Cryptographic postage stamping

ISSE

Cryptographic Postage Stamping

Public key cryptography was discovered in the 1970s. Among other things, it provides strong authentication of digital information without the need to distribute pieces of secret information in advance.

HEINRICH KRÜGER-GEBHARD

I can therefore get proof of origin without having to agree upon a mutual secret passphrase in advance. As the price for this, public keys must be acquired authentically. This requires a public key infrastructure, where trust can be traced upwards up to commonly trusted authority.

In recent years, public key cryptography has received a lot of interest in connection with buzz-words like e-commerce, m-commerce, electronic banking and secure internet communication. But there are other applications which receive much less public attention and nevertheless may turn out to be as pervasive for our future every-day life.

We describe an application that is quite interesting in itself and also features some techniques that may turn up in many other present and future IT-based systems.

Postage Meters

With the advent of modern communication techniques like fax, e-mail etc., traditional mail delivery systems might appear outdated. This is not so:

In 1998, the German Deutsche Post AG delivered 20 billion letters and 4,5 billion parcels, at an annual growth rate of about 5 %. In the same year, the US Postal Service delivered about 197 billion mail pieces – nearly 540 millions a day. About 80% of all letters are processed by computer based systems. Mostly, this includes an automated metering machine which, instead of attaching an ordinary stamp, prints a special postage mark called indicium. In the USA, there are about 1,5 million postage meters, which process a total postage value of about 20 billion dollars every year.

Traditional postage meters are vulnerable to a number of attacks. e.g.: Metering machines may be (and have been) manipulated, such that imprints are generated without payment.

Legitimate imprints may be copied or forged. Postage meters may be used by unauthorised personnel. Postage meters may be stolen and abused at the cost of the legitimate customer. Postal authorities actually suffer quite significant losses due to postage meter abuse and fraud: In 1996, 82 000 postage meters were reported stolen in the United States. It is estimated that the US Postal Service loses about 100 million dollars of revenue a year due to stolen postage meters.

In recent years, new methods of revenue protection became possible by combining the following key techniques:

- Elliptic curve cryptography is a relatively new type of public key cryptography that yields high security levels at significantly lower computational effort than traditional techniques like RSA.
- New 2-dimensional barcodes enjoy the benefits of traditional barcodes – such as easy printing, flexibility, automatic reading and processing with inexpensive devices – while encoding much higher volumes of data.
- Cryptographic modules serve as a secure storage of sensitive data as well as a cryptographic co-processor. They can be built in a way that effectively prevents unauthorised reading or changing of the stored data and programs – even in the presence of determined

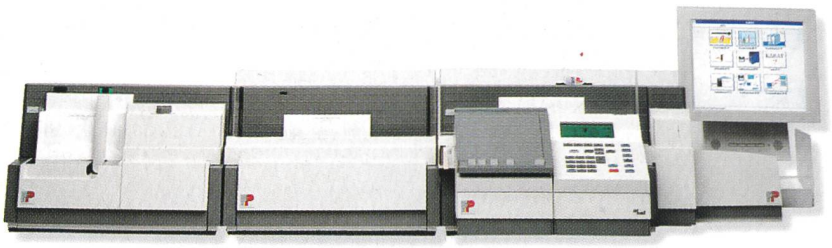

Fig. 1. An automated metering machine which, instead of attaching an ordinary stamp, prints a special postage mark called indicium.

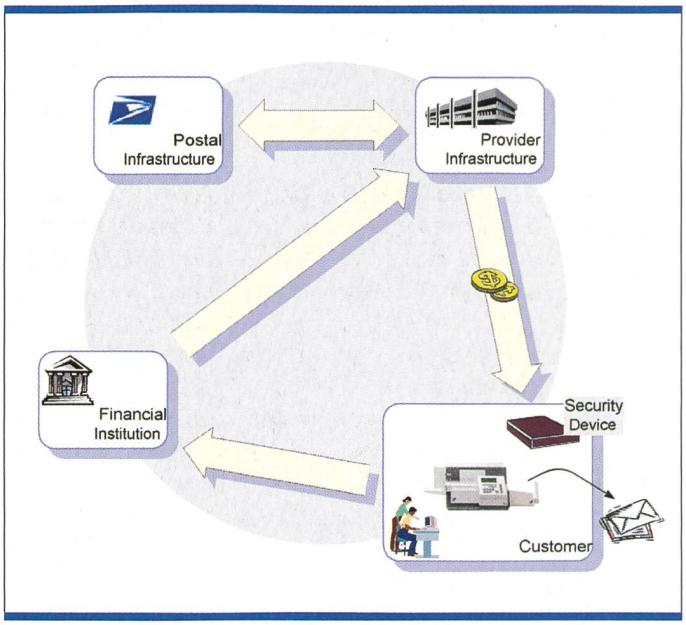

Fig. 2. The operation of electronic postage meters is backed by an elaborated infrastructure.

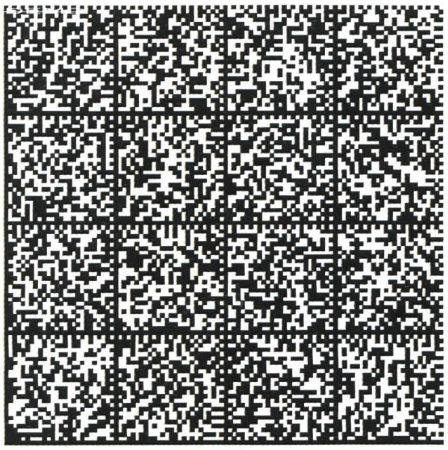

Fig. 3. The barcode DataMatrix encodes 1075 characters.

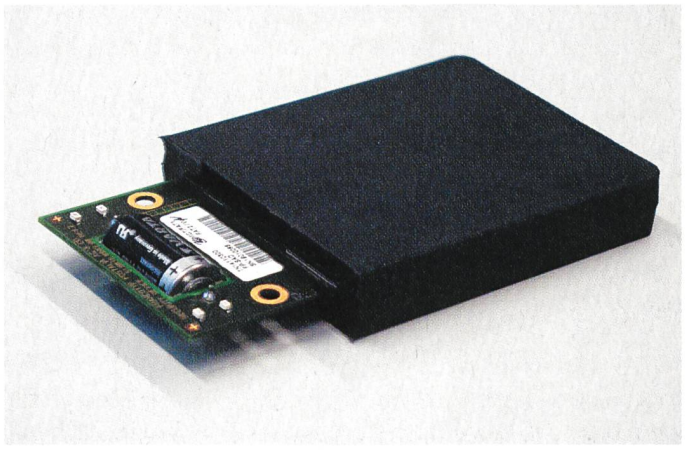

Fig. 4. For Francotyp's postage meters, the security device is a cigarette-pack sized box.

attacks like drilling, probing, dissolving in acid etc.

The postal authorities of the USA and Canada were the first to specify frameworks for cryptographic metering systems based on these techniques. Other countries are expected to follow in the near future. To achieve better protection from indicium forging and postage meter abuse, electronic signatures are applied to link postal information to individual customers. This way, within a few years, every single household will most likely touch on public key cryptography daily.

Francotyp-Postalia AG (FP) is a European market leader for mail processing solutions. To serve the North American markets, FP has developed a cryptographic module – called postal security device (PSD) – conforming to the US and Canadian specifications. In addition, FP is in the process of building a worldwide infrastructure to support these devices. Rohde & Schwarz SIT GmbH has developed the cryptographic mechanisms of the PSD and has assisted in the security evaluation process.

Infrastructure

The operation of electronic postage meters is backed by an elaborated infrastructure. This is to guarantee adequate revenue for the delivered mail pieces to the postal service and at the same time assure the customer that he is served what he paid for. Postage meters are owned by a franking service provider and leased to the end-customers. To generate indicia, the security device within the postage meter has to be loaded with an appropriate postage value. To achieve this, the following steps have to be followed:

The customer makes a payment to a bank account of the provider or the postal authorities and indicates this to the provider. The provider checks the payment. The customer then establishes a modem connection between the provider's data center and the postage meter. Provider and security device check their mutual identity by strong cryptographic techniques. After this, the provider loads the appropriate postage value into the security device. Within the security device, the postage value download results in an increase of an internal postage register.

2D-Barcode and the Structure of the Indicium

Traditional barcodes have been used to label retail articles, medication, library books etc. for decades. Some of them allow the coding of arbitrary ASCII strings or even binary data. The sample besides codes a 22-character ASCII string with a barcode of type Code-128. Barcodes like this are called 1-dimensional, because the information is coded in the reading direction. They are typically read with infrared laser scanners.

In recent years, barcodes have been developed that encode information in two directions (2D barcodes). Among the better known of these are the codes PDF417 and DataMatrix. These barcodes achieve much higher data densities. The DataMatrix encodes 1075 characters. 2D-Barcodes are read by laser scanners or charge coupled devices. This is inexpensive off-the-shelf equipment costing in the range of 10 to 20 Euro. Error correction techniques are employed such that a 2D-barcode can be read even with 40% of the surface being covered.

Using 2D-barcodes as part of the indicium, it becomes possible to link customer data, the current value of the security device's internal postage registers and other data and let them sign digitally inside the security device.

This way, the following is achieved:

- An indicium can not be forged, as it is impossible to create a digital signature without knowing the security device's hidden private key.
- Copying a legitimate indicium is of limited use, because it is linked to the specific data of the original mail piece.
- A postage meter reported stolen will no longer receive postage value downloads, and therefore will be useless once the postage contingent inside its security device is exhausted.
- An employee who wishes to perform a transaction with the security device, has to authenticate himself. This way, abuse by unauthorised personnel may be tracked more easily at the customer's side.

Elliptic Curve Cryptography

Public key cryptography and digital signatures were introduced in the 1970's by W. Diffie, M. Hellman, R. Merkle, R. Rivest and others. The most widely employed signature algorithm over the past 20 years has been RSA (Rivest-Shamir-Adleman), with the NIST's[1] DSA (digital signature algorithm) gaining popularity in the 1990's. Both require a signature length of 128 Bytes or higher for a security level considered adequate today.

Elliptic curves are a mathematical structure that has been investigated for centuries. They played an important role in the recent proof of the famous Fermat's last Theorem by Andrew Wiles. In 1984, it was proposed to use elliptic curves for public key cryptography. This approach

[1] The American "National Institute of Standards"

received a lot of attention in the academic world throughout the 1990's.
Digital signatures based on elliptic curves have two decisive advantages over the traditional algorithms:
- They achieve the same security level as RSA or DSA with a signature length of about 40 Bytes, with the gap still widening in the future.
- Generating and verifying signatures requires less computing resources.

As the cryptographic community has good reasons to be conservative on these issues, RSA and DSA – having been investigated for a long time – are still the most popular algorithms for now and the near future. But elliptic curves are gaining ground, especially for applications with resource limitations, like smart cards, mobile radio etc.
For the US digital indicium specification, the barcode part of the indicium contains 50 Bytes of data. The digital signature takes another 42 Bytes making up for a total length of 92 Bytes. For RSA, the figure would be 178 Bytes total, i.e. the barcode would have to be nearly twice as large.

Postal Security Devices
At the heart of the postage meter lies a cryptographic module, called Postal Security Device. The security device provides a secure storage medium for the indicium signature key and other authentication keys, as well as for postage value parameters and other data items.
For Francotyp's postage meters, the security device is a cigarette-pack sized box cast in epoxy resin, endowed with tamper proof storage and an ARM7 micro controller to perform all relevant cryptographic operations.
The internationally accepted standard for modules of this kind is the NIST's FIPS 140-1 (Federal Information Processing Standard 140-1) of 1994. The postal authorities require a level 3 certificate with some additional requirements ("level 3+"). The security evaluation is done by a NIST accredited laboratory – these have been exclusively American laboratories so far, but this is currently going to change. Properties under evaluation include:
- Physical security: The security device has to be wrapped in an opaque coating with tamper evidencing circuitry. Every attempt to cut or drill through the coating, to dissolve the coating in acid etc. must result in the erasure of all security relevant data within the device.
- Software security: The behaviour of the module must be specified in a formal finite state model. The security relevant parts of the software have to be written in a high level language.
- Controlled interfaces with role based authentication: The interface must consist of a set of distinguishable services protected by role-based authentication.
- Validation of algorithms: FIPS 140 requires the validation of the implementation of relevant cryptographic algorithms. 4

Zusammenfassung

Kryptografisches Stempeln

Die Kryptografie mit Public Keys wurde in den 70er-Jahren entdeckt. Sie bot unter anderem leistungsfähige Authentifizierung digitaler Information, ohne dass vorher geheime Informationen ausgetauscht werden mussten. Somit ist es möglich, einen Ursprungsbeweis zu erhalten, ohne zuvor ein beiderseitiges, geheimes Passwort vereinbaren zu müssen. Der Preis dafür besteht darin, dass Public Keys authentisch erworben werden müssen. Dazu ist eine Public-Key-Infrastruktur erforderlich, wobei Vertrauen aufwärts bis zu einer allseitig als vertrauenswürdig betrachteten Stelle nachverfolgt werden kann. In den letzten Jahren hat die Public-Key-Kryptografie viel Interesse in Verbindung mit Begriffen wie E-Commerce, M-Commerce, Electronic Banking und sicherer Internet-Kommunikation gewonnen. Es gibt jedoch andere Anwendungen, die zwar nicht so viel öffentliche Aufmerksamkeit erregen, die sich aber trotzdem als ebenso beherrschend für unser zukünftiges Alltagsleben erweisen könnten. Wir beschreiben eine Anwendung, die selbst sehr interessant ist, und die auch einige Techniken verwendet, die in vielen derzeitigen und zukünftigen IT-Systemen auftauchen könnten.

Heinrich Krüger-Gebhard *studied mathematics and physics. He received the doctor title in mathematics in 1984 with a thesis on partial differential equations. After three years of implementing a finite element package, he entered the software industry in 1987. Here, he worked as a developer, systems engineer and project manager on simulation systems and computer based logistics. Since 1998, he has worked as a project manager for Rohde & Schwarz SIT GmbH, a company specialised in communication security and cryptography. He has managed cryptographic projects for satellite radio, professional mobile radio and postage metering machines. Email: Heinrich.Krueger-Gebhard@sit.rohde-schwarz.com*
Heinrich Krüger-Gebhard will be speaking at ISSE 2001 – Information Security Solutions Europe, from 26-28 September 2001 at QEII Conference Centre, London