

Security of the italian legal digital signature scheme

Stefano Zanero
Dip. di Elettronica e Informazione
Politecnico di Milano
Via Ponzio 34/5
20133 Milano (Italy)
zanero@elet.polimi.it

Summary

The early adoption of a national, legal digital signature scheme in Italy has brought forth a series of issues and vulnerabilities, often claimed to be defects of the digital signature technology itself.

In this poster we address these issues, and we show that in each case the issue does not lie in the algorithms and technology adopted, but either in faulty implementations, bad design choices, or political and methodological issues.

Italian Law on Digital Signatures: key facts

- Introduced in **1997** with the DPR 513, creating the concept of "law-strong" digital signature (in short, ILDS, Italian Legal Digital Signature).
- Revolutionary decree which:
 - Gives to electronically signed documents (prepared with prescribed methods) the same value of paper documents, signed by the author
 - Recognizes that if the protocol is tamper-proof "enough", the electronic document can be trusted to show the actual will of the signer
- A digital signature can't be "unrecognized": **you can not claim that it is not your own signature**, something you can do with a handwritten signature.
- PKI architecture described in DPCM 08/02/99:
 - standard X.509 certificates
 - Mandated use of tamper-proof hardware devices for generating the keys
 - Certificates created and signed by trusted CAs, registered by the regulatory agency AIPA
- Requirements for trusted CAs:
 - to be "S.p.A." (a particular form of society) and have a minimum capital of about 6.500.000 EUR
 - requirements of "honorability" for their administrators (no bankruptcy filings, ...)
 - Their technicians must show due diligence and competence to fulfill technical regulations
 - Their IT processes must respect international standards for quality assurance
- Each authorized CA has created its own application for the creation and the verification of the digital signatures.** This has created problems for interoperability, and also the vulnerabilities we describe
- The ILDS can be used to:
 - sign contracts,
 - sign documents for the government offices
 - generate a timestamp for a document.
- It cannot be used:
 - to buy an house (since the italian law requires the presence of buyer and seller in front of a notary)
 - to sign a petition for a referendum consultation (for this will require you to be recognized by a public officer).
 - To authenticate against SSL servers for e-commerce transactions (you can actually do this, but it will have no particular legal effect)

Three failures of the Digital Signatures

Word macros and fields

- Vulnerability first described by the author
- Flaw in the application design, first discovered in the software DiKe (developed by InfoCamere), but affects also most of the other softwares available
- Main idea of attack: if a MS Office document containing a "dynamic field" is signed, and then verified at a later time, the application shows it in the integrated viewer along with the updated field, without either detecting the variation or alerting the user that a dynamic field is present.

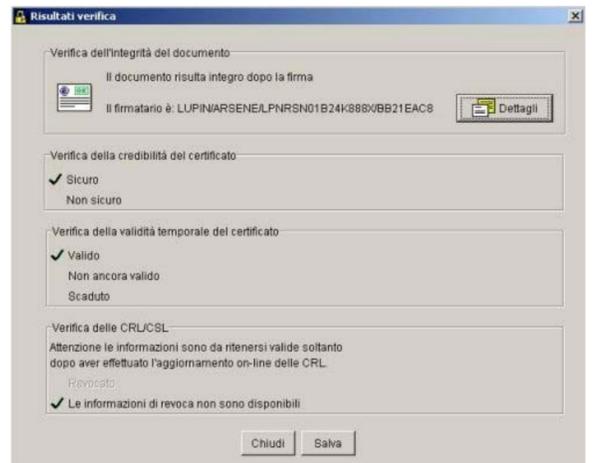


- InfoCamere said that the defect had little impact, and was not a defect anyway. However, they fixed it in following versions ;-)
- DiKe, like any other ILDS software, digitally signs (and verifies) an hash of the file containing the document, not the textual content. The variation generated by the macro execution does not alter the file, thus DiKe reports that the file integrity has not been broken
- However, in Italian Law, "document" does not mean "file". **The document is the representation of the file, it is what the reader can see.** A digital signature software should verify the representation, not the file itself. In addition, DPCM 8/02/1999, art. 10, says that ILDS applications must represent to the signer "in an unambiguous manner" what he is going to sign. This is a problem after all ;-)
- Possible solutions:
 - disqualify formats that can be modified by macros: **operationally inefficient**
 - The application could automatically generate a PDF copy of the document, and let the signer sign this copy: **problem of "royalties"**
 - Office Macros could not be deactivated from 3rd party doc viewer APIs. **MS has acknowledged this flaw and released an add-in**
- The real problem is that any decoding system used to represent the document to the signer should be validated and incorporated into a secure ILDS application. This is evidently impossible. **A standard format such as XML could be the ideal solution for this type of problems**

The PosteCom failure

- Firma&Cifra: application released by PostE-Com. It contains a macroscopic vulnerability which makes it totally insecure
- Again, the problem does not reside in the cryptographic algorithms.

- In ILDS signatures, for efficiency, the digital certificate used to generate the signature is appended to the signature itself, using a PKCS#7 envelope. The certificate should be first verified (using the trusted certificates of the authorized AIPA CAs already stored) and then added to a cache list of verified certificates.
- However, **if the certificate inserted in the PKCS#7 envelope is a root certificate**, Firma&Cifra does not discard it (as it should), but **it caches the certificate and uses it to verify other certificates!**
- This incredible error leads to astonishing results, you may see in the figure the "authentic" signautre of Arsène Lupin !
- Also in this case, the CA tried shamelessly to minimize the importance of the problem !



Who's got my Smart Card anyway ?

- One of the most critical points in the certification chain is the roll-out of smart cards to subjects and their identification
- In at least one documented case, a CA created a number of certificates for the clients of a single professional accountant, which were given (along with their PIN) to the accountant himself...
- We may remember the story of VeriSign and a Microsoft code signing certificate... but a law-strong signature which cannot be unrecognized poses even bigger problems!

Proud to be the first...

- 13/05/03: press says that the Network and Security Laboratory of the University of Milan has completed "the first practical realization world-wide" (sic) of attack against a digital signature device
- No reliable scientific document available on this experiment
- The attack consisted simply in demonstrating how a pre-installed trojan on the user's machine was able to intercept the PIN and use it
- Remarks that an insecure system cannot be used for generating trusted, secure digital signatures

Conclusions

- In each case the issue does not lie in the cryptographic algorithms, but in:
 - bad design choices
 - incredibly faulty implementations
 - methodological issues dealing with certificate distribution and user education
 - well-known problems in generating trusted signatures on an untrusted machine
- If you think that cryptography can solve your problem, you don't understand your problem and you don't understand cryptography**