auf Applikationsschicht durchgängig kryptographisch sichergestellt werden kann, ohne einem Systemadministrator hinsichtlich integrer Verwaltung von Kundenkonten vertrauen zu müssen.

In jüngster Vergangenheit ist der Pionier E-stamp an dem oben beschriebenen Interessenkonflikt gescheitert und hat sein Geschäft mit PC-Porto im November 2000 an einen Mitbewerber verkauft. E-stamp droht nun der Ausschluß aus dem NASDAQ Index.

Die Deutsche Post will im Jahr 2001 ebenfalls ein PC Frankiersystem anbieten und versucht, den beschriebenen Interessenkonflikt von Anfang an dadurch zu entschärfen, dass sie beim Betrieb von Datenzentren für PC Frankiersystem keine Mitbewerber zulässt, sondern ihr Monopol bei der Beförderung von Briefen auf den Verkauf von elektronischem Porto ausdehnt [DPAG_00].

Literatur

Adams_01	http://www.adamsl.com/pub/russadam/stack.html
ANSIX9.42_98	Public Key Cryptography For The Financial Services Industry: Agreement of Symmetric keys on Using Diffie-Hellman and MQV Algorithms. Working Draft, Oct 2, 1998
ANSIX9.62_98	Public Key Cryptography For The Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA). Working Draft, Sep 20, 1998
Bleumer_00	Gerrit Bleumer: Secure PC-Franking for Everyone. Proceedings of EC-WEB'00, LNCS 1875, Springer-Verlag, Berlin 2000, S. 94-109
CPC_00	Canada Post: Digital Postage Indicia Standard for Canada Post. Draft Version 2.0, März 2000
DPAG_00	Deutsche Post AG : Voraussetzungen zur Einführung von Systemen zur PC-Frankierung . Version 1.1, 20.09.2000, http://www.dpag.de/pc-frankierung/
FIPS140-1_94	National Institute of Standards and Technology: Security Requirements for Cryptographic Modules. FIPS-PUB 140 Version 1, 1994 http://www.itl.nist.gov/fipspubs/fip140-1.htm
IEEEP1363_99	IEEE: Standard Specifications for Public Key Cryptography. Draft Version 13, Nov 1999, http://grouper.ieee.org/groups/1363/
Johnson_99	Don Johnson, Alfred Menezes: The Elliptic Curve Digital Signature Algorithm. Technical Report CORR 99-31, Dept. of C&O, University of Waterloo, Canada, http://www.cacr.math.uwaterloo.ca/
Lenstra_99	Arjen. K. Lenstra, Eric R. Verheul: Selecting Crytographic Key Sizes. Oct 1999, http://www.cryptosavvy.com/

PCIBI-C_99 The United States Postal Service (USPS): Information-Based Indicia Program (IBIP) —Performance Criteria for Information-Based Indicia and Security Architecture for closed IBI Postage Metering Systems (PCIBI-C). Draft, Jan 1999, http://www.usps.gov/ibip/

Pintsov_98 Leon A. Pintsov, Scott A. Vanstone: Postal Revenue Collection in the Digital Age. 1998, http://www.cacr.math.uwaterloo.ca/

Smith1_99 Sean W. Smith, Steve. Weingart: Building a High Performance, Programmable Secure Coprocessor. Computer Networks 31, Apr 1999, http://www.research.ibm.com/secure_systems/scop.htm

Smith2_99 Sean W. Smith, Ron Perez, Steve Weingart, Vernon Austel: Validating a High-Performance, Programmable Secure Coprocessor. Secure Systems and Smart Cards, IBM T.J. Watson Research Center, Oct 1999, http://www.research.ibm.com/secure_systems/scop.htm

Tygar_96 J. Douglas Tygar, Bennett S. Yee, Nevin Heintze: Cryptographic Postage Indicia. 1996, http://www.cse.ucsd.edu/users/bsy/papers.html