SPECIAL THEME: E-GOVERNMENT

ERCIM News No.48, January 2002 [contents]

Adopting the Digital Signature: A Proposal for Cooperative Work in the Italian Judicial System

by Domenico Laforenza

The creation of a system for cooperative work between Italian law courts and Italian lawyers using the national public administration network could greatly improve the efficiency of the Italian judicial system. At the basis of this co-operation is the safe and secure transmission of electronic documents.

The widespread employment of computational tools by Italian courts and Italian lawyers has greatly encouraged the easy and economic exchange of electronic documents between them. In particular, the introduction of Electronic Filing (EF) systems has resulted in considerable benefits to all those involved in the Italian legal system, including the ordinary citizen who, in some way or another, interacts with it.

Clearly, in order for EF systems to be used in legal operations, the confidentiality and inviolability of documents must be guaranteed. Methods that ensure the privacy and security of electronically transmitted information must be employed, and data encryption techniques are becoming increasingly common for this purpose. For example, while traditional e-mail systems do not guarantee security, if they are used together with an encryption system, it is possible to ensure that the document transmitted:

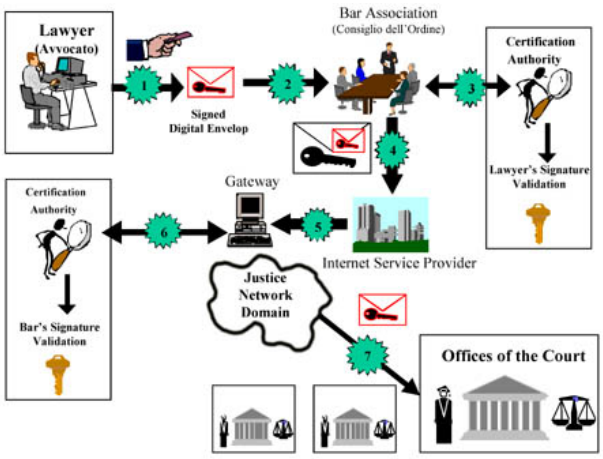
- comes from a given, identified sender (guarantee of authenticity)
- cannot be disclaimed by the sender (guarantee of non-repudiation)
- cannot be read by third parties during transmission (guarantee of confidentiality)
- cannot be modified by third parties during transmission (guarantee of data integrity).

The problem of the correct identification of individuals is crucial in modern society, see for example the use of badges that permit selective access to public or private sites. Computerised systems can be adopted in a similar way to control the access of users to given services.

A new approach to the identification of individuals is the use of electronic or digital signature technology, which is based on Public Key Cryptography (aka Asymmetric Key Cryptography). Each person is associated with a pair of asymmetric keys, one of which is 'private' and used to sign documents, the other is 'public' and used to verify signature authenticity.

The digital certificate has been introduced as a means of guaranteeing the safe transmission of the 'public' key. A digital certificate associates the personal data of an individual with one or more 'public' keys. It has a function in Internet/Intranet transactions similar to that of an identity card or passport in the non-virtual world. A digital certificate is validated by a Certification Authority (CA). Standards have been studied to define the data structure of digital certificates and the distribution procedures that can be used by a CA. The currently most popular standard for digital keys is ISO X.509 version 3.

A Model for Co-operation between Italian Courts of Law and Lawyers
The figure shows a proposal for co-operation within the Italian legal system, presented in the framework of a broader feasibility study commissioned from CNUCE-CNR by the Italian Ministry of Justice at the beginning of 2000. Most of the operations described below are performed automatically.



Model for Co-operation between Italian Courts of Law and Lawyers

A document is transmitted as follows:
Lawyers:
• prepare an electronic document and sign it using their private key (step 1)
• transmit the electronic documentation to their Bar Association (BA) (step 2).

The Bar Association:
• validates the authenticity of the documentation through the Certification Authority which holds the public key of the lawyer (step 3)
• adds its own digital signature and transmits the documentation (step 4) to the ISP of the BA so that it can be sent to the gateway of the National Justice Network Domain (step 5)
• when the documentation is received by the gateway the following controls are made:
• validation of the authenticity of the documentation received by the BA (step 6)
• transmission of the document to its final destination, the receiving court of law (step 7).

In order to authenticate the lawyers, documents sent by them to the Courts must obtain a countersignature from their professional association (Bar Association). For this purpose, they will have a pair of asymmetric keys for authentication, one private (and kept in safe custody in a smart card, for example) and the other public (and known to a Certification Authority). Lawyers should have the facilities available (eg, smart card writer/reader) to be able to generate their own keys rather than entrusting the supply of the keys to the Bar Association. In this way, the risk of the private key being used by unauthorised persons is reduced to a minimum. With this model, the lawyer is free to use any suitable Internet Service Provider (ISP) and can transmit a legal document to any Italian court, complete with a digital signature.

Costs and Benefits
The model proposed specifies that the document transmitted by the lawyer must be countersigned by the Bar Association. This introduces an additional level of security and also speeds up the process of validation of the electronic documents received by the gateway (of the Justice Network Domain). In this way, it is not necessary to check the authenticity of each single lawyer, just of the relevant Bar Association (in Italy there are 164 Bar Associations for more than one hundred thousand lawyers). However, this model implies that each Bar Association must possess the necessary hardware and software and implement a suitable infrastructure. An alternative and more cost-effective solution would be for Bar Associations to entrust specialized (outsourcing) agencies with the task of digital signature verification.

The model for nationwide telematic co-operation between Italian lawyers and the courts proposed above is both technically and legally feasible, and could play an important role towards alleviating many of the problems that are the cause of the current inefficiency of the Italian civil judicial system.

Please contact:
Domenico Laforenza, CNUCE-CNR
Tel: +39 050 3152992
E-mail: domenico.laforenza@cnuce.cnr.it