Missbrauchs-Schutz von Frankier-Maschinen durch Public-Key Kryptografie

G. Bleumer[1], H. Krüger-Gebhard[2]

Zusammenfassung:
In den USA und in Kanada wurden in den letzten Jahren Verfahren entwickelt, mit denen die missbräuchliche Verwendung von Frankier-Maschinen wesentlich erschwert werden soll. Diese Verfahren verwenden starke Authentisierungs-Techniken auf der Basis von Public-Key Kryptografie — sie sind eng verwandt mit den zuletzt stärker publizierten Verfahren für die Frankierung am PC. Es wird damit gerechnet, dass in den nächsten Jahren ähnliche Verfahren auch von europäischen Post-Behörden spezifiziert werden. Wenn diese sich durchsetzen, wird in absehbarer Zeit jeder einzelne Haushalt fast täglich mit Public-Key Kryptografie in Kontakt kommen.
Unsere Firmen entwickeln gemeinsam die Software für ein kryptografisches Modul (Postal Security Device), wie es von den Post-Behörden der USA (/PCIBI-C/) und Kanadas (/CPC 2000/) gefordert wird bzw. in Kürze gefordert werden wird.
In Abschnitt 1 geben wir einen Überblick über die geforderten Verfahren und den dadurch erreichten Schutz. In den darauf folgenden Abschnitten werden die einzelnen System-Elemente genauer beschrieben.

Stichwörter: Public-Key Kryptografie, Digitale Signaturen, Hardware-Sicherheitsmodule, 2D-Barcode, Frankier-Maschinen.

1. Technischer Überblick

Trotz moderner elektronischer Kommunikations-Systeme wie Email und Fax spielt das Versenden von materiellen Post-Stücken noch immer eine zentrale Rolle im privaten und wirtschaftlichen Leben. In den Aufsätzen /Tygar et al/ und /Plintsov et al/ werden dazu die folgenden Informationen gegeben:

- Die US-Postbehörde USPS (US Postal Service) stellt jährlich etwa 165 Milliarden Post-Stücke zu.
- Ungefähr 80 % der Briefpost wird dabei von Computer-gestützten Systemen versendet.
- In den USA existieren ca. 1,5 Millionen Frankier-Maschinen, über die jährlich Post mit einem Porto-Wert von 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 Frankier-Maschinen spielt eine große Rolle:

- 1996 waren in den USA ca. 82.000 Frankier-Maschinen als gestohlen gemeldet.

[1] Francotyp-Postalia AG, Birkenwerder (gbleumer@francotyp.com)

[2] Rohde & Schwarz SIT GmbH, Berlin (Heinrich.Krueger-Gebhard@sit.rohde-schwarz.com)

- Es wird geschätzt, dass dem USPS pro Jahr ca. 100 Millionen Dollar Verlust durch gestohlene Frankier-Maschinen entsteht.

Bisher werden Frankier-Maschinen mit traditionellen Techniken wie Siegeln etc. geschützt. Gedruckt wird üblicherweise mit weniger zugänglichen Druckfarben, etwa fluoreszierender Tinte. Der Aufdruck selbst (engl.: indicium) enthält Angaben über den Porto-Wert, Ort und Datum des Drucks, ggf. Werbe-Logos, den Hersteller der Frankier-Maschine und weitere Informationen.

Die bisherigen Verfahren bieten keinen effektiven Schutz gegen die folgenden Angriffs-Szenarien:

- Manipulation von Frankier-Maschinen sodass kostenlose Aufdrucke erzeugt werden können,
- Kopieren oder Fälschen von korrekten Aufdrucken,
- Benutzung einer Frankier-Maschine durch eine nicht autorisierte Person,
- Diebstahl einer Frankier-Maschine.

In den USA und Kanada wurden daher seit Mitte der 90‘er Jahre Verfahren entwickelt, die eine erheblich größere Sicherheit vor betrügerischem Missbrauch bieten. Diese Verfahren basieren auf den folgenden Techniken:

- Durch neue 2-dimensionale Barcodes (PDF417, Data Matrix, Aztec, …) können 300 Bytes und mehr auf einer Fläche von 6 – 8 cm^2 untergebracht werden. Diese Daten können mit preiswerten Scannern eingelesen und automatisch verarbeitet werden.
- Das ECDSA-Signaturverfahren (elliptic curve digital signature algorithm) bietet nach heutigem Wissensstand bei Signaturlängen von 40 – 50 Bytes eine vergleichbare oder höhere Sicherheit als 1024-bit-RSA (mit einer Signaturlänge von 128 Bytes). Der Standardisierungs-Prozess für ECDSA ist sowohl beim ANSI (X9.62) als auch beim IEEE (P1363) in der Endphase.
- Die kryptografischen Daten und Mechanismen einer Frankier-Maschine — insbesondere die Verwendung des Signaturschlüssels — sowie die geladenen Porto-Kontingente werden in einem speziell geschützten Sicherheits-Modul gekapselt. Jeder legitime Benutzer muss sich durch einen starken Authentisierungs-Mechanismus ausweisen. Das Sicherheits-Modul muss zertifiziert werden nach dem FIPS 140-1 Standard.

In den Aufdruck werden weitere Daten einbezogen, etwa eine Identifikation der Frankier-Maschine, eine Zähl-Variable sowie der aktuelle Stand der Porto-Register der Frankier-Maschine. Der gesamte Aufdruck einschließlich einer digitalen Signatur wird als Barcode kodiert — ein Teil der Informationen wird weiterhin auch in lesbarer Form gedruckt.

Dadurch wird unter anderem Folgendes erreicht:

- Das Fälschen von Aufdrucken ist praktisch unmöglich, da eine korrekte Signatur für gefälschte Daten nicht erzeugt werden kann.
- Das mehrfache Kopieren eines gültigen Aufdrucks kann an Hand des konstanten Zähler-Standes schnell erkannt werden.
- Das Verwenden einer gestohlenen Frankier-Maschine ist wesentlich erschwert: Das Laden von Porto-Kontingenten in das Sicherheits-Modul verlangt eine starke kryptografische Authentisierung. Der Zugang zu den Druckfunktionen ist Passwort-geschützt.

In den folgenden Abschnitten werden die Elemente des Sicherheits-Systems genauer beschrieben.

2. Das Sicherheits-Modul (Postal Security Device)

Das Kernstück der beschriebenen Techniken ist ein Sicherheits-Modul (*PSD*, postal security device), das in die Frankier-Maschine eingebaut wird und das sichere Laden und Verwalten von Porto-Werten auch in einer feindlichen Umgebung ermöglichen soll. Unser PSD ist ein etwa zigarettenschachtel-großes, in Epoxit-Harz eingegossenes Hardware-Modul mit auslesegeschütztem Speicher-Medium und einem Micro-Controller (ARM7) für die kryptografischen Funktionen.

Der weltweit bekannteste Standard für Sicherheits-Module dieser Art ist der /FIPS 140-1/ der amerikanischen Standard-Behörde NIST (National Institute of Standards and Technology). /FIPS 140-1/ beschreibt vier Sicherheits-Level. Der USPS verlangt die Zertifizierung des PSD für Level 3 mit einigen Zusatzanforderungen („Level 3+“).

Die Zertifizierung erfolgt über 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 enthalten die Papiere /Smith et al 1, 2/, die den Zertifizierungsprozess für den Sicherheits-Koprozessor *IBM 4758* beschreiben, das erste Sicherheits-Modul, für das eine Level 4 Zertifizierung erreicht wurde.

2.1 Sichere Ummantelung

Das PSD muss vollständig umgeben sein von einer nicht ablösbaren, undurchsichtigen, manipulations-sensitiven Hülle. Manipulations-Versuche durch Anbohren, Feilen, Sägen oder chemische Auflösung müssen erkannt werden. Außerdem wird gefordert, dass Temperatur- und Spannungs-Schwankungen erkannt werden (Environment Failure Protection). Bei einem Manipulations-Versuch müssen alle sicherheits-relevanten Parameter gelöscht (auf Null gesetzt) werden.

Die Zertifizierungs-Labors verfügen über Ausrüstung, um eine Reihe von Angriffen selbst durchzuführen, etwa Präzisionssägen, Bohrer im $^{1}/_{10}$-mm-Bereich, …

Für das Erreichen dieser Anforderungen wird die Platine unseres PSD mit einer 7 mm dicken, von Serpentinen-Kontakten durchzogenen, Schicht aus Epoxit-Harz umgossen. Auf der Platine sind Spannungs- und Temperatur-Sensoren sowie eine Batterie angebracht, um das Löschen der sicherheits-relevanten Parameter auch bei Abfall der äußeren Spannung zu gewährleisten.

2.2 Software, Schnittstellen

Die wesentlichen Teile der PSD-Software müssen in einer Hochsprache geschrieben sein — in unserem Fall C++. Die Sicherheitspolitik des PSD muss in einem Finite-State-Modell beschrieben werden; die Software muss so dokumentiert sein, dass der Zusammenhang mit dem formalen Modell gezeigt 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 ganz einfach auf die passwort-orientierten Vorstellungen aus /FIPS 140-1/ abbilden.

2.3 Validierung kryptografischer Algorithmen

/FIPS-140-1/ verlangt spezielle Konformanz-Testreihen für die Implementierung von „offiziellen“ FIPS-Algorithmen — z. Zt. sind dies DES, Triple-DES, Skipjack und DSS (Digital Signature Standard). Für uns ergaben sich daraus Tests für unsere Implementierungen von DES, Triple-DES und SHA-1.

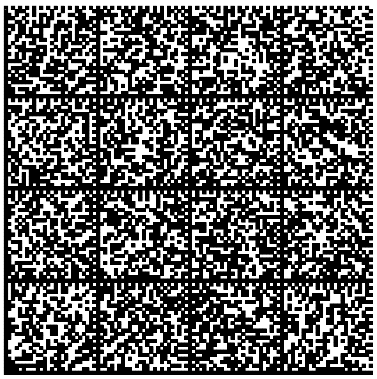
Die Testbeschreibungen umfassen jeweils einige hundert Seiten und sind nicht immer eindeutig, sodass es einige Iterationen kostete, um zu einer akzeptierten Implementierung der Test-Rahmen zu kommen — besser wäre es u. E., wenn das NIST die Test-Rahmen selber stellte. Für die mindestens eben so wesentlichen Public-Key Algorithmen — wie 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 Einzelhandels-Artikeln, Transport-Stücken, Medikamenten, Bibliotheksbüchern, etc. eingesetzt. Einige Barcodes erlauben das Kodieren beliebiger Strings von ASCII-Zeichen oder Binärdaten. Der nebenstehende *Code-128* Barcode kodiert die ersten Worte unsere Zusammenfassung („In den USA und Kanada“). Solche Barcodes heißen eindimensional, da die Information nur in Lese-Richtung kodiert ist.

In den letzten Jahren sind Barcodes entwickelt worden, die die Information in zwei Richtungen kodieren, und daher als zweidimensionale (2D-) Barcodes bezeichnet werden. Die am weitesten verbreiteten 2D-Barcodes sind die Codes *PDF417* und *Data Matrix*. (PDF417 steht für „Portable Data File“, nicht zu verwechseln mit Adobes „Portabel Document Format“.)

2D-Barcodes erreichen erheblich höhere Informationsdichten als traditionelle Barcodes: mit PDF417 kann — abhängig von der Druckqualität, dem eingesetzten Scanner und dem Grad der Fehlerkorrektur (s.u.) — eine Zeichen-Dichte von bis zu 100 Bytes pro cm^2 (binär) erreicht werden. Der obenstehende PDF417-Code enthält die Zusammenfassung dieses Aufsatzes (1075 Zeichen). Mit Data Matrix können theoretisch noch höhere Zeichendichten erreicht werden; nebenstehend das entsprechende Bild.



Durch Fehlerkorrektur-Verfahren kann erreicht werden, dass der Code noch gelesen werden kann, wenn bis zu 40% der Fläche verschmutzt oder abgedeckt sind.

Der USPS unterstützt als Bestandteil des Aufdrucks die 2D-Barcodes *PDF417*, *Data Matrix* und andere, die kanadische Post die Barcodes *Data Matrix* und *Aztec*. Gedruckt wird mit einer Auflösung von 200 dpi. Die Lesefehler-Rate muss unter 0,5 % liegen. Die Zeichendichte beträgt ca. 8 - 10 Bytes pro cm^2 nach Fehlerkorrektur.

4. Postalische Transaktionen und die Struktur des Porto-Aufdrucks

4.1 Porto Value Download, Postalische Register

Die wesentlichen finanziellen Transaktionen einer Frankier-Maschine sind das sichere Laden von Porto-Kontingenten (Fernwert-Vorgabe) und die darauf basierenden Porto-Aufdrucke.

Das Porto-Laden geschieht in folgenden Schritten:

- Der Kunde zahlt einen Geld-Betrag auf ein Konto ein, das entweder dem Frankier-Maschinen-Hersteller oder der Post-Behörde gehört. Die Bank benachrichtigt die Niederlassung des Frankier-Maschinen-Herstellers von der erfolgten Zahlung.
- Der Hersteller erhöht daraufhin den Kontostand eines speziellen Porto-Kontos des Kunden. Gleichzeitig wird ggf. der entsprechende Betrag auf ein Konto der Post-Behörde eingezahlt.
- Der Kunde stellt nun durch Knopfdruck an der Frankier-Maschine eine Modem-Verbindung zu dem Sicherheits-Modul der betreffenden Frankier-Maschine her und leitet einen *Porto Value Download* ein.
- Es findet eine gegenseitige Authentisierung statt; gleichzeitig werden Sitzungs-Schlüssel für die Authentisierung von Nachrichten sowie zum Verschlüsseln von Daten vereinbart.
- Schließlich wird ein dem angeforderten Geldbetrag entsprechendes Porto-Kontingent auf das Sicherheits-Modul der Frankier-Maschine geladen. Gleichzeitig wird das Porto-Konto des Kunden beim Hersteller um den entsprechenden Betrag belastet.

Im Sicherheits-Modul werden dazu die folgenden postalischen Register geführt:

- ein *aufsteigendes Register*: hier werden die Werte aller jemals durch das Modul erzeugten Porto-Aufdrucke aufsummiert,
- ein *absteigendes Register*: dieses Register wird durch das Porto-Laden um den geladenen Betrag erhöht und beim Erzeugen eines Aufdrucks um den entsprechenden Porto-Wert erniedrigt.

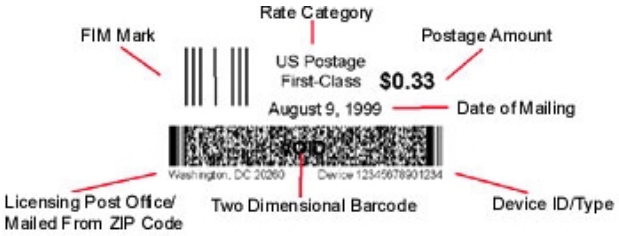
4.2 Weitere Transaktionen

Neben dem Porto-Laden sind weitere Transaktionen spezifiziert, z.B.:

- Das Zurücksetzen von Porto-Kontingenten auf dem PSD (refunding),
- Transaktionen, die den Lebenszyklus des PSD betreffen, wie Inbetriebnahme, Außerbetriebnahme, Kundenzuordnung, Standortwechsel, …

4.3 Porto-Aufdruck, USA

Das nebenstehende Bild zeigt die Struktur und die enthaltenen Daten eines Porto-Aufdrucks, wie er vom USPS für das IBI-Programms (Information Based Indicia) gefordert wird (weitere Informationen enthält die Web-Seite des IBIP, http://www.usps.gov/ibip/).



Gemäß /PCIBI-C/ enthält der Barcode-Teil des Aufdrucks die folgenden Daten:

	Barcode-Daten, USA													
Feld	Indicium Version	Algorithmus-OID	Zertifikats- Serien-Nummer	Geräte-ID (PSD)	Aufsteigendes Register	Portowert	Frankier-Datum	Ursprungs-ZIP	(unspezifiziert)	Software ID	Absteigendes Register	Porto-Kategorie	Signatur (ECDSA)	(unspezifiziert)
Länge [Bytes]	1	1	4	8	5	3	4	4	5	6	4	4	42	?
	49													

Ein Teil dieser Daten wird auch in lesbarer 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 aufsteigenden Registers).

Der (geheime) Signatur-Schlüssel wird im PSD erzeugt und verlässt dieses nicht. Der zugehörige Verifikations-Schlüssel wird von der Hersteller-Niederlassung zertifiziert. Das Schlüssel-Paar hat eine Lebensdauer von etwa einem Jahr.

Das Zertifikat des Verifikations-Schlüssels wird an die postalische Infrastruktur übertragen. Die Prüfstellen müssen auf die Zertifikate aller Sicherheits-Module zugreifen können, für die eine Prüfung durchgeführt werden soll.

4.4 Porto-Aufdruck, Kanada

Gemäß /CPC 2000/ enthält der Barcode-Teil des Aufdrucks die folgenden Daten:

	Barcode-Daten, Kanada														
Feld	Country Code	Indicium Kenner	Algorithmus-OID	Zählnummer	Frankier-Datum	Absende-Datum	Aufsteigendes Register	Absteigendes Register	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[3]
		33														

Ein Teil dieser Daten wird auch in lesbarer Form aufgedruckt. Die Signatur erstreckt sich über die grau markierten Daten sowie 31 Padding-Bytes. Unterschiede zum USPS:

[3] Je nach Schlüssellänge.

- Der Signatur-Schlüssel wird mit dem zugehörigen (öffentlichen) Verifikations-Schlüssel vor jedem Porto-Laden neu erzeugt.
- Der Verifikations-Schlüssel wird — zusammen mit einem Datensatz, der das PSD sowie den Stand der Post-Register zum Zeitpunkt des Porto-Ladens eindeutig beschreibt — an die Hersteller-Niederlassung geschickt.
- Die Hersteller-Niederlassung signiert den Verifikations-Schlüssel und die genannten Daten mit ihrem Signatur-Schlüssel. Ein von der Post-Behörde signiertes Zertifikat für den zugehörigen Verifikations-Schlüssel ist frei verfügbar.
- Die Signatur der Hersteller-Niederlassung wird dem Barcode angefügt.
- Auch die lesbaren Teile des Aufdrucks werden in einem OCR-Zeichensatz (Optical Character Recognition) gedruckt und sind damit automatisch auswertbar. Der Barcode enthält einen MAC-Wert (Message Authentication Code) über diese Daten.

Bei diesem Verfahren muss eine Prüfstelle lediglich über das Zertifikat des Hersteller-Schlüssels verfügen; die Prüf-Infrastruktur kann damit wesentlich einfacher gehalten werden — in den USA muss für jedes PSD ein Zertifikat vorhanden sein. Im Gegenzug sind aber längere Datensätze und damit größere Porto-Aufdrucke erforderlich.

Neben dem hier dargestellten wird in /CPC 2000/ ein weiteres Verfahren beschrieben, das mit einem impliziten Zertifizierungs-Schema der Firma *Certicom* arbeitet (*bullet certificates*) und etwas kürzere Datensätze erlaubt.

5. Infrastruktur des Frankier-Maschinen-Herstellers

Die Post-Behörden der USA und Kanadas stützen sich zu einem gewissen Grad auf die Sicherheits-Infrastruktur des Frankier-Maschinen-Herstellers.

Üblicherweise betreibt jeder Hersteller ein eigenes Datenzentrum für seine Frankier-Maschinen und bietet speziell auf seine Maschinen abgestimmte Zusatzdienste an. Das Datenzentrum versorgt die elektronischen Frankier-Maschinen mit Porto-Kontingenten, auditiert sie in regelmäßigen Zeitabständen und bietet weitere Dienste.

5.1 Weltweite Infrastruktur

Ein weltweit agierender Frankier-Maschinen-Hersteller betreibt typischerweise eine Public-Key-Infrastruktur mit folgenden Hierarchie-Ebenen:

- Die Stamm-Niederlassung des Herstellers 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 Hierarchie-Stufe bilden die PSDs.

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

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

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

5.2 Landes-Niederlassungen

Der USPS verlangt, dass der Betrieb der Datenzentren von Frankier-Maschinen-Herstellern im US-Markt nicht übergeordneten Wurzel-CAs des Herstellers abhängen soll. In diesem Fall könnte der Root-Key des Frankier-Maschinen-Herstellers außerhalb der USA kompromittiert werden und dadurch Dienste für US-Kunden beeinträchtigt werden.

Das Datenzentrum USA hält zu jedem Zeitpunkt zwei unabhängige öffentliche Schlüssel bereit, die von der Wurzel-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.

5.3 Sicherheit als Kostenfaktor

Die Postbehörde muss vermeiden, dass sich das elektronische Porto im Datenzentrum eines Frankier-Maschinen-Herstellers oder in einer Frankier-Maschine erhöht, ohne dass vorher eine Einzahlung in derselben Höhe erfolgt.

Gegenüber dem Endkunden wird dieses Problem durch das PSD gelöst. — Dem Datenzentrum selbst kann jedoch auch nicht bedingungslos vertraut werden. Ein Systemadministrator hat üblicherweise Zugriffsrechte auf alle Tabellen seines Datenbank-Systems und könnte dafür sorgen, dass bestimmte Konten gelegentlich aufgefüllt werden, ohne dass eine entsprechende Einzahlungs-Bestätigung eingegangen ist. Die US-Post hat seit Auflegung ihrer IBIP Spezifikation die Sicherheitsanforderungen immer wieder erhöht, um bekannt gewordenen Missbrauchsfällen zu begegnen. Dazu gehört, dass verschiedene Transaktionen innerhalb des Hersteller-Datenzentrums ebenfalls durch kryptografische Module geschützt werden.

Der USPS kontrolliert darüber hinaus Fertigung und Vertrieb der PSDs sowie das Schlüssel-Management des Herstellers. Dies führt zu erhöhten Kosten, denen kein er-

kennbarer Nutzen für den Endkunden oder den Frankier-Maschinen-Hersteller gegenübersteht — ein typisches Problem in einem stark regulierten Markt-Segment.

6. Postalische Infrastruktur, Prüfprozeduren

Die Postbehörden der USA und Kanadas betreiben Infrastrukturen, die weitgehend unabhängig von den Hersteller-Infrastrukturen sind. Auch diese Infrastrukturen werden Public-Key-Infrastrukturen enthalten; Berührungspunkte ergeben sich dort, wo Verifikations-Schlüssel aus der Hersteller-Infrastruktur für die Verwendung innerhalb der postalischen Infrastruktur zertifiziert werden müssen. Hier wird es voraussichtlich zu Cross-Zertifizierungen auf der Ebene der Hersteller-Niederlassungen kommen.

Zum Schutz vor Frankier-Maschinen-Missbrauch hat der USPS u.a. folgende Regelungen getroffen:

- Die PSDs bleiben Eigentum des Herstellers und dürfen den Endkunden nur leihweise zur Verfügung gestellt werden.
- Nur zugelassene Hersteller dürfen PSDs besitzen. Der Hersteller ist verantwortlich für Betrieb, Wartung, Auswechslung von PSDs etc. Vor Auslieferung an einen Kunden wird das PSD vom Hersteller initialisiert und für den Kunden autorisiert.
- Jeder Betreiber einer IBI-Frankier-Maschine muss sich beim USPS registrieren lassen. Die Anmeldung enthält Angaben über das zu verwendende PSD, das Heimat-Postamt, bei dem die frankierte Post aufgegeben wird, … Jede Änderung muss sofort mitgeteilt werden.
- Die Registrierung kann widerrufen werden, wenn es Anzeichen für eine missbräuchliche Verwendung gibt, wenn der Betreiber keine ausreichende Kontrolle über den Betrieb der Frankier-Maschine ausübt, wenn 12 Monate lang kein Aufdruck erzeugt worden ist, …
- Der geladene Porto-Wert muss alle 3 Monate auf Null zurückgesetzt werden, um dem Hersteller eine Konto-Kontrolle zu erlauben. Alle 6 Monate muss dem Hersteller ein auf der Frankier-Maschine erzeugter Aufdruck zur Qualitäts-Kontrolle zugeschickt werden.
- Ein Defekt, Verlust oder Diebstahl eines Geräts muss dem Hersteller sofort gemeldet werden.

Die Struktur des Aufdrucks ermöglicht es, die Aufdrucke einer Reihe von Prüfungen zu unterziehen, etwa durch:

- Prüfung zufälliger Stichproben,
- Selektives Prüfen bei vorliegendem Verdacht,
- Vollständiges Screening.

Einfache Missbrauchs-Fälle können an den Abgabestellen offline kontrolliert werden, etwa das Fälschen von Aufdrucken, das Verwenden eines gestohlenen, verlorenen oder

nicht registrierten Geräts, die Vervielfachung eines gültigen Aufdrucks, die Abgabe an einer falschen Abgabestelle.

Weitere Prüfungen wären an zentralen Sammel- oder Verteilstellen durch überregionale Verknüpfung von Datenbeständen denkbar. Allerdings können hier auch Datenschutz-Belange tangiert werden.

7. Kryptografische Mechanismen

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

- Für Signaturen und Authentisierung innerhalb der Hersteller-PKI wird das RSA-Verfahren mit SHA-1 gemäß /PKCS #1/ und /IEEE P1363/ verwendet. Die Schlüssellänge beträgt für das PSD 1024 Bits, für alle anderen Instanzen 2048 Bits.
- Für die Authentisierung zwischen PSD und Hersteller-Infrastruktur wird X.509 *three-way-authentication* in Verbindung mit RSA-Authentisierungs-Schlüsseln verwendet.
- Zertifikats-Requests werden nach /PKCS #10/ formatiert.
- Für den Austausch von Sitzungs-Schlüsseln zwischen PSD und Hersteller-Infrastruktur wird Diffie-Hellman gemäß /ANSI X9.42/ verwendet.
- Für die Integrität der zwischen PSD und Hersteller-Infrastruktur übertragenen Daten wird SHA-1 und HMAC gemäß RFC 2104 verwendet.
- Für die Verschlüsselung von Datenfeldern während einer Verbindung zwischen PSD und Hersteller-Infrastruktur wird Triple-DES verwendet. Tatsächlich werden nur wenige Daten verschlüsselt — die für das PSD zentralen kryptografischen Dienste sind Authentisierung und Daten-Integrität.

Für das Signieren der Barcode-Daten wird das ECDSA-Verfahren gemäß /ANSI X9.62/ verwendet. /PCIBI-C/ und /CPC 2000/ enthalten jeweils eine Liste zulässiger Kurven aus /ANSI X9.62/. Wir werden uns wahrscheinlich für eine Kurve über GF(2^{163}) mit zufällig erzeugten Punkten entscheiden (Schlüssellänge 163 Bits; Signaturlänge 42 Bytes).

Im Vergleich zu RSA oder DSA sind bei ECDSA für ein vergleichbares Sicherheits-Niveau erheblich kürzere Signaturen erforderlich. Die nebenstehende Tabelle gibt einen Überblick über die vergleichbare Sicherheit verschiedener kryptografischer Verfahren in Abhängigkeit von der Schlüs-

Schlüssellängen vergleichbarer Sicherheit nach /Lenstra, Verheul/			
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

sellänge sowie der zu einem bestimmten Zeitpunkt voraussichtlich zur Verfügung stehenden kryptanalytischen Hilfsmittel (Rechner-Kapazität, theoretische Fortschritte).

8. Offene Frankier-Systeme (PC-Frankierung)

In den USA und Kanada sind auch sogenannte *offene* Frankier-Systeme spezifiziert worden, mit denen Privatpersonen oder kleine Firmen Porto-Aufdrucke auf einem PC-Drucker erzeugen können. Hierfür werden ebenfalls 2D-Barcodes und digitale Signaturen verwendet. Das Porto-Laden erfolgt in diesem Fall über das Internet. Die Firma *e-stamp* verwendete ein PSD in Form eines kryptografisch 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-Datenbank-Systems bei *stamps.com* realisiert. Beide Systeme sind von der US-Post zugelassen, allerdings mit Auflagen, die für viele Benutzer nicht akzeptabel sind.

Während Frankier-Maschinen mit fluoreszierender Tinte drucken, die einen gewissen Schutz vor schlichtem Kopieren bietet, sind Frankier-Aufdrucke aus Laserdruckern oder Tintenstrahldruckern einfach zu reproduzieren. Die IBIP-Spezifikation für offene Frankier-Systeme sieht daher vor, im Aufdruck eine Reihe weiterer Merkmale aufzunehmen und unterschreiben zu lassen, die ein Kopieren wenig sinnvoll erscheinen lassen. So wird z.B. eine knappe Gültigkeitsdauer definiert. Diese muss zusammen mit der Postleitzahl des Empfängers im Aufdruck enthalten sein und vom PSD unterschrieben werden.

Das Kopieren eines gültigen Frankier-Aufdrucks ist dann nutzlos: Post-Stücke mit kopiertem Aufdruck 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 Porto-Aufdruck abgeschickt werden muss. Außerdem verlangt die US-Post, dass nur solche Empfängeradressen angegeben werden dürfen, die in einem von der US-Post bereitgestelltem Adressverzeichnis enthalten sind. Auslands-Adressen sind überhaupt nicht enthalten. Durch die hohe Mobilität in den USA werden diese Restriktion für Kunden noch unbequemer.

Hier zeigt sich, dass der Interessenkonflikt zwischen Sicherheitsbedürfnis der Postbehörden und Kostenminimierung der Frankier-System-Hersteller bei offenen Frankier-Systemen verschärft auftritt. Die Risiken für die jeweilige Postbehörde sind noch größer, wegen der einfacheren Kopierbarkeit der Abdrücke und weil die Datenzentren der Frankier-System-Hersteller am Internet betrieben werden müssen, was weitere Angriffs-Szenarien ermöglicht.

Technisch gesehen muss die Integrität der Kundenkonten auf Applikations-Ebene gesichert werden — das ist bis heute in fast keinem Datenzentrum im kommerziellen Bereich realisiert. In /Bleumer/ wurde gezeigt, wie in einem Frankiersystem die Integrität von elektronischem Porto auf Applikations-Ebene durchgängig kryptografisch 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 die Streichung von der NASDAQ Liste.

Die Deutsche Post will im Jahr 2001 ebenfalls ein offenes Frankiersystem anbieten und versucht, den beschriebenen Interessenkonflikt von Anfang an dadurch zu entschärfen, dass sie beim Betrieb von Datenzentren für offene Frankier-Systeme keine Mitbewerber zulässt, sondern ihr Monopol bei der Beförderung von Briefen auf den Verkauf von elektronischem Porto ausdehnt (/DPAG/).

Literatur

/ANSI X9.42/	Public Key Cryptography For The Financial Services Industry: Agreement of Symmetric keys on Using Diffie-Hellman and MQV Algorithms; Working Draft, Oct 2, 1998
/ANSI X9.62/	Public Key Cryptography For The Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA); Working Draft, Sep 20, 1998
/Bleumer/	G. Bleumer: Secure PC-Franking for Everyone; Proceedings of EC-WEB'00, LNCS 1875, Springer-Verlag, Berlin 2000, 94-109
/CPC 2000/	Canada Post: Digital Postage Indicia Standard for Canada Post; Draft Version 2.0, März 2000
/DPAG/	Deutsche Post AG : Voraussetzungen zur Einführung von Systemen zur PC-Frankierung ; Version 1.1, 20.09.2000 (→ http://www.dpag.de/pc-frankierung/)
/FIPS 140-1/	Security Requirements for Cryptographic Modules; Version 1, Jan 1994
/FIPS 140-2/	Security Requirements for Cryptographic Modules; Version 2, 1999
/IEEE P1363/	IEEE P1363; Standard Specifications for Public Key Cryptography; Draft Version 13, Nov 1999
/Lenstra, Verheul/	A. K. Lenstra, E. R. Verheul: Selecting Crytographic Key Sizes; Oct 1999 (→ http://www.cryptosavvy.com/)
/PCIBI-C/	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, Januar 1999 (→ http://www.usps.gov/ibip/)
/Pintsov et al/	L. A. Pintsov, S. A. Vanstone: Postal Revenue Collection in the Digital Age; 1998 (→ http://www.cacr.math.uwaterloo.ca/)

/PKCS #1/	RSA Laboratories PKCS #1: RSA Cryptography Standard; Version 2.0, Oct 1, 1998
/PKCS #10/	RSA Laboratories PKCS #10: Certification Request Syntax Standard ; Version 1.0, Nov 1, 1993
/RFC 2104/	HMAC: Keyed Hashing for Message Authentication; Feb 1997
/Smith et al 1/	S.W. Smith, S. Weingart: Building a High Performance, Programmable Secure Coprocessor; Computer Networks 31, April 1999 (→ http://www.research.ibm.com/secure_systems/scop.htm)
/Smith et al 2/	S.W. Smith, R. Perez, S. Weingart, V. 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 et al/	J. D. Tygar, B. S. Yee, N. Heintze: Cryptographic Postage Indicia; 1996 (→ http://www-cse.ucsd.edu/users/bsy/papers.html)
/X.509/	ITU-T Recommendation X.509, Information technology — Open Systems Interconnection — The Directory: Authentication framework; Version 3, Aug 1997