FI MU

Faculty of Informatics
Masaryk University

Trustworthiness of signed data

by

Petr Švéda

FI MU Report Series **FIMU-RS-2002-06**

September 2002

Trustworthiness of signed data

Petr Švéda

Faculty of Informatics, Masaryk University Brno
Botanická 68a, 602 00 Brno, Czech Republic

E-mail: `xsveda@fi.muni.cz`

Abstract

Use of digital signatures is not as straightforward as one would like to see it. We have to be aware of the fact that computers sign all electronic documents on behalf of humans and only few computers can be considered as fully trustworthy. Visual representation of file formats can be dramatically changed by settings of a viewer or a text processor. Users cannot be absolutely sure that they sign only the data visible on their computer screen. Proprietary signature solutions are not fully compatible as there are no standards.

This paper reviews the problem of the document content interpretation. Introductory section reviews problems related to the use of digital signatures in practice. The second section briefly summarizes necessary cryptographic assumptions and gives an overview of signature functional properties. The third section discusses questions and possible ways of an interpretation of documents content. The fourth section suggests design principles for trustworthy electronic document structure.

Keywords: content interpretation, digital signature, electronic document, signed data, trust, WYSIWYS.

1 Introduction

Business requirements and a practical usage of a digital signature advert to many questions which are not considered either in signature techniques, known from the field of cryptography, or in the law, regulations and standards. The open problems include:

- Trustworthy signing time.
- Long-term validity of electronic documents.
- Bilateral and multilateral signatures of the same document.
- Interoperability between individual proprietary and / or national signature solutions.
- Unique way of document content interpretation.

This paper summarizes the problem of a document content interpretation – it gives an overview of signature functional properties, discusses questions and possible ways of a document content interpretation and suggests possible design principles for a trustworthy structure of an electronic document.

2 The field of asymmetric cryptography

There are two separate keys for encryption and decryption in the *asymmetric cryptography* [1]. A *public key* is used for encryption or signature verification. Decryption and signature creation are performed with a *private key*. The keys are related to each other. Yet obtaining the private one from its public counterpart is an NP-complete problem and is thus computationally infeasible to undertake (see [4, 7]).

This section summarizes the background of digital signature techniques known from the field of cryptography. An electronic document can be considered as a special case (or a part) of a message.

2.1 Digital signatures and hash functions

From the technical point of view[1] the signed message consists of two parts – the original message and the attached (or embedded) signature. The digital signature is a unique message characteristic (computed by hash function) encrypted by signer's private key (see figure 1).

The use of hash functions provides a means for validating the data source and integrity. *Hashing* is the process of obtaining a smaller dataset

[1] We consider the basic digital signature scheme with an appendix (e.g., DSA, ElGamal, Schnorr). There also exist digital signature schemes with message recovery (e.g., RSA, Rabin, Nyberg-Rueppel). The later type can be exchanged for the former one (see [4, 7]).

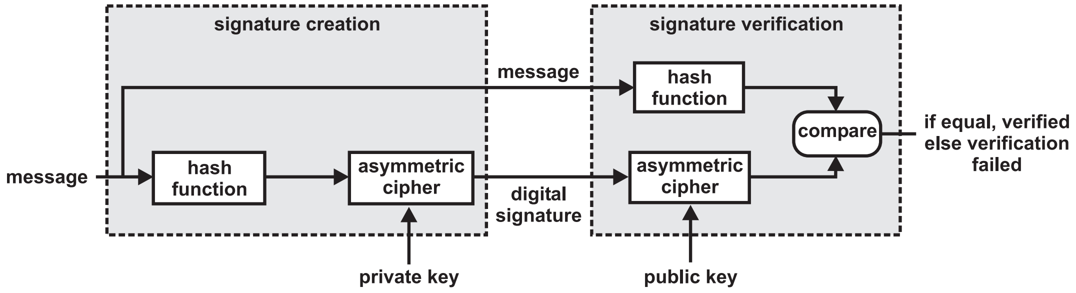

Figure 1: Signature creation and verification process.

from the original data by using a transformation prescribed by the hash function (see [4, 7]).

Consider the signature verification process shown in figure 1. The recipient uses an appropriate sender's public key to decrypt the attached signature, computes the hash value of received message and compares both characteristics. If they are equal, the signature (and message) is verified. In other cases the message has been modified by an attacker or due to transmission error in a communication channel.

2.2 Functional properties

From a functional point of view the signed document is a message, which is authenticated by the secret information – *private key*. This secret piece of information always has to be under the direct control of the key owner (signing person). There exists a widely spread public counterpart of some secret information – *public key*. It has to be unforgeably tied to the key owner's identity. The basic use of asymmetric digital signature techniques (as figure 2 shows) assures three functional properties.

- *Authenticity of a message in relation to the signing person* – the recipient knows who has participated in a transaction (as only the owner of private key can make the signature).

- *Integrity of a message* – the recipient can easily verify that the content of a message has not been changed or altered, either accidentally or maliciously (by an attacker or due to error transmission in the communication channel).

- *Non-repudiation of a message* – the signer of a document at one end of a transmission cannot deny having sent the message nor can the

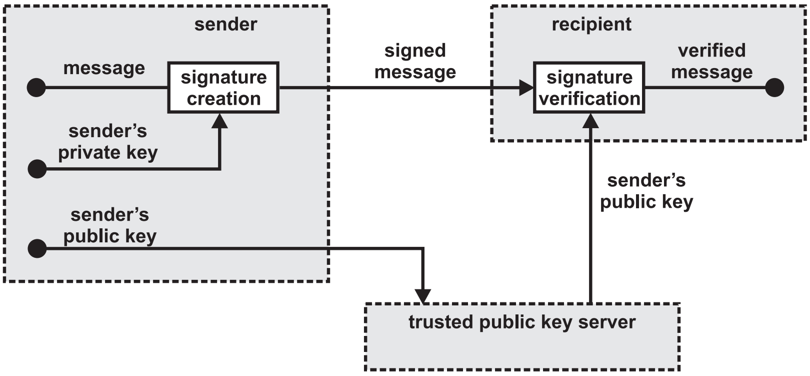

Figure 2: Assuring authenticity, integrity and non-repudiation.

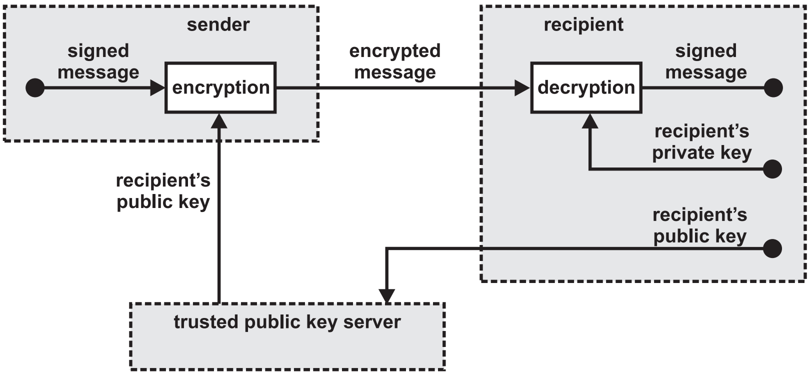

Figure 3: Assuring confidentiality.

recipient deny having received it (non-repudiation means that an act cannot be disclaimed, similar to a witnessed handwritten signature on a paper document).

It is also possible to ensure *confidentiality* of a signed message. As figure 3 shows, the sender encrypts the signed message with the proper recipient's public key.

2.3 Attached versus embedded signatures

If it is necessary to sign previously signed message once more, there are in principle two possibilities how to achieve this.

- *Attached signature* – sign only the content of the message again. The second signature would not cover the first signature. Both signatures are fully independent – it is possible to modify or delete the preceding signature without affecting the following ones. This technique can be sometimes called *parallel signature*.

- *Embedded signature* – sign the whole message covering the inner content and the first signature. It is impossible to change or delete the preceding signature without corrupting all the following ones. This technique can be sometimes referred as *serial signature*.

Both these techniques can be combined in an arbitrary order. It is possible to realize any practical business requirements.

3 Interpretation of document content

There are three types of information that an electronic document can involve.

- *Logical structure* – refers to the relationship between data elements. For example, the logical structure includes subheadings, paragraphs, and bulleted lists.

- *Physical format* – is appearance of a document. For instance, a section number, by definition, might be centered at the right side of a page. Likewise, a section number could, by definition, be aligned on the left side of a page. The same logical structure can be presented by many physical formats.

- *Content data* – electronic document may include types of media, such as text, hypertext, graphics, video, or sound. Data can also include predefined data elements, such as name, address, or phone number. Importantly, data in an electronic document do not have to be visible to the human eye. That is data, such as author, creation date, transfer date, time-stamp, state, can be embedded in a document. Embedded data can be extracted and used by a computer, even though it is not visible. Embedded data is sometimes called metadata.

Existing file and data formats can be divided (according to the data structure) into three groups.

- *Mark-up based* – formats that capture logical structure and may include some necessary metadata for viewable transformation (for instance XML or TEX file formats).

- *Page describing oriented* – formats that capture layout, e.g. Portable Document Format (PDF) or PostScript (PS).

- *Combined* – mixture of layout and structure. An example is Rich Text Format (RTF) or Microsoft Word Document (DOC).

The rest of this section is oriented to documents that can be presented in a text-based form.

3.1 Content and its presentation

Different devices and applications have different capabilities and options determining what they can display and how they display data. Electronic form of a document, which exists in a digital world (magnetic medium or computer memory), is represented in a binary form by logical values true and false. All actual known file and data formats interpret binary data. This interpretation is either direct or text-based.

Only plain ASCII text, according to the standard [8], has a special position in some respects – the format is in fact a prescriptive norm. It is supported as the basic format by all known operating systems. But interpretation does not have to be always unique and the same as there are extensions of the standard like national character sets.

Presentation of an electronic document can be layered into five stages.

- *Binary presentation* – stream of logical values true and false (binary represented as '1' and '0').

- *Text-based presentation* – digital information is decoded according to standard [8]. Not all file or data formats have to be necessarily meaningful on this level – especially multimedia-oriented formats directly interpret binary data.

- *Logically structured presentation* – can be simply viewed in many ways, because it is easy to transform it. Structured content data is always the same, because it is platform- and device independent. Final viewable presentation is given by the set of transformation rules. Set of transformation rules has to be unambiguous and comprehensive for applications of digital signatures.

- *Viewable presentation* – a visualized form of content data depends on capabilities of a viewing application and displaying device. All the data is still in an electronic form and can be edited.

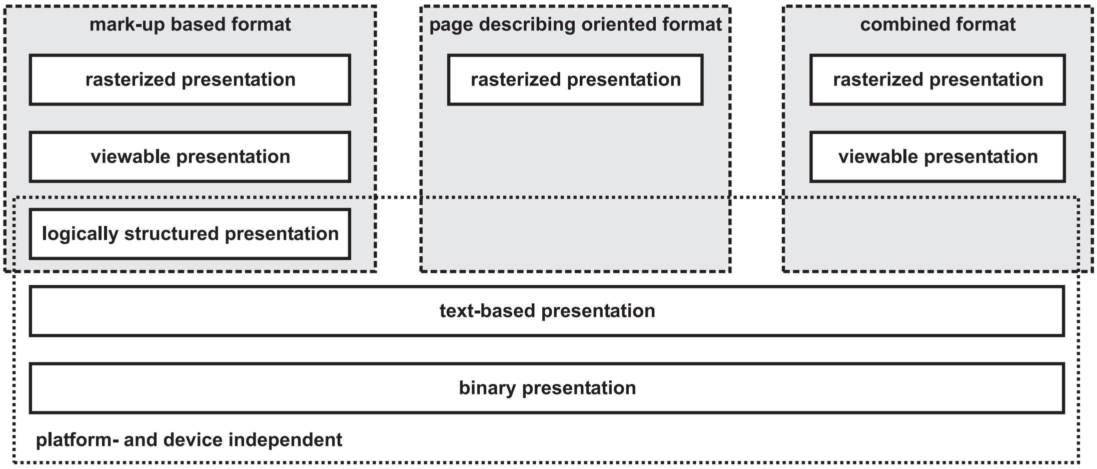

Figure 4: Format types and presentation levels.

- *Rasterized presentation* – final form is displayed on a computer screen. Information is not in editable electronic form yet, because it is rasterized into pixels (or dots in case of printing).

Figure 4 illustrates connection between document viewable layers and file format types.

Consider one unique document on the binary presentation layer. It is possible to create many different readings on the viewable presentable layer. A lot of possible ones do not have to be meaningful necessarily. It states the problem how to choose the right one which was perceived by the signing person from between all meaningful interpretations by unique defined algorithmic way. Applicable reading may meet these following requirements.

- All content data in the document is visible.
- Content of the document is presented in a comprehensible form.

The statement, which requires a presentation in a comprehensible form, cannot be achieved by a simple technique. There might be a lot of potential barriers in understanding of the content.

- *Physical objectives* – e.g., handicaps (color blindness, deafness).
- *Mental capabilities* – e.g., language abilities (reading ability, understanding ability), education level in the case of specialized text.

- *Settings and preferences of a text editor (or processor)* – e.g., notices, annotations, hidden text, pasted and embedded objects from other applications.

3.2 Non-unique interpretation

Digital signature functional properties, described in subsection 2.2, assures functional requirements on the binary presentation level. At other presentation layers these requirements are not directly assured because all known data and file formats might have a lot of optional settings. A visual appearance of an electronic document may radically change. The problem increases because there is not assured unique content data interpretation for the data or file format in form that is *perceivable by human senses*. This topic is covered neither by the EU directive [9] nor by any national law or regulations of European countries.

Consider widely spread Microsoft Word document format – viewing items such as notices, hidden text or annotations are dependable on settings of an editor or a viewer, that is used for a document opening. In the case of multimedia file formats a lot of content information can be hidden in side channels. The hidden information can be searched by techniques known from the field of *steganography* [5].

3.3 WYSIWYS paradigm

The idea behind WYSIWYS[2] approach is to ensure that the application really presents all contents accurately and in the same way. It should prevent the user from signing data unintentionally caused by a wrong, incomplete, unrecognizable or ambiguous presentation. General functional requirements can be summarized in the following way.

- It is a signed instance of an electronic document, which is visible on signer's screen at the moment of signing.
- The signed instance has a unique content interpretation.
- Signed instance can be verified against document content and it is unforgeably tied to the electronic document.

[2] What You See Is What You Sign – principles developed jointly in the largest Pan-European project on electronic commerce, SEMPER [2]; implementation in XML by [6].

3.4 Solution approaches

Requirements demanded by the WYSIWYS paradigm in subsection 3.3 can be assured by three approaches.

- Content data structure with the use of metadata.
- Visual document interpretation.
- File or data format with unique visual interpretation.

Individual solution approaches have a lot of pros and cons. Any of approaches listed above cannot be perceived as an integral solution. Time, space or computational requirements transform these ideas for same specialized applications into fantastic myths.

3.4.1 Metadata tagging

The tagging solution approach requires strictly guaranteed visual presentation form for an every metadata item. There are solutions on the basis of XML format, which uses signing on the level of metalanguage tags. Practical implementations sign a logically structured content and a set of transformation and presentation rules (uniqueness, unambiguousness and comprehensiveness are not obviously checked). It is not necessary to include rules when the visual presentation of tags is defined in a standard, law, bi- or multi-lateral agreement.

3.4.2 Rasterized view

This type of analogy with paper based documents uses some proprietary solutions. The instance of a document is virtually printed (e.g., in a quality of fax document) and signed. In some proprietary implementations the original document might be optionally attached for future possible modifications. Pure rasterized way is in the current state-of-the-art rather suitable for document archiving systems.

3.4.3 Universal data format

These days it is common to consider one universal widely spread data format with unique visual interpretation as an illusion. The idea like this can be observed for instance in US law, where plain text ASCII format can be signed. PDF (Portable Document Format) might be used as a universal format only for special applications. It is possible to define a format and its presentation by an agreement between two or more parties in the tagging approach.

4 Trustworthy document structure

People trust data in the context of a document. It is possible to secure an electronic document by digital signature techniques – this document would be trusted and unalterable. The key points of an electronic document are flexibility and editability. So it is infeasible to trust an editable file format, which has a lot of optional settings that can change a visual representation of an electronic document dramatically.

There exists a fundamental conflict between trust and usability in nowadays combined file and data formats. Mark-up based formats can be trusted if the problem of an unambiguous presentation is solved correctly. Discussion about trust issues for XML documents can be found in [3].

4.1 Functional properties

It is possible to summarize properties of a trustworthy electronic document structure in the following way.

- Consists of separated content data and its static interpretation instance.
- Assures data in a presentation instance, which can be verified against content data.
- Corresponds to functional properties from subsections 2.2 and 2.3 on the level of arbitrary content data or interpretation instance parts.
- Can include unlimited number of signatures.
- Supports standardized metatags (and allows to be customized).
- It is based on public data standard definition.
- All previous states of the document structure are fully and unforgeably described.

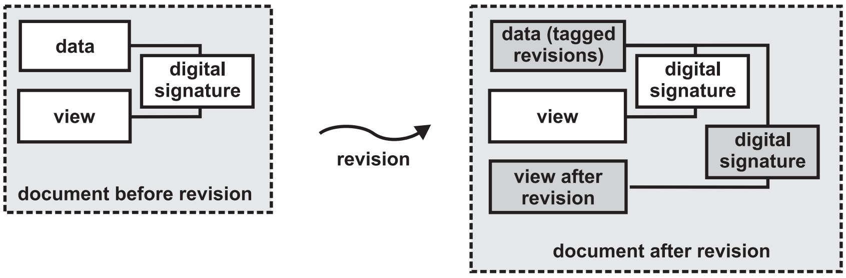

Figure 5: Design approach for a trustworthy electronic document structure.

4.2 Design approach

As it results from the section 3 and functional properties in the previous subsection, it is suitable to separate content data and its presentation. According to requirements of WYSIWYS paradigm, document structure has to contain a signed instance of an electronic document, which was visible on a signer's screen at the moment of signing. A processing viewer or editor uses the trusted signed instance, called view, later. The view might be constructed as:

- *Interpreted* – if all input data is logically structured and there exists a unique set of presentation rules, which is unambiguous and comprehensive.
- *Rasterized* – any time, but the information contained in view cannot be used for later editing and might not be easy to connect editable content data and view.
- *Standardized* – according to a well-known public standard, which has a unique interpretation.

Figure 5 gives the overview of a design approach. The key point is integrity. It is necessary to assure integrity between data and view together with all cryptographic input values used in digital signature techniques.

5 Conclusion

The law, regulations and standards do not identify which technology has to be used to implement digital signatures nowadays. Digital signatures techniques, known from the field of cryptography, assure legal signature requirements on the binary presentation level. Human beings cannot perceive data on this presentation level and do not understand them. People depend on widely spread file and data formats.

Widely spread combined file and data formats cannot be trusted. They have a lot of optional settings that can change the visual representation of an electronic document dramatically. A signed electronic document can be trusted if all its possible future presentations are the same. This paper states functional requirements and suggests a design approach for a trustworthy electronic document structure, which is based on views.

References

[1] Whitfield Diffie and Martin E. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, IT-22(6):644–654, 1976.

[2] Gerard Lacoste, Birgit Pfitzmann, Michael Steiner, and Michael Waidner (Eds.). *SEMPER – Secure Electronic Marketplace for Europe.* Springer-Verlag, 2000. ISBN 3-540-67825-5.

[3] Nicklas Lundblad. Trusted documents. In *XML Europe 2001*, Berlin, 21.-25. 5. 2001.

[4] Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone. *Handbook of Applied Cryptography*. CRC Press, 1996. ISBN 0-8493-8523-7.

[5] Fabien Petitcolas. Steganography, watermarking and cryptography. In *Mikulášská kryptobesídka 2001*, pages 37–42, Praha, 10.-11. 12. 2001. ISBN 80-903083-0-9.

[6] Karl Scheibelhofer. What you see is what you sign – trustworthy display of XML documents for signing and verification. In *Communications and Multimedia Security, CMS '01,* pages 3–13, Darmstadt, 21.-22. 5. 2001. ISBN 0-7923-7365-0.

[7] Bruce Schneier. *Applied Cryptography*. John Wiley & Sons, Inc., 1996. ISBN 0-471-11709-9.

[8] *Coded Character Set – 7-Bit American National Standard Code for Information Interchange.* American National Standards Institute, New York, 1986. ANSI X3.4-1986.

[9] *Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures*. European Parlament, 1999.

Publications in the FI MU Report Series are in general accessible via WWW and anonymous FTP:

```
http://www.fi.muni.cz/informatics/reports/
ftp  ftp.fi.muni.cz (cd pub/reports)
```

Copies may be also obtained by contacting:

Faculty of Informatics
Masaryk University
Botanická 68a
602 00 Brno
Czech Republic