Acta Informatica Pragensia, 2015, 4(3): 302–309
DOI: 10.18267/j.aip.76
Peer-reviewed paper

Verifiable Distribution of Material Goods Based on Cryptology

Radomír Palovský*

Abstract

Counterfeiting of material goods is a general problem. In this paper an architecture for verifiable distribution of material goods is presented. This distribution is based on printing such a QR code on goods, which would contain digitally signed serial number of the product, and validity of this digital signature could be verifiable by a customer. Extension consisting of adding digital signatures to revenue stamps used for state-controlled goods is also presented. Discussion on possibilities in making copies leads to conclusion that cryptographic security needs to be completed by technical difficulties of copying.

Keywords: Digital signature, Verifiable distribution, Material goods, QR code, Revenue stamp.

1 Introduction

Distribution of consumer goods in a real world suffers from counterfeiting of desirable brands or of goods in state-controlled licensed flow, mostly with an excise tax. Many organizational, repressive law enforcement methods are used to reduce amount of counterfeiting. In this paper, I present a method based on cryptography which is able to provide customers with sufficient certainty about the producer of this particular item.

The problem of proving the authorship of the document was dealt with in the eighties. (Baker & Hurst, 1998) Various methods of digital signatures have been developed as a solution. (Smid & Branstad, 1993) (Schneier, 2007), (Pfitzmann, 1996) These methods change natural uncertainty about who the creator of the document is, in situation when anybody can imitate anything at almost zero cost, to a pretty sureness about the authorship of the digitally signed document. During the years digital signature became real equivalent of handwritten signature and is widely accepted not only as a proof of communication between persons or businesses but also as a proof of communication between the state and some other subject. In particular, Czech Republic approved Law on digital signature in 2000, and soon after that papers were written about how digital signature would change our businesses (Hrubý & Mokoš, 2001) or document processing (Tvrdíková, 2003).

I would like to propose, that the same principles that lead to the acceptance of digital signatures in the digital world, can be used in the material world, where material goods are being distributed. A digitally signed document consists of two parts. One part is the document itself. The second part is digitally signed hash of the document. Hashing of documents

* Department of Information and Knowledge Engineering, Faculty of Informatics and Statistics, University of Economics, Prague, nám. W. Churchilla 4, 130 67 Praha 3, Czech Republic
✉ palovsky@vse.cz

changes a document of an arbitrary length to a hash value of a fixed length and signing of the hash clearly and indisputably declares the author of document. There is no strict constraint on the length of the digital signature. Usually, this is only a fraction of the document's length, and in practice, adding to the length makes not a problem. This paper does not mention legal aspects of digital signing of material goods, only the technical architecture is presented.

2 Signing of a material goods

Usage of cryptography for signing the goods in the material world is quite different. There is some information, which producers of goods individually print on labels of consumer goods, but amount of this information is quite limited. Examples of such are serial numbers of electric appliances or "used by date" of food. Digital signature of material goods would be something different then simple human readable information. At first, it would not be verifiable without technical equipment, so the signature needs to be a machine readable code. Second, amount of information must be much greater than simple serial numbers or human readable date, so we need to effectively put a lot of data in a small area.

One very good machine-readable code with high space efficiency is QR code, designed for the automotive industry in Japan and later adopted as the ISO/IEC 18004:2000 standard and revised as the ISO/IEC 18004:2006 standard. (ISO 18004, 2006) Possible resolution and formats of QR codes have many variants and the codes are able to store information till 2933 8bit bytes in its largest version (Version 40) and lowest ECC correction level (Level L).

Fig. 1. *An example of QR code. Source: Author.*

Information which could be signed is the unique serial number, which is assigned to each particular product item. The serial numbers used on products are usually short numbers, from cryptographic point of view. They usually consist of 10 or less digital numbers and of some letters, mostly less than 4. That makes less than 35 bits of entropy. We can enlarge the entropy of signed information by concatenating the human readable serial number with a random number. A full length of the signed message should be greater than desired security level; this level for short term use is recommended as 80 bits.

An algorithm recommended for digital signature should be of very good efficiency of security against the signature length. One of the best signatures is Boneh Lynn Shacham signature scheme (Boneh, Lynn, & Shacham, 2004). BLS has signature length 2 times security length. That means, if we need 80 bits security (at present security level, which is sufficient for short-term safety) a BLS signature will be of 160 bits length. Moreover, the BLS signature scheme is provably secure in the random oracle model and there has been quite a lot of its cryptanalysis in models without random oracle, since its invention (Zhang et al., 2011), (Boneh & Boyen, 2004). The comparison of a signature length of BLS, DSS and RSA provide

Zhang (Zhang et al., 2011) and it is BLS - 160 bit, DSS - 320 bits and RSA - 1024 bits. The main drawback of BLS scheme is the fact, that not every system uses it.

Next best, with respect to the efficiency against the signature length, currently used algorithm is the elliptic curve digital signature algorithm (ECDSA) (Johnson, Menezes, & Vanstone, 2001). Precisely, the signature length is the same as in case of ordinary DSS for the same security, but the ECDSA has shorter keys. It was accepted in 1999 as an ANSI standard, and was accepted in 2000 as IEEE and NIST standards. It was also accepted in 1998 as an ISO standard. Unlike an algorithm based on the ordinary discrete logarithm problem and the integer factorization problem, no sub exponential time solution is known for the elliptic curve discrete logarithm problem.

3 Distribution of certificates

A digital signature alone is not enough. We need a proof that the public key for the digital signature belongs to the subject which claim is ownership. The certificate is such a proof; it is the public key together with ownership information digitally signed by a certification authority. But the certificate is a quite large object for small area on QR code. Encoding a certificate into limited space of the QR code will consume lot of (perhaps all) available bytes. The certificates scheme X.509 was not designed with space efficiency in mind. But we need the certificate to prove that digital signature is really issued by the trustworthy signer. So, when there is not enough space for the certificate and certainly not for the chain of certificates, a solution can be not to include any certificate at all. The certificate would be accessed on-line on demand of the verifier. Instead of the certificate, only a certificate URI will be included in the physical signature.. We need to use binary mode to store URI as the alphanumerical mode of QR codes is only for numbers and letter in one case, no mixed case is possible. As URI is of quite small information density we can think of some compression e.g. LZW compression before storing into QR code.

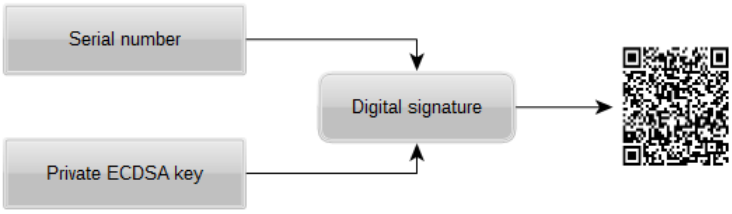

Fig. 2. *A simple signature. Source: Author.*

4 Trusted timestamping

The digital signature scheme described above is fully dependent on the goods producer reliability. We can enhance the scheme in the way that a trusted third party would digitally sign SN. Such third party could provide not only a verified digital signature but also a trusted timestamp if acting as Time Stamping Authority (TSA). Standards providing reliable timestamping are Internet X. 509 public key infrastructure timestamp protocol described in RFC 3161 (Adams et al., 2001), ANSI X9.95-2012 standard and ISO/IEC 18014: Information technology-security techniques time stamping services (ISO 18014, 2008). We can use any of the time stamping schemes mentioned above as we need only a basic time stamping service.

In such a case QR code on material goods would provide not only a verification of goods producer but also a partially verified time of production. Why only "partially"? The time stamps for digital goods can ensure that these digital goods existed before the stamped time. In the case of material goods, the situation is not so simple. Formally, the time stamp ensures that the digital serial number existed before the stamped time, but it is not a claim about the existence a material goods. However, we can claim that if the QR code containing signature and time stamp is an integral part of the product i.e. printed on its surface before the last clear coat is applied, the material goods were produced after the stamped time. If the QR code was printed on a label and affixed to a product, we could claim that the printing and affixing of the label took place after the stamped time, but the sequence of production and time stamping would be not known.

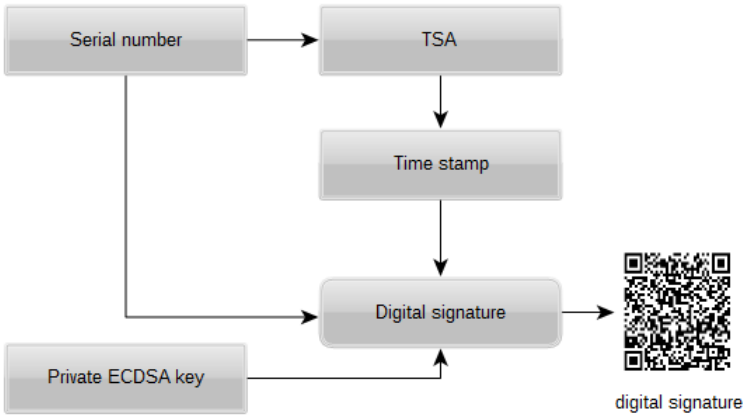

Fig. 3. *A signature with a time stamp. Source: Author.*

5 The distribution scheme with a revenue stamp

Distribution of some goods is state-controlled, mainly it involves alcohol and tobacco products, but this can be easily extended to other goods. The state control is carried out by distribution of stamps (revenue stamps) which the product must be labeled with. Since December 12, 2013, the revenue stamps for alcohol in Czech Republic should have serial numbers not only printed in a human readable format but also in computer readable QR code. Such configuration makes it possible to sign the serial number generated for the product by the producer, and also to sign the serial number of the stamp. The producer needs to read the QR code printed on stamp (the stamp number), to generate his own serial number, possibly obtain time stamp for his serial number and to collect all the information. Finally, he needs to add the digitally signature of all collected data, transform this to QR code and print it on the product.

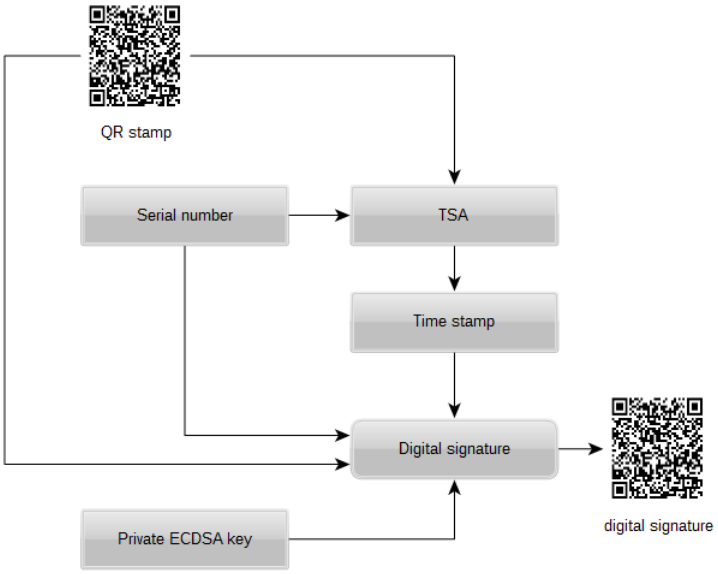

Fig. 4. *A signature with a time stamp and a serial number from a revenue stamp. Source: Author.*

6 Verification

The digital signature of material goods could be verified by any customer having a smartphone. Nowadays, every smartphone is equipped with a digital camera and also a QR reader application is available for all major mobile OS. In case of a plain signature, the QR code will contain the serial number, the digital signature and a link to the public key certificate. A verifying application will download the certificate, verify its validity and verify the digital signature from the QR code with the public key from the certificate.

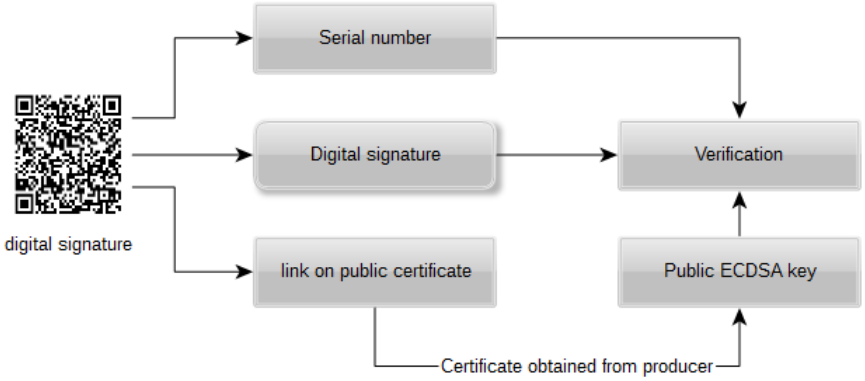

Fig. 5. *A verification of the simple signature. Source: Author.*

In case of digital signature with time stamp, the verification will be quite similar. The verifier will check the same information as in the basic model and moreover will check the validity of the time stamp.

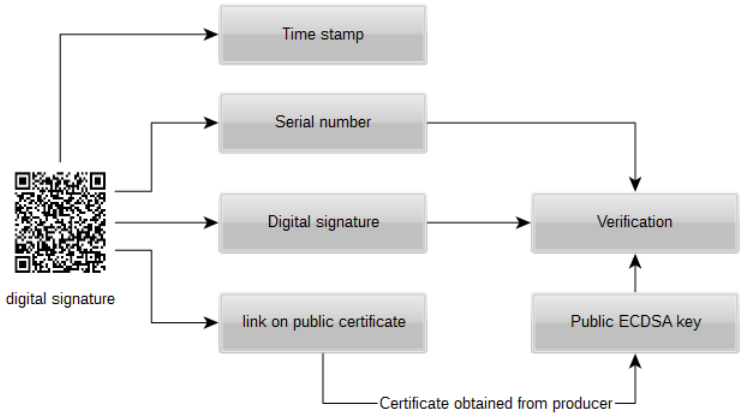

Fig. 6. *A verification of the signature with the time stamp. Source: Author.*

The verification of state controlled distribution of goods will need a little more checking. First of all, the verifier needs to scan both QR codes – the code from the revenue stamp and the main code containing digital signature and the other. After that, the stamp number must be extracted from the digital signature QR code and checked if it is equal to number of the revenue stamp. Then the validity of digital signature will be verified in the same process as in the previous simpler situation.

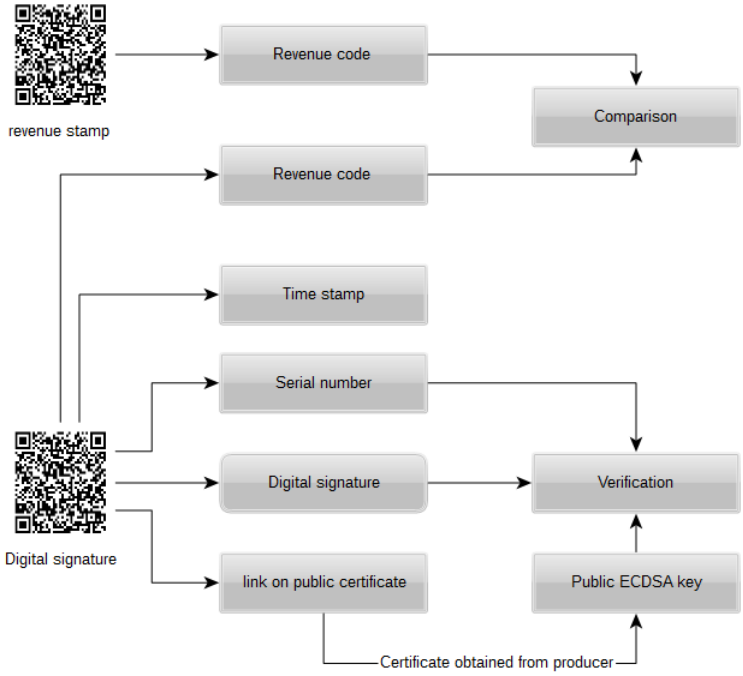

Fig. 7. *A verification of the signature with the revenue code and time stamp. Source: Author.*

7 Discussion and limitations of the architecture

When a digital message with a digital sign is copied, the result is the same message as the original and it carries the same information. Both, the original and the replica provide the message as well as a proof of the authorship of the message, and they are indistinguishable. A replica of a material item always creates a new item and, contrary to the digital world, the replica is not "the same indistinguishable item". From a cryptographical point of view if the counterfeiter exactly copies the original with all dots of the QR code, the replica will be cryptographically valid. But that is the case with all verification signatures. The authenticity of the signature must be furthermore supported by technical difficulties in creating a copy. A banknote is a typical example of an item in the material world with many features preventing from copying. A revenue stamp is a simpler example, with fewer features. A digital signature of material goods can't prevent from counterfeiting by itself. The signing needs to be materialized by means technically difficult to be copied. One of such methods was described in part 5 (The distribution scheme with a revenue stamp). The revenue stamp is equipped with features to prevent copying and digital signature proves the real producer. If neither the revenue stamp nor other non copyable sign is used, the counterfeiter must produce only exact copies; serial numbers can't increase and so it will be easier to detect counterfeiting when more than one item is available.

The presented architecture is designed to reduce possibility to counterfeit material goods. Goods digitally signed in accordance with this architecture would be much more complicated to counterfeit, and it would be much more difficult to create cryptographically valid fake item. Nevertheless, when the counterfeiter exactly copies the original with all dots on the designed QR code, then the replica would be also cryptographically valid; so cryptographic security should be completed by technical difficulties in making exact copies. Especially, usage of a cryptographically signed revenue stamp embodied in a product would be very secure.

References

Adams, C., Cain, P., Pinkas, D., & Zuccherato, R. (2001). *RFC 3161: Internet X. 509 public key infrastructure timestamp protocol (TSP)*. Retrieved from https://www.ietf.org/rfc/rfc3161.txt

Baker, S. A., & Hurst, P. R. (1998). *The limits of trust: cryptography, governments, and electronic commerce*. Boston: Kluwer Law International.

Boneh, D., & Boyen, X. (2004). Short signatures without random oracles. In *Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques* (pp. 56–73). New York: Springer. doi: 10.1007/978-3-540-24676-3_4

Boneh, D., Lynn, B., & Shacham, H. (2004). Short Signatures from the Weil Pairing. *Journal of Cryptology*, 17(4), 297-319. doi: 10.1007/s00145-004-0314-9

Hrubý, J., & Mokoš, I. (2001). K zákonu o elektronickém podpisu, jeho dopadu na ekonomiku a bezpečnostních hlediscích. *Crypto-World,* 3(2), 7-14.

ISO 18004, (2006). ISO/*IEC 18004: Information Technology-Automatic Identification and Data Capture Techniques-QR Code Bar Code Symbology Specification*. Retrieved from http://www.iso.org/iso/catalogue_detail?csnumber=43655

Johnson, D., Menezes, A., & Vanstone, S. (2001). The elliptic curve digital signature algorithm (ECDSA). *International Journal of Information Security*, 1(1), 36-63. doi: 10.1007/s102070100002

ISO 18014. (2008). *ISO/IEC 18014-1:2008 Information technology — Security techniques — Time-stamping services — Part 1: Framework*. Retrieved from https://www.iso.org/obp/ui/#iso:std:50678:en

Pfitzmann, B. (1996). *Digital Signature Schemes: General Framework and Fail-Stop Signatures*. New York: Springer.

Schneier, B. (2007). *Applied cryptography: protocols, algorithms, and source code in C*. New York: John Wiley & Sons.

Smid, M. E., & Branstad, D. K. (1993). Response to comments on the NIST proposed Digital Signature Standard. In *Proceedings of the 12th Annual International Cryptology Conference* (pp. 76–88). New York: Springer. doi: 10.1007/3-540-48071-4_6

Tvrdíková, M. (2003). Správa digitálních dokumentů. In *Proceedings of the Systems Integration Conference* (pp. 586-591). Praha: Vysoká škola ekonomická v Praze.

Zhang, M., Yang, B., Zhong, Y., Li, P., & Takagi, T. (2011). Cryptanalysis and Fixed of Short Signature Scheme without Random Oracle from Bilinear Parings. *International Journal of Network Security*, 12(2), 159–165.