A technician's views on the digital signature in Italy

ING. FRANCO RUGGIERI

Italians, like most of the civil law countries citizens, enjoy the best and the worst of having a great number of laws, decrees, etc. to pave their way or to hamper it: In my view, this is turning out to be useful in implementing electronic signatures.

Since 2001, I have been working in the EESSI,[1] where I have witnessed a two pronged effort: on the one hand the technicians, like myself, have strived to find a technical solution to all possible problems in the electronic signature domain, in order to prevent fakes and to provide these signatures with long lives, possibly for decades; on the other hand the jurists, who bring the technicians down to earth about the actual achievability and practical feasibility of the solutions they devised.

I must admit that I am an apostate, in that, after joining the flock of those who had the illusion of solving everything by technical means, I have now struck a balance, or at least I think I have. I found my way when I realised that the most reasonable goal one could hope to attain in the electronic signature domain is just achieving a security and reliability level at least comparable to that of the handwritten signature: whatever better is achieved is welcome, but it is not the goal.

The European Union Directive on electronic signatures[2] (EU Directive) at article 5(1) states:

"Member States shall ensure that advanced electronic signatures which are based on a qualified certificate and which are created by a secure-signature-creation device:

satisfy the legal requirements of a signature in relation to data in electronic form in the same manner as a handwritten signature satisfies those requirements in relation to paper-based data; and

are admissible as evidence in legal proceedings."

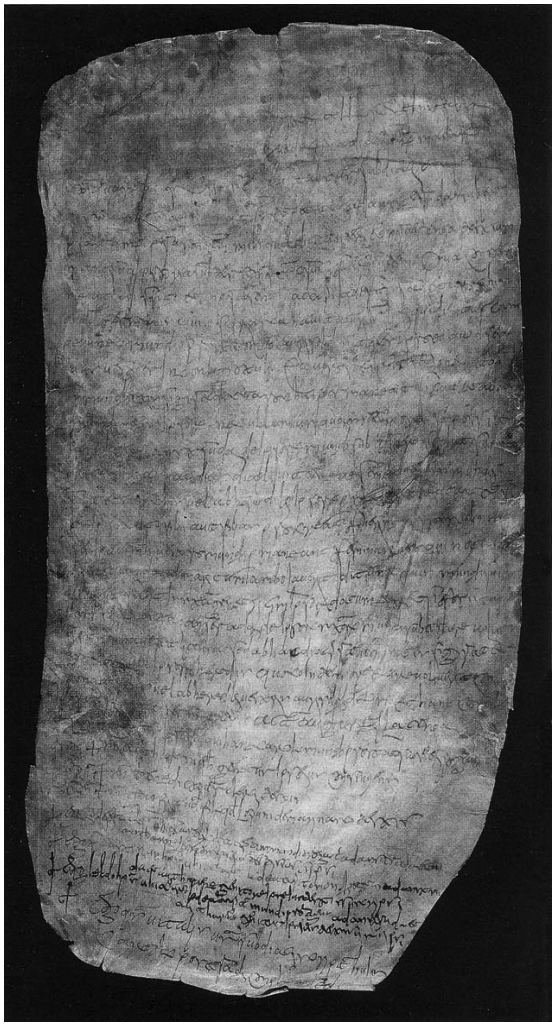
These are the qualified electronic signatures I address in this article: advanced electronic signatures which are based on a qualified certificate and which are created by a secure-signature-creation device.

Some people consider that to ascertain if an electronic signature is valid, assuming all the technical requirements have been met, an expert is necessary, since a lay person does not possess the skill to tell forged electronic signatures apart from authentic ones. Moreover, there is uncertainty on the capability to read an electronically signed document centuries, or even decades, from now. Let me briefly comment on these two objections.

- Has a reader even been given a 50 euro note that turns out to be a counterfeit? Yet, apparently, euro banknotes teem with anti-counterfeiting mechanisms.
- Some years ago Prof. Luigi Di Bella, an Italian doctor, claimed he had an anti cancer cure that was far less destructive than the usual chemotherapy with (in some cases at least) better outcomes. They formally tested this in several protocols, with controversial results. But Prof. Luigi Di Bella said, about one of the protocols: "Yes, this is my signature, but I never put it on this protocol: someone else must have done I wonder what with copiers and the like."
- Years ago a fuss was raised about some forged handwritten Hitler diaries. It took a number of experts at calligraphy to find out it was a well crafted fake.
- Finally: in the autumn of 2001 the Milan State Archive hosted an EESSI meeting, and we were shown the glories of the archive, among which included an eight century parchment.[3] What was interesting, aside from its content which, for the curious ones, was kind of a morganatic marriage agreement, was that you

[1] European Electronic Signature Standardisation Initiative.
[2] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures (OJ 19.1.2000 L13/12).
[3] A view of this document in electronic format is available at http://213.156.63.135/html/attivita/cataloghi/covers/02.jpg.

could see neatly crafted characters, but a lay person could not understand what it said. This did not depend on the language (it was written in a form of Latin), but it depended on the fact that words and even sentences were abbreviated and "coded" according to the common use at the time it was written. As a conclusion: only a dozen or so expert people around the world could understand the content of the document.



The publishers are grateful to the Archivio di Stato di Milano for permitting the image of the cartola de accepto mundio to be reprinted in accordance with numero di protocollo Prot. N. 3518/IX.5.2.

So: is the good, old paper document really fake-proof and time-proof?

When we face reality, we know that absolute security and certainty do not exist and will never exist in any field. At most we can endeavour to implement as many technical measures as it is reasonably possible: for the rest we must rely on the legal system that, it is worth reminding ourselves, has the final say. To put it differently: if a number of independent trustworthy persons (notaries, public officers, judges, honourable people) can testify they saw a certain signature being issued by a person different from the claimed one, no matter if the claim is strengthened by a number of technical measures, that signature will most probably be deemed as forged in court.

Let me conclude this preliminary discussion with this assertion that leads me back to the EU Directive and article 5(1): given the human impossibility to achieve certainty in the authenticity of an electronic signature, just as it occurs with handwritten signatures and with any other human deed, let us just be happy that, by applying all reasonably possible technical and organisational measures, a so called "qualified signature" or "art. 5(1) electronic signature" is equivalent to a handwritten one. In any case, it can be argued that a qualified signature is, by and large, more reliable than a handwritten one, provided that the technical and organisational preconditions are met.

The Italian case

Luigi Martin and Roberto Pascarelli pointed out in their article,[4] that Italy has a number of rules, the roots of which date back to 1997.[5]

The current Italian legislation, that may be changed by when the next issue of the e-Signature Law Journal is published, addresses four types of electronic signatures:

- the "simple" electronic signature (EU Directive article 2(1))
- the advanced electronic signature (EU Directive article 2(2))
- the qualified signature – meeting the requirements of EU Directive article 5(1)
- the digital signature – a qualified signature implemented through asymmetric cryptography.

As Martin and Pascarelli highlighted in their article, the Italian Legislator has included the digital signature in the new set of rules established by the Directive, considering it as a species within the wider genus of the qualified electronic signature, and hence of the advanced electronic signature. This is an interesting point, because it highlights the difference in the use of language between the lawyer and the technician. Let me now add my

[4] Dr Luigi Martin and Dr Roberto Pascarelli, *Electronic signature: value in law and probative effectiveness in the Italian legal system*, e-Signature Law Journal, Volume 1 Number 1, 2004, pp 17 – 22.
[5] See the list of the most prominent Italian rules of law at the end of this article.

views as a technical consultant in this discussion.

Italy, thanks to the former Autorità per l'Informatica nella Pubblica Amministrazione (Authority for IT in the Public Administration) (AIPA), now Centro Nazionale per l'Informatica nella Pubblica Amministrazione (National Centre for IT in the Public Administration – CNIPA), with an active cooperation by Assocertificatori (voluntary association of the certification authorities accredited as per the Italian rules of law) achieved a great result, which is often thought of as the Holy Grail: interoperability. Just to give an idea of the size of the Italian market, let me mention the following data, as of December 2004:

- CAs accredited as per the Directive: 18.
- Qualified certificates issued: over 1,700,000, all of them on Secure Signature Creation Devices (SSCD) meeting the requirements of the EU Directive Annex III.

Interoperability has been achieved in the following areas:

- certificate format
- certificate revocation list (CRL) format
- signature format
- SSCD.

Also, the procedures implemented by the several CAs to enrol users, to issue and maintain certificates, have reached an equal trust level on all CAs. The above results have been achieved for the reasons discussed below.

Detailed legal rules

The first Decree laying down the technical rules was issued as a Decree by the President of the Council of Ministers (DPCM) on 8 February 1999. It detailed the measures a CA had to put in place to achieve approval (now the Directive calls this "accreditation") by the then AIPA. These requirements have been updated by the new DPCM that replaced the previous one on 13 January 2004. These requirements are very detailed, to the point that no need is felt for a common policy document called by technicians "Certificate Policy",[6] since the requirements this document should provide are in fact painstakingly set out in this Decree, that as a matter of fact acts as the Italian Certificate Policy. It is a pity it is only available in Italian. What is required from the CAs is, instead, a document, that some compare to a Certification Practice Statement,[7] called Manuale Operativo (Operating Manual), that is to be approved by AIPA/CNIPA.

No reference is made in the Decrees to the more commonly acknowledged Certificate Policy and Certification Practice Statement. This is because it was actually drafted in 1998, well before publication of the de facto standard RFC 2527:[8] a law could not make reference to a document that had not been published. The current Decree does not include any further information in this respect. Similarly detailed requirements are defined for the secure signature creation devices (SSCD). The formats of certificates, certificate revocation lists, signatures were originally defined in an additional rule issued by AIPA in 2000 (AIPA/CR/24) and recently replaced by another CNIPA rule: its Deliberation 4/2005.

Compliance to all these requirements has been constantly monitored by AIPA/CNIPA, with the Assocertificatori support, and the result is that documents signed by anyone using one of the various signature creation or verification software clients and SSCDs distributed by the Italian accredited CAs, can be smoothly verified by any other user based on any other Italian accredited CA.

Farsightedness

In 2000, no major result had been achieved in the distribution of digital signatures, but in 2000, law 340/2000 was issued that, at article 31(2), requires applications, declarations and accompanying acts (e.g. Company books) to be deposited and sent by Companies to the Chambers of Commerce solely in electronic format, complying with law 59/1997 that opened the way to all the Italian rules on digital signature. In other words: they must be digitally signed. As a consequence, as of December 2004 over 1,200,000 certificates were issued to Company officers.

Additional impetus was given to the increased use of digital signatures by other rules of law specific to the Public Administrations, such as making the electronic document register mandatory since January 2004,[9] and by a number of Public Administrations initiatives regarding, among other things, e-purchasing. Other legal

[6] Certificate Policy: a named set of rules that indicates the applicability of a certificate to a particular community and a class of application with common security requirements.
[7] Certification Practice Statement: a statement of the practices that a certification authority employs in issuing, managing, revoking, and renewing or re-keying certificates.
[8] IETF RFC 2527 – Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework.
[9] Decree by the President of the Republic No 445 of 28 December 2000 art. 50.

I was blatantly wrong: digital signatures are too complex for the layman to understand and therefore to take full advantage of its benefits

provisions, addressing electronic registered mail (named "Certified e-mail"), electronic archiving, e-Invoicing, are triggering an increasing adoption and usage of the digital signature.

As an example, one among the largest Italian companies issues around 100,000 digitally signed and time stamped electronic invoices per month. For all of them, factoring is implemented and the factoring company is a French bank. So we can say that cross-border in digital signature is already a fact.

Another interesting item is the administrative and civil trial that can now be implemented by telematic means. This is so important that the Bar Association set up a CA of its own, that has obviously also been accredited, to issue digital signature certificates to lawyers. The rule of law enforcing this is the Decree by the Minister of Justice n. 123, of 13 February 2001 that states its scope in Art. 2(1): "Creation, communication and notification of acts for the civil trial is allowed through electronic documents …", and specifies in Art. 2(2): "Transmission, communication, notification of electronic document is done by telematics means through the civil Information technology system, …"

Is this all? Well, no.

A consolidated act on electronic documents, called "Code for the digital Administration", is to replace the previous Decree by the President of the Republic (DPR) 445/2000 and is approaching its issue date. This Decree may come into force by when this article is published. This "Code" will be a Legislative Decree that summarises and updates all rules regarding the relationships between Public Administrations, Citizens, Companies. This Decree will be such a "revolution", especially if you think of which is the country that is issuing it, that it might deserve an entire set of articles, both by legal and technical experts.[10]

A number of Regions have already launched, or are about to launch, projects on several areas, like health (Lombardy, for instance is in the process of issuing 9,000,000 certificates to its citizens for this purpose[11]), e-Government,[12] and e-procurement.[13]

The new rule on interoperability also extends the current number of acceptable electronic signature formats (only one now), in a way that will encompass also the most commonly used portable document format described in a number of official and de facto standards, the latest of which is RFC 3778.[14] No doubt this will give a further spurt to electronic signature usage.

The EESSI role

In February 1999, under the European Commission mandate M279, the ICT Standards Body launched the European Electronic Signature Standardisation Initiative, to develop a consistent standards set to support the EU Directive. This task was taken over by ETSI[15] and by CEN[16] who have since developed a number of standards covering all the electronic signature areas, among which: signature device protection profiles, certificate policies, electronic signature formats, certificate profiles, time stamp token profile. Explicit reference is made to these certificate and time stamp token profiles in the recently issued decree on interoperability.

Current implementations

Some of my colleagues say I usually am overly optimistic. In fact I had foreseen a brilliant and immediate future to digital signatures in 1999: it was too evident to me that private companies would be able to take advantage of digital signatures in terms of time and money saved. I was blatantly wrong: digital signatures are too complex for the layman to understand and therefore to take full advantage of its benefits.

But, step by step, changes are taking place both in the public and in the private sectors: I already mentioned the around 100,000 electronic invoices are issued per month by one company, an Italian car manufacturer. In addition:

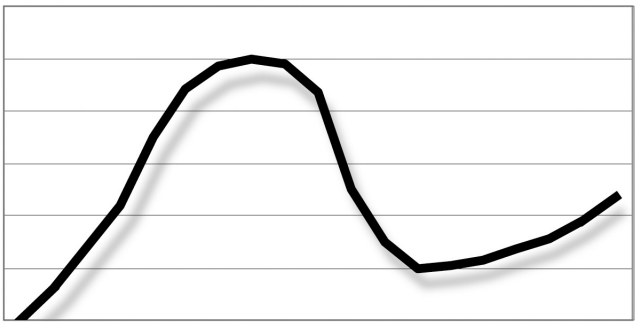
- The Public Administration is taking advantage of a unified negotiation performed by a centralised body that publishes the price list of several thousand goods in what is called Market Place, the purchase of which goods is increasingly being done electronically with orders issued and accepted with digital signatures.[17]
- The Lombardy health care project is taking off, albeit foreseeable hindrances are raised by users who are, largely, computer near-illiterate; an experience France has already had.[18]

[10] For a press release please visit http://www.innovazione.gov.it/eng/comunicati/2005/2005_02_11.shtml.
[11] See http://www.lisit.it/, although it is only in Italian.
[12] For a broad view on what is being done in this field please visit http://www.mininnovazione.it/eng/index.shtml.
[13] See http://www.acquistinretepa.it/, where you can find an overview in English.
[14] IETF RFC 3778 – The application/pdf Media Type.
[15] European Telecommunications Standards Institute.
[16] Comité Européen de Normalisation.
[17] See http://www.acquistinretepa.it/.
[18] See http://www.lisit.it/.

- Other Italian regions are following suite in the health care arena.[19]
- The electronic document register is now up and running in nearly all public administrations.[20]
- The Italian major banks have been accredited as CAs at CNIPA, in order to issue digital signature certificates to their customers to, finally, substitute the vulnerable ID and password system with something by and large more reliable.[21]
- The ICT company of the Ministry of Finance has been accredited as a CA at CNIPA; the possible consequences span from a minimal goal for Ministry internal usage, to a widespread distribution of certificates to taxpayers. It is too difficult to make a forecast as of now.[22]

An outlook

After an initial excitement (in years 1999 and 2000 I often had to split seminars on digital signatures because of the excess of applications to attend) the attention dwindled quite a bit: too much unmet hype raised by makeshift experts disappointed the public. Now that real achievements are not at hand but in our hands the interest of the public is more consciously increasing. If I may try to draw a curve, the interest of the public in digital signature is something like this: [This is an "attention" curve, not intended to quantify, merely to illustrate the point]



And as a matter of fact, as a consultant, I am now seeing a growing interest by large companies in e-invoicing, which was an easy prediction, but other implementations are getting real too.

- Electronic archival: the current official rules on this topic make it possible to destroy paper documents, provided they are archived abiding by the same rules.[23] This is the natural follow on to document electronic management for companies wishing to get rid of their paper archives. Once they experienced the usefulness of having all document in electronic format, the possibility to also legally destroy even official documents is becoming too tempting for them.
- The Ministry of Finance issued a Decree on 23/1/2004 enforcing digital signature and time stamping to all fiscal documents, not only for invoices, and this would be a natural consequence for companies that experienced e-invoicing.[24]
- The Ministry for Welfare issued a Decree and a Circular addressing the management of payrolls and roll lists through digital signature and time stamping.[25]

[19] See http://www.rete.marche.it/public/docu_fd.asp; http://www.regionedigitale.net/wcm/erdigitale/province/archivio.htm; http://www.e.toscana.it/home.shtml; http://www.provinz.bz.it/arbeit/1903/signatur_i/ (this is also in German) unfortunately these are in Italian.
[20] See http://protocollo.gov.it/.
[21] For the entire list of accredited CAs, visit http://www.cnipa.gov.it/site/it-IT/Attivit%c3%a0/Elenco_Certificatori_(firma_digitale)/.
[22] See http://www.sogei.it/index_eng.htm.
[23] See Deliberazione CNIPA/11/2004 – www.cnipa.gov.it.
[24] See http://gazzette.comune.jesi.an.it/2004/27/11.htm: Do not be surprised to find out it is neither the official Ministry of Finance site nor the Official Gazette site: it is a trustable site in any case, since it is managed by a Municipality.
[25] See http://www.welfare.gov.it/eachannel/menuistituzionale/lavoro/tutelacondizionidilavoro/rapporti+di+lavoro/norme/circolari/20031020circ+33+del+20+ottobre+2003.htm http://www.welfare.gov.it/EaChannel/MenuIstituzionale/normative/2002/2002-10-30-D.M.+30+ottobre+2002.htm.

European Directives 2004/17/EC[26] and 2004/18/EC[27] on e-procurement are too recent to predict when they will be implemented in the Italian legislation, but e-purchasing is already of interest among the Public Administrations: I am convinced that some day in the future we will see them issuing tenders on the internet.

I am also very sanguine on electronic documents being dealt with in a document workflow. This stems from the fact that the already mentioned Decree on interoperability paves the way to giving force of law also to the pdf internal signature format, which, in my opinion, is the real path to success for digital signature. I believe that when one person is able to draft a document, sign it, forward it to the next employee who applies any changes or additions they deem necessary and signs the resulting document, and so on until the document is finalised by the officer that, for example, makes it publicly available, then the real document workflow will be complete: in this case anyone will be able to see how the document exactly looked upon a specific employee's corrections. It is interesting to note that the Italian Social Security has already began using this type of process for one public pilot application addressing a wide number of people.

Do I need to specify further why I am sanguine on the digital signature future? ■

Franco Ruggieri is an independent consultant in the electronic signature field. Since 2001 he has co-operated with ETSI ESI, and with the now closed CEN El-sign workshop, in developing the electronic signature related standards in support of Directive 1999/93/EC. He also helped three Italian certification authorities obtain accreditation in accordance with the Directive.
FIR DIG Consultants, Lungomare delle Sirene 138, 00040 Pomezia, Italy

f.ruggieri@flashnet.it

Prominent Italian rules of law on digital signature

Legge 15 marzo 1997, n. 59 – Delega al Governo per il conferimento di funzioni e compiti alle regioni ed enti locali, per la riforma della Pubblica Amministrazione e per la semplificazione amministrativa. Art. 15(2) of this law is the paragraph relevant to digital signature that it introduces.

Decreto del Presidente della Repubblica (DPR) 10 novembre 1997, n. 513 – Regolamento recante criteri e modalità per la formazione, l'archiviazione e la trasmissione di documenti con strumenti informatici e telematici, a norma dell'articolo 15, comma 2, della legge 15 marzo 1997, n. 59. This Decree by the President of the Republic lays down the organisational and mostly legal requirements to implement Law 59/97 art. 15(2): in other words: it enforces the legal requirements for CAs and digital signature users (repealed by DPR 445/2000).

Decreto del Presidente della Repubblica (DPR) 20 ottobre 1998, n. 428 – Regolamento recante norme per la gestione del protocollo informatico da parte delle amministrazioni pubbliche . This decree lays down the legal requirements to implement the electronic document register (repealed by DPR 445/2000).

Decreto del Presidente del Consiglio dei Ministri (DPCM) 8 febbraio 1999 – Regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici ai sensi dell'articolo 3, comma 1, del Decreto del Presidente della Repubblica, 10 novembre 1997, n. 513. This Decree by the president of the Council of Ministers lays down the technical (very strict) requirements to implement DPR 513/97 (repealed by DPCM 13/1/2004).

Circolare 19 giugno 2000, n. AIPA/CR/24 – Art. 16, comma 1, dell'allegato tecnico al decreto del Presidente del Consiglio dei Ministri 8 febbraio 1999, pubblicato nella Gazzetta Ufficiale - serie generale - del 15 aprile 1999 n. 87 - Linee guida per l'interoperabilità tra i certificatori iscritti nell'elenco pubblico di cui all'art. 8, comma 3, del decreto del Presidente della Repubblica 10 novembre 1997, n. 513. This Circular, issued by the Authority for IT in the Public Administration,

[26] Directive 2004/17/EC of the European Parliament and of the Council of 31 March 2004 coordinating the procurement procedures of entities operating in the water, energy, transport and postal services sectors (OJ 30.04.2004 L 134/1);

[27] Directive 2004/18/EC of the European Parliament and of the Council of 31 March 2004 on the coordination of procedures for the award of public works contracts, public supply contracts and public service contracts (OJ 30.04.2004 L134/114).

laid down the technical provisions to achieve interoperability (superseded by Deliberation CNIPA 4/2005)

Legge 24 novembre 2000, n. 340 – Disposizioni per la delegificazione di norme e per la semplificazione di procedimenti amministrativi. This law specifies procedures and means to make administrative proceedings simpler. Article 31(2) makes it mandatory to deposit only digitally signed company documents at the Chambers of Commerce.

Decreto del Presidente della Repubblica (DPR) 28/12/2000, N. 445 – Recante il testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa. This decree summarises all provisions relevant to administrative documentation, including all the digital signature relevant provisions in DPR 513/97, DPR 428/98 on electronic document register, etc. that it repeals.

Circolare 7 maggio 2001, n. AIPA/CR/28 – Articolo 18, comma 2, del decreto del Presidente del Consiglio dei ministri 31 ottobre 2000, pubblicato nella Gazzetta Ufficiale 21 novembre 2000, n. 272, recante regole tecniche per il protocollo informatico di cui al decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 – Standard, modalità di trasmissione, formato e definizioni dei tipi di informazioni minime ed accessorie comunemente scambiate tra le pubbliche amministrazioni e associate ai documenti protocollati. This related to the technical rules to implement the electronic document register.

Decreto Ministero della Giustizia 13 febbraio 2001, n. 123 – Regolamento recante disciplina sull'uso di strumenti informatici e telematici nel processo civile, nel processo amministrativo e nel processo dinanzi alle sezioni giurisdizionali della Corte dei conti. This Decree by the Ministry of Justice lays down the organisational and Technical rules to implement the electronic civil and administrative trial.

Decreto del Ministro del Lavoro e delle Politiche Sociali 30 ottobre 2002 – tenuta dei libri paga e matricola. Decree by the Minister of Welfare on management and hold of payrolls and roll lists.

Circolare N. 33/03 del Ministero del Lavoro e delle Politiche Sociali 20 ottobre 2003 – Modalità applicative per la tenuta dei libri paga e matricola. Issued by the Minister of Welfare on the ways to manage and hold payrolls and roll lists.

Decreto Legislativo 23 gennaio 2002, n. 10 – Attuazione della direttiva 1999/93/CE relativa ad un quadro comunitario per le firme elettroniche. Legislative decree to implement Directive 1999/93/EC

Decreto del Presidente della Repubblica (DPR) 7 aprile 2003, n. 137 – Regolamento recante disposizioni di coordinamento in materia di firme elettroniche a norma dell'articolo 13 del Decreto legislativo 23 GENNAIO 2002, N. 10. This DPR provides legal and organisational rules on the implementation of Directive 1999/93/EC.

Decreto del Presidente del Consiglio dei Ministri (DPCM) 13 gennaio 2004 – Regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici. This DPCM provides technical rules on the implementation of DPR 137/2003 (repeals DPCM 8/2/99).

Deliberazione CNIPA 19 febbraio 2004 n. 11/2004 – Regole tecniche per la riproduzione e conservazione di documenti su supporto ottico idoneo a garantire la conformità dei documenti agli originali - Art. 6, commi 1 e 2, del testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa, di cui al decreto del Presidente della Repubblica 28 dicembre 2000, n. 445. This Deliberation by CNIPA provides technical rules on the implementation of electronic archival of documents, also of documents originally on paper, that can be destroyed after proper archival, with some exception for document with cultural relevance.

Deliberazione CNIPA 17 febbraio 2005 No 4/2005 - Regole per il riconoscimento e la verifica del documento informatico, published in the Official Gazette of the Italian Republic No 51 of 3 March 2005.