A proposal for a cryptographic digital stamp to fight fraud.

Jason Bercher

Faculty of Computer and Information Science
University of Ljubljana, Slovenia
jb4966@student.uni-lj.si

Abstract.
For almost two centuries, people have been exchanging letters through post companies, against a small amount of money called postage fee. The proof that the fee was really paid, is the stamp appended to the letter. But since it just consists in sticky printed paper, it is easy to forge them. Using today’s technologies and cryptographic properties, how can we protect postal companies from fraud?

Keywords: postage, stamps, forgery, cryptography

1 Introduction

Traditional postage stamps have been used for a long time now. It was in 1680, when the British merchant William Dockwra created the *London Penny Post*, that the concept of paying to send a mail was introduced. It cost one penny, and the letter was hand-stamped directly on the envelope, confirming the payment of the postage fee. Even though the idea of using affixed postal stamps was firstly suggested by the Slovene Lovrenc Košir in 1835 [1], it’s only in 1840 that it really begun to be used. The *Penny black* was available in the United Kingdom, it cost one penny, and could be used to send a letter up to 14 grams in the UK [2]. Also, a postmark was applied by the post office to prevent re-use of the stamp.

Even though they are cheap and simple, it is possible for anyone with printing skills to forge these stamps, as they don’t include so many protections by design. Also, the current system provides the possibility to get a postage meter, but these are not revocable and many of them are reported lost or stolen. So how would it be possible to prevent anyone from forging postage stamps or misusing postage meters?

The answer is in cryptographic systems.

This paper will present a proposal for a new postage system that brings protection of forgery, emitter or/and recipient privacy and integrity, and monitoring of postage meters. Of course there are many properties that can be improved or added later, but this is just a sketch to switch from an ancient out-dated system.

2 Requirements for a digital stamp

The ideal digital stamp should fulfill these requirements as much as possible:

- Unforgeable. It should be impossible for someone who doesn’t pay the postage fee to forge a stamp.
- Prevents second use. A stamp that has been reapplied should return the mail to the initial sender.
- Optional privacy. The sender and receiver addresses and details should be unrecoverable for anyone who intercepts the mail.
- Possibility of revocation. The material used for encryption, decryption, creation or verification of postage stamps should be revocable. It means that if an equipment, data such as certificates or keys are compromised, it should be possible to disable these.
- As much as possible, a network or a power outage should not prevent the system from delivering, checking, or decrypting stamps.
- If possible, a decentralized system should be used.

3 Digital stamp Establishment Steps

3.1 Self-printed stamp, using online means

Following is a basic concept of how to provide protection of postage forgery and protection of the emitter and recipient privacy. Of course, this doesn’t provide physical protection of the mail, so one may still open letters and read the content. Only the identity of the sender and the recipient are protected.

When the postage stamp is printed by the emitter:

- The emitter requests a *Mail ID* by sending details for the mail (recipient address, return address, name, contact details, etc.) to the post.
- The post acknowledges request, emits a *Mail ID* and now demands payment of the postage fee.
- The emitter pays the postage to the post.
- The post checks payment with the payment platform, and sends *Mail Signature* which contains *Mail ID* and the hash of the mail details, both signed with the post signing private key and certificate. The post also generates a public and private key for this *Mail ID* and sends the public key to the emitter.
- The client encrypts details using the public key he just received, and generates the digital stamp that includes:
    - *Mail ID*
    - *Mail Signature*
    - Encrypted details
- The client can now print the digital stamp, affix it to the mail, and send it.

When the mail reaches the post office, workers can decrypt the recipient address using the private key associated with the *Mail ID*, and can also check if the postage was indeed paid, by checking the *Mail Signature*.
It is recommended to use intermediary certification authorities and certificate revocation lists in case of a security compromise at the post office or regional office.

The *Mail ID* is associated to the mail's details and the key set to encrypt and decrypt the mail's details. So in case the digital stamp is copied, one has no way to modify the stamp and change the destination address.

In case of mail interception, nobody except the post is able to decrypt the details.

3.2 Purchased stamp

If someone wants to use digital stamps (or if the post bans the traditional stamps) but does not possess a computer, printer, online access or doesn't want to use the first mean for any reason, purchasable stamps may be a possibility.

There are two possibilities:

- Stamps are printed widely by printing houses, and distributed to sale points afterwards.
- Stamps are printed directly at the sale point, when someone makes an order.

The first option offers more simplicity, costs less, and doesn't require any knowledge from either the employee at the sale point, and the person looking to get stamps.

On the other hand, the second option offers more security. Because the printing house would need to get the post signing private key, it means that they should be trusted. Again, use of intermediary certification authorities and certificate revocation lists are recommended in this case.

Also, it is impossible to use sender and recipient's addresses privacy in the case of purchased stamps.

3.3 Offline stamp establishment

Offline needs are quite uncommon today, but may be needed for post offices in case of network outage.

If the mail is sent directly from the post office, and the stamp is established there, the problem is that it's impossible for the post office to communicate the key set used to encrypt and decrypt the mail's details. It's also impossible to use payment platforms and credit cards.
But the signing private key and certificate are most likely already stored in the post office systems, so establishing new digital stamps would still be possible. The problem arises further, when sorting offices or delivering offices need to check the destination address. If the originating post office couldn't communicate the key set, then it's impossible to decrypt the mail's destination address. In this case, mail should not be sent out of the office until network resumes.

Another case is when the post office picks up the mailbox and needs to send all these mails.
In this case, the post office can still check the veracity of a digital stamp, because it already possesses the public key used to check the signature. The problem arises when it comes to decrypt the mail's details, because each mail has its own key set.
Because there is always a delay between the creation of the stamp and the reception of the letter

by the post office (usually one day), we can think of a solution: post offices should regularly synchronise their list of new registered mails, so that in case of a network outage, key sets are already saved.

In case of sale points, they can still buy pre-printed stamps in prevision of a network or electricity outage. For individuals, they still can go to sale points or post offices, or use another option (cellular network, office computer, etc.)

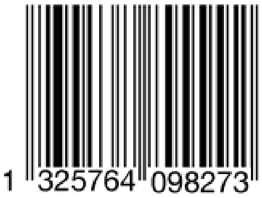
4 DIGITAL STAMP ENCODING

In the last chapter, we have seen what the content of a digital stamp is and how this content is established. But before actually printing this “content” on the mail, it shall be encoded in some way so that it is easy and fast to read the content afterwards.

There are a few possibilities in order to encode data into a visual code. In our case, the requirements are the following:

- The code should support large capacities to encode all the data we need and predict future use cases.
- The code should provide error correction. Because double reading takes a lot of time, it should be avoided.
- The code should have quite the same physical size as traditional stamps.

The first possibility was to use traditional one dimensional bar codes, such as EAN code below.



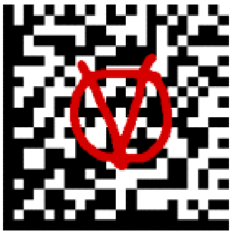
But these codes cannot transport so much data, usually between a few bytes to a hundred.
This is the reason why two dimensional bar codes should be used. Following are the three most popular 2D bar codes standards [3].

QR-Code:
Probably the most popular code now, because it is free to use, it has a flexible physical size, a high fault tolerance and fast readability.

Datamatrix Code:
These codes are rather small, widely used to label small products, and are not so different from the QR-code.

PDF417 Code:
These codes are used in multiple applications that require to store a very large amount of data. But they also have a physical format that doesn’t fit with traditional postage stamps.

Both QR-Code and Datamatrix code are very suitable for our application, because they can carry enough data, and can be fitted in traditional stamps. They also provide very good error correction. For example, the Datamatrix code below was tagged in a violent vendetta, but it still can be read perfectly fine.



Even though these two codes are similar, the Datamatrix can actually encode more data than the QR-code, because the control zone is smaller. But the QR-code is by design supposed to read codes faster (QR meaning *quick response*). In practice, the reading time is nearly the same for both codes. [4]

5 Conclusion

The motivation behind cryptographic stamps is strong, because post companies are losing a lot of money from fraud. In this paper, we have seen how it was possible to create a new, cryptographically based, stamp and postal system. This shall prevent anyone from forging illegal stamps, as well as it shall bring new protections such as sender and recipient privacy.

References

[1] Biography of Lovrenc Košir, from Jan Kosniowski, http://www.stampdomain.com/stamp_invention/kosir.htm

[2] Postage stamp, https://en.wikipedia.org/wiki/Postage_stamp#History

[3] www.scandit.com, https://www.scandit.com/types-barcodes-choosing-right-barcode/

[4] QR code https://en.wikipedia.org/wiki/QR_code