



Digitally signing PDF documents with Open Source tools: Opensignpdf

Abstract

In the beginning of year 2006, PDF signature (that is, digital signature according to PDF specifications) became one of the legally accepted file formats for digital signature in Italy [0].

Formerly, the only legal format was PKCS#7, which is a standard format but not so widespread in use for electronic documents, and is more an envelope for carrying cryptography informations such as digital signature of a generic binary content.

We at “Sistema Informativo” (IT department) of City of Trento were contacted by Antonino Iacono, an independent developer wich is very active in designing open source tools for digital signature; he is the creator of OpenSignature [2], which won in 2004 the Open Source Contest prize [3] as most innovative project. We already collaborated with Antonio for porting our j4sign project under Linux OS, and he asked to us to evaluate his prototype of an open source tool for digitally sign a generic PDF document.

1. PDF Signature pro and cons.

Signing PDF files is interesting because of the very widespread use of this file format; it is not an independent format, because its development is not responsibility of a standard organization, but no royalty will be required to build tools for reading or writing PDF documents, and specifications are publicly available [4].

Italian law, furthermore, mandates who control the development of a legal digital signature file format to provide a tool for verification at no cost.

In general, the criteria to admit a new format are the following [1]:

- a) availability of technical specification for developing products and relative sw libraries for generating or verifying signatures ;
- b) absence of royalties of similar dues to develop the products on point a);
- c) availability of modifications to specifications at point a), minimum 90 days before a new product implementing them is released.
- d) availability, at no cost, of a tool for personal use for verifying digital signatures conforming to specifications at point a)

Since digital signature is built in as a feature of the file format, many practical advantages are possible:

1. It is possible to sign different parts with different signatures, and providing a visual clue about both the signer and the signature scope.



2. It is possible (and is what the standard tool for PDF visualization does) to detect what parts of the documents are subject to change dynamically (this is forbidden by Italian law, that is, digital signature of dynamically changing content is not valid).

The main problem with PDF signature is a lack of independent tools implementing digital signature features of the specification. In particular, there is no Open Source tool for implementing MDP signatures. MDP stands for Modification Detection and Prevention signatures, informally known also as “owner signatures”, and are a particular type of signature that “seals” the document, providing to the owner of the document the ability to admit only some types of modifications of the document or no modification at all.

For example, a formal act could be subject to modifications only for some parts (for example for adding formal acknowledgement by some other entity), and sealed with his signature by the creator for the rest.

Opensignpdf is an effort to address the lack of tools for PDF signature in the Open Source domain.

2. Opensignpdf

Opensignpdf is written in Java language, and is based on the well-known opensource java library iText [5].

We collaborated to the project in particular for adding support for timestamping. The current version is 0.0.4, it supports smart cards that provide a pkcs11 interface, and can be used to create normal PDF signatures and also MDP ones. Timestamping services support according to RFC 3161 is also provided.

The code is freely available under GPL license from the Download section of Opensignature site:

http://sourceforge.net/project/showfiles.php?group_id=67103&package_id=188602

Currently it is possible to add simple signatures of the whole content, and MDP ones without further modifications permitted.

Opensignpdf has already received interest by iText library creators for a possible inclusion in the mainstream.

References

- [0] – February 16, 2006 - announcement of [CNIPA-Adobe Memorandum of Understanding](#) (in Italian).
- [1] – CNIPA (National Centre for IT in the Public Administration) - [act 5/2005, February 17, 2005](#) (in Italian).article 12.9.
- [2] – OpenSignature [website](#).
- [3] – Open Source Context [winners](#) .
- [4] – [PDF specification](#) .
- [5] – iText website: <http://www.lowagie.com/iText/> .