ARTICLE:

COMMENTS ON THE ITALIAN 'CODE FOR THE DIGITAL ADMINISTRATION'

By **Franco Ruggieri**

On 16 March 2005, the Official Journal of the Italian Republic (Gazzetta Ufficiale della Repubblica Italiana) published the new 'Codice Dell'Amministrazione Digitale' 'Code for the digital administration'.[1] Unusually, it was decided to enable the Code to be amended, and although not very common with Italian legislation, it was duly amended by Decreto Legislativo 4 aprile 2006, n. 159 (Dlgs 159/2006),[2] leading to its current version. The new Code has altered the Italian legal framework significantly. The changes are outlined in this article.

An outline of the main provisions of the Code

Those used to dealing with the Italian Public Administration will find this Code refreshing. The provisions set out in article 3(1) are significant:

> '1. I cittadini e le imprese hanno diritto a richiedere ed ottenere l'uso delle tecnologie telematiche nelle comunicazioni con le pubbliche amministrazioni e con i gestori di pubblici servizi statali nei limiti di quanto previsto nel presente codice.'
>
> '1. Citizens and companies have the right to request and obtain the adoption of information technologies in their communications with public administrations and with national utility providers within the limits laid down by the present code.'

Not only citizens and companies have the right to 'request', but, and this is the significant point, also to 'obtain' the adoption of information technologies in their communications with public administrations, both locally and nationally. The fans of René Goscinni and Albert Uderzo of Asterix may be aware that one of 'The Twelve Tasks of Asterix' (Les Douze travaux d'Astérix)[3] was to go through the 'The Place That Sends You Mad' 'Maison de la Folie administrative' mentally unscathed. This is where citizens were sent from one counter to the next just to withdraw papers to be submitted to the first one, to be sent to a third counter, and so on. Asterix finally succeeds by asking for an imaginary permit that nobody is aware of, causing pandemonium, and he is eventually given Permit A-38 to make him leave and stop causing trouble. The Code may end this incredible nightmare in Italy.

Unfortunately, the subsequent subsection to article 3(1) acts to limit the provisions of the Code:

> '1bis. Il principio di cui al comma 1 si applica alle amministrazioni regionali e locali nei limiti delle risorse tecnologiche ed organizzative disponibili e nel rispetto della loro autonomia normativa.'
>
> 'The principle asserted in paragraph 1 applies to regional and local administrations within the limits of their available technological resources'.

This means that the central administration is bound by this requirement, but local administrations can freely decide within the bounds of their autonomy if and when this requirement can be fulfilled.

Article 4 sets out what can be expected of public administration in the future:

[1] *Decreto legislativo 82/2005 del 7 marzo 2005 (in G.U. n. 112 del 16 maggio 2005) entrata in vigore 1 gennaio 2006, (Legislative Decree 82/2005 of March 7th 2005 (in Official Journal no. 112 of March 16th 2005) entered into force January 1st 2006.*

[2] *Disposizioni integrative e correttive al decreto legislativo 7 marzo 2005, n. 82, recante codice dell' amministrazione digitale (GU n. 99 del 29 aprile 2006 - Suppl. Ordinario n.105) (Legislative Decree No 159 of 4 April 2006, published in the Gazzetta Ufficiale della Repubblica Italiana N. 99 of 29 April 2006).*

[3] *An animated feature film based on the Asterix comic book series, with the screenplay written by Pierre Tchernia.*

The Protocollo Informatico complements the ability of people to obtain access to public documents in accordance with the data protection rules.

> ‘4. Partecipazione al procedimento amministrativo informatico.
>
> 1. La partecipazione al procedimento amministrativo e il diritto di accesso ai documenti amministrativi sono esercitabili mediante l’uso delle tecnologie dell’informazione e della comunicazione secondo quanto disposto dagli articoli 59 e 60 del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445.
>
> 2. Ogni atto e documento può essere trasmesso alle pubbliche amministrazioni con l’uso delle tecnologie dell’informazione e della comunicazione se formato ed inviato nel rispetto della vigente normativa.’

Paragraph 1 states that citizens can exert the right to participate in the administrative proceedings and to obtain access to administrative documents through ICT technology (each administration will define which terms for this usage are relevant to its own needs), and paragraph 2 states that any act or document can be transmitted to public administrations through ICT technologies, provided the document is compliant with the rules in force.

The provisions of the Code reinforce the rights and powers that are relevant to the ‘Protocollo informatico’ (‘electronic document register’),[4] by which public administrators must record each and all the documents received from outside or sent from within the organization. The Protocollo Informatico complements the ability of people to obtain access to public documents in accordance with the data protection rules. The requirements of the Protocollo informatico fits well within the provisions of article 4(1) regarding the establishment of electronic dossiers by public administrations. Now ‘duly’ authorised persons, even from outside the administration, will be able to obtain secure access to both the Protocollo and the dossiers to ascertain the status of a specific proceeding.

The provisions of article 38 represent a further advance: it is possible to implement electronic fund transfers between public administrations and members of the public, provided that the technical rules, to be specified in a subsequent Decree, are met. Article 5 requires central public administrations to be in a position to make electronic payments possible from 30 June 2007.

Article 6 provides that central public administrations, and, where not differently provided for, local administrations, are required to make use of the ‘registered electronic mail’ (Posta Elettronica Certificata) for each and every exchange of documents and information with anyone who requests this type of exchange. This means that if a legal or natural person demands the exchange documents with a specific administration via registered e-mail, the administration is required to use registered e-mail.[5] However, the proposed changes are subject to a subtle provision in article 40(1):

> ‘1. Le pubbliche amministrazioni che dispongono di idonee risorse tecnologiche formano gli originali dei propri documenti con mezzi informatici secondo le disposizioni di cui al presente codice e le regole tecniche di cui all’articolo 71.’

[4] *The Protocollo Informatico is governed by the Decreto Del Presidente Della Repubblica 28 dicembre 2000, n. 445 Disposizioni legislative in materia di documentazione amministrativa. (Testo A) (pubblicato nella Gazzetta Ufficiale n. 42 del 20 febbraio 2001- Supplemento ordinario n. 30) (Decree by the President of the Republic No 445 of 28/12/2000), that absorbed the Decreto Del Presidente Della Repubblica No. 428/1998 Regole tecniche per il protocollo informatico di cui al DPR 20 ottobre 1998, n. 428 (Decree by the President of the Republic No 428 of 20 October 1998), and by the implementation rules of law Decreto PCM del 31/12/2000: Regole tecniche per il protocollo informatico di cui al DPR 20/10/1998 n.428 Circolare AIPA del 7/5/2001 di cui all.art. 18, comma 2, del DPCM (Decree by the President of the Council of Ministers – DPCM – of 31/10/2000, AIPA Circular Letter AIPA/CR No 28 of 7 May 2001).*

[5] *The Technical Committee ‘ Electronic Signatures and Infrastructures’ of the European Telecommunications Standards Institute (ETSI) is developing through its Specialised Task Force (STF) 318 a set of Technical Specifications with the purpose of providing a set of standards for Registered E-Mail. These Specifications are expected to be published in the second half of 2008.*

The ' digital signature' is not referred to in the Code as the basic cryptographic mechanism, but it means a Qualified Electronic Signature based on asymmetric cryptography.

> '1. Public administrations that have adequate technological resources shall form the original copies of their documents using information technology according to the provisions of this code and the technical requirements set out in Article 71.'

This provision appears to apply to the preparation of documents, but everything can be deemed a 'document'. This means that the provisions of this paragraph might enable an administration to circumvent the rules on the basis that it does not have the necessary technological resources. Article 40(2) attempts to provide an economic rationale for not putting too much on paper, and taken in combination with article 40(3), there is an attempt to ensure that suitably equipped administrations can keep drafting (or copying) documents on paper only in cases that will be addressed by a subsequent Decree. Article 7 requires the ICT implementation of public administrations to be monitored by two Ministries each year, the Ministro delegato per la funzione pubblica and the Ministro delegato per l'innovazione e le tecnologie.

Electronic signature

Although the Code does not refer to the advanced electronic signature, it has retained the term 'digital signature' as a legacy from the previous law. The 'digital signature' is not referred to in the Code as the basic cryptographic mechanism, but it means a Qualified Electronic Signature based on asymmetric cryptography. This means the Code now refers to the electronic signature, the Qualified Electronic Signature and the digital signature. This implies that, whenever an advanced electronic signature is required, it is necessary to 're-invent' it again, by calling it a different name and assigning it the same characteristics as provided for in article 2(2) of the Directive.[6]

The legal effectiveness of Qualified Electronic Signatures

The previous law, now having been replaced by the Code, was extensively covered by Dr Luigi Martin and Dr Roberto Pascarelli,[7] so the differences need to be considered. The previous Decree, Decreto del Presidente della Repubblica (DPR) 28 dicembre 2000, n. 445 provided, in article 10(2), as follows:

> 'Il documento informatico, sottoscritto con firma elettronica, soddisfa il requisito legale della forma scritta. Sul piano probatorio il documento stesso é liberamente valutabile, tenuto conto delle sue caratteristiche oggettive di qualità e sicurezza. Esso inoltre soddisfa l'obbligo previsto dagli articoli 2214 e seguenti del codice civile e da ogni altra analoga disposizione legislativa o regolamentare.
>
> Il documento informatico, quando è sottoscritto con firma digitale o con un altro tipo di firma elettronica avanzata, e la firma è basata su di un certificato qualificato ed è generata mediante un dispositivo per la creazione di una firma sicura, fa inoltre piena prova, fino a querela di falso, della provenienza delle dichiarazioni da chi l'ha sottoscritto.'
>
> 'The electronic document, when subscribed with an electronic signature, fulfills the requirement of legal writing. On the evidence the document itself is freely evaluated, in view of its objective characteristics of quality and safety. Furthermore it fulfils the obligation in accordance with articles 2214 and subsequent of the civil code and in accordance with any other legislative or regulatory provision.
>
> The electronic document, when it is signed with a digital signature or with any other type of advanced

[6] *Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, OJ L 13, 19.01.2000, p.12.*

[7] *Dr Luigi Martin and Dr Roberto Pascarelli, ' Electronic signature: value in law and probative effectiveness in the Italian legal system' , Digital Evidence and Electronic Signature Law Review, 1 (2004) 19 - 24.*

> electronic signature, and the signature is based on a qualified certificate and was generated with a secure signature creation device, also provides full evidence, until a complaint of a false signature of the origin of declarations from the subscriber,

Article 21(2) of the new Code instead makes explicit reference to article 2702 of the Italian Civil Code:

> '2. Il documento informatico, sottoscritto con firma digitale o con un altro tipo di firma elettronica qualificata, ha l'efficacia prevista dall'articolo 2702 del codice civile. L'utilizzo del dispositivo di firma si presume riconducibile al titolare, salvo che questi dia la prova contraria.'

> '2. The document, when subscribed with a digital signature or another type of qualified electronic signature, is effective as provided for under Article 2702 of the Civil Code. The use of the signing creation device is presumed as being that of the owner, unless they give evidence to the contrary.'

Article 2702 of the Civil Code states as follows:

> 'La scrittura privata fa piena prova, fino a querela di falso (Cod. Proc. Civ. 221 e seguenti), della provenienza delle dichiarazioni da chi l'ha sottoscritta, se colui contro il quale la scrittura è prodotta ne riconosce la sottoscrizione, ovvero se questa e legalmente considerata come riconosciuta (Cod. Proc. Civ. 214, 215; Cod. Nav. 178, 775).'

> 'The private writing gives full evidence, except where there is a complaint of a false signature (Cod. Proc. Civ. 221 et seq), of the origin of the declarations of the person who signed it, if the person whose signature it is acknowledges the subscription, or if it is legally considered as recognized (Cod. Proc. Civ. 214, 215; Cod. Nav. 178, 775).'

The Code provides a presumption that when a person has issued a digital signature or another type of qualified electronic signature, they are presumed to have used their own signature creation device, and if they claim the signature was not affixed by them, they have to prove they did not affix the signature to the document. This is reinforced by the provisions of article 20(2), added by article 8 of Dlgs 159/2006, which states as follows:

> '2. Il documento informatico sottoscritto con firma elettronica qualificata o con firma digitale, formato nel rispetto delle regole tecniche stabilite ai sensi dell'articolo 71, che garantiscano l'identificabilita' dell'autore, l'integrita' e l'immodificabilita' del documento, si presume riconducibile al titolare del dispositivo di firma ai sensi dell'articolo 21, comma 2, e soddisfa comunque il requisito della forma scritta, anche nei casi previsti, sotto pena di nullita', dall'articolo 1350, primo comma, numeri da 1 a 12 del codice civile.'

> '2. A document signed with qualified electronic signature or digital signature, formed in compliance with the technical requirements established under Article 71, which guarantee the identity of the author, and the integrity of the document, is assumed to be ascribed to the holder of the signature creation device in accordance with Article 21, paragraph 2, and still meets the requirement of writing, even in cases provided under penalty of invalidity, by 1350, the first paragraph numbers from 1 to 12 Civil Code.'

The article of the Civil Code referred to, covers contracts, acts of waiver, and acts that provide for life annuities, amongst others. In essence, it appears that all legal acts regarding the Civil Code can be drafted electronically and signed with a qualified electronic signature.

But another interesting provision has been added to the Code by the addition of a sentence to article 32(1) by article 14 of the Dlgs 159/2006. Article 32(1) now reads:

> '1. Il titolare del certificato di firma è tenuto ad assicurare la custodia del dispositivo di firma e ad adottare tutte le misure organizzative e tecniche idonee ad evitare danno ad altri; è altresì tenuto ad utilizzare personalmente il dispositivo di firma.'

> '1. The owner of the signature certificate is required to ensure the custody of the signature creation device and to take all necessary organizational and technical measures capable of preventing damage to others; he is also required to personally use the signature creation device.'

The implications of article 32(1) mean that a person can no longer entrust their smart card and the related activating PIN to a person they trust to enable him or her to act on behalf of the card holder, even if the card holder cannot use the card themselves (perhaps because they are frail or physically incapable of using a smart card) and bear the consequences for what the trustee does with their smart card on their behalf. For example, the chief accountant of Telecom Italia cannot entrust a signing creation device bearing his own private key to the ITC operator in charge of issuing electronic invoices that must be signed in accordance with European Directive 2001/115/EC:[8] each single operator have to be issued a signing certificate, and will be necessary to issue the invoices with their own Qualified Signature (Italian legislation requires electronic invoices, when signed, to be signed with a Qualified Electronic Signature: Decreto del 23 gennaio 2004 Modalità di assolvimento degli obblighi fiscali relativi ai documenti informatici ed alla loro riproduzione in diversi tipi di supporto (G.U. n. 27 del 3 febbraio 2004 n. 27) (Decree by the Minister of Economy and Finance DMEF 23/1/2004).

A number of further changes have been introduced, such as the provisions of article 32(3)(j), that require the certification authority to keep all the information relating to a qualified certificate for at least twenty years from the date it was issued. Furthermore, article 25 of the new Code, provides for a public officer to attest by electronic means that an electronic signature has been issued in their presence. The article reads as follows:

> '25. Firma autenticata.
>
> 1. Si ha per riconosciuta, ai sensi dell'articolo 2703 del codice civile, la firma digitale o altro tipo di firma elettronica qualificata autenticata dal notaio o da altro pubblico ufficiale a ciò autorizzato.
>
> 2. L'autenticazione della firma digitale o di altro tipo di firma elettronica qualificata consiste nell'attestazione, da parte del pubblico ufficiale, che la firma è stata apposta in sua presenza dal titolare, previo accertamento della sua identità personale, della validità del certificato elettronico utilizzato e del fatto che il documento sottoscritto non è in contrasto con l'ordinamento giuridico.
>
> 3. L'apposizione della firma digitale o di altro tipo di firma elettronica qualificata da parte del pubblico ufficiale ha l'efficacia di cui all'articolo 24, comma 2.
>
> 4. Se al documento informatico autenticato deve essere allegato altro documento formato in originale su altro tipo di supporto, il pubblico ufficiale può allegare copia informatica autenticata dell'originale, secondo le disposizioni dell'articolo 23, comma 5.'

> '25. Authenticated signature.
>
> 1. It is recognized, in accordance with Article 2703 of the Civil Code, if the digital signature or other type of qualified electronic signature is certified by a notary or other authorized public official.
>
> 2. The authentication of digital signatures or other qualified electronic signature consists of the attestation by the public official that the signature was affixed in his presence by the owner after assessing his personal identity, of the validity of an electronic certificate used and the fact that the document signed is not contrary to the legal system.
>
> 3. The affixing of the digital signature or other type of qualified electronic signature by the public official has the effectiveness of Article 24, paragraph 2.
>
> 4. To be authenticated, the document must be attached to a document in original format on another kind, the public official can attach to the data an authenticated electronic copy of the original, in accordance with the provisions of Article 23, paragraph 5.'

The provisions of this article raise the bar for would-be attackers trying to compromise a private key or to compel the signatory to subscribe to an offer they cannot refuse. When authenticating the electronic signature, the public officer is required to ascertain if the signing party is the owner of the certificate, thus preventing certain attacks that are describe in the next paragraph, and whether the person has signed the document freely.

Establishing the credentials of the signing party

When using a digital signature, the Certification Authority (CA) maintains Certificate Revocation Lists (CRL), used to post details of certificates that have been revoked for some reason. There is another mechanism

[8] *Council Directive 2001/115/EC of 20 December 2001 amending Directive 77/388/EEC with a view to simplifying, modernising and harmonising the conditions laid down for invoicing in respect of value added tax, OJ L 15, 17.1.2002, pp. 24–28.*

that can be used for the same purpose. This is provided by a trusted service provider. The trusted service provider offers to provide relevant information about a specific certificate. The recipient of a message signed with a digital signature can make a request to a trusted service provider to provide them with the status of the certificate. Where such a request is made, the trusted service provider replies with a response such as 'good, no good, do not know', using the Online Certificate Status Protocol (OCSP) defined in IETF RFC 2560. Unfortunately, this is easier to explain than execute, for a number of reasons that cannot be covered in this article, because they are too technical and require a detailed explanation. It is for this reason that the Italian legislation, whilst not forbidding the use of OCSP, explicitly requires that CRLs must be used, and that any information provided by the OCSP must be consistent with the information provided by a CRL.

Anatomy of an attack

A Certification Authority should issue a Certificate Revocation List at defined intervals. The interval will differ as between Certification Authorities, but a 12 hour interval is not inconceivable. Every CRL specifies what is technically called the 'nextUpdate', that is, the time at which a new CRL will be issued. A CA might issue 'extemporary' CRLs,[9] which may be issued at any time, and these can become subject to the 'man in the middle' attack. Assume an attacker (Alice) is interested in compromising the signing private key of an individual (Bob), so to cause another person (Carol) to rely on an error. The sequence would be:

> Alice gets ready to compromise Bob's signing private key quickly (there may be several methods: a PIN of a smart card can be captured via micro-cameras as occurs at times near an ATM machine).
>
> Alice stores a CRL soon after it is issued.
>
> Alice compromises Bob's key.
>
> Alice produces a fake document with Bob's compromised key and sends it to the victim (Carol).
>
> The CA issues an contemporaneous CRL, perhaps one hour after the previous CRL.
>
> When Carol tries to download the current CRL to verify if Bob's certificate is valid, Alice intercepts this request and sends back to Carol the previously stored CRL, where the certificate at issue is obviously not listed.
>
> Carol would see that the CRL has not yet expired, since the time specified in the nextUpdate has not passed, and would trust it. The attack would then succeed.

A crucial issue is that the recipient should always verify the certificate and thereby become a relying party,[10] and when they verify the certificate, the method they use to verify it. One question is whether they should wait until a CRL is issued after the time the document was signed, or at least after the time the document was received, and assume that this CRL is reliable. If this course of action is taken, then the usefulness of an extemporary CRL is debatable. The real issue is to assess the actual risk, which in turn depends on how important the consequences of a successful attack might be.

Converting paper documents to digital documents

The provisions of article 23 are of interest, since they clarify when a notary or a similar public officer is required to validate a conversion from paper to digital format by scanning: validation using a digital signature or other qualified electronic signature is necessary when the analogue document is considered to be a 'unique original'. The technical rules currently in force in this regard, are set out in Deliberazione CNIPA n. 11/2004 del 19 febbraio 2004[11] (Deliberation No 11 of 2004 by the Italian National Centre of IT in the Public Administration (CNIPA)) which provides, in article 1(1)(c):

> 'documento analogico originale: documento analogico che puo' essere unico oppure non unico se, in questo secondo caso, sia possibile risalire al suo contenuto attraverso altre scritture o documenti di cui sia obbligatoria la conservazione, anche se in possesso di terzi;'
>
> 'analogue original document: an analogue document can be unique, or not unique if it is possible to retrieve the content through other writings or

[9] *The word 'contemporaneous' CRL is used by some people, somewhat erroneously.*

[10] *Stephen Mason, Electronic Signatures in Law, (Tottel, 2nd edn, 2007), 12.2.*

[11] *G.U. 9 marzo 2004, n. 57.*

documents that must be conserved, even if they are in possession of third parties.'

Requirements placed on Certification Service Providers

All administrators and legal representatives of Certification Service Providers (CSP) established in Italy, even those that do not issue qualified certificates, must abide by the same 'honourableness' rules that apply to similar officers in the banking world, as provided in article 26(1) of the Code:

> 'L'attività dei certificatori stabiliti in Italia o in un altro Stato membro dell'Unione europea è libera e non necessita di autorizzazione preventiva. Detti certificatori o, se persone giuridiche, i loro legali rappresentanti ed i soggetti preposti all'amministrazione, devono possedere i requisiti di onorabilità richiesti ai soggetti che svolgono funzioni di amministrazione, direzione e controllo presso le banche di cui all'articolo 26 del testo unico delle leggi in material bancaria e creditizia, di cui al decreto legislativo 1° settembre 1993, n. 385, e successive modificazioni.'

> 'The activities of certification service providers established in Italy or in another EU Member State is free and does not require prior authorization. Such certification service providers or, if legal persons, their legal representatives and those responsible for their administration, must meet the requirements of honourableness required of persons who perform administrative functions, direction and control at the banks under Article 26 of the single text laws in material banking and credit, of Legislative Decree 1 September 1993, No 385, and subsequent amendments.'

This requirement gives a remarkable standing, and responsibility, to CSPs, even to those that do not issue qualified certificates.

The requirements are even more stringent for CSPs seeking accreditation in accordance with the provisions of article 3(2) of Directive 1999/93/EC: the CSP auditors must also comply with the 'honourableness' rules, and the company's capital must be at least equal to the minimum required for banks (article 29(3)). All the other Directive 1999/93/EC requirements on CSPs issuing qualified certificates are met, nor it could be differently, but a few of them deserve some attention:

> no copy of any signatory's private key can be kept by the CSP; (Art 32(3)(f))

> the CSPs can be requested to revoke a certificate that has been issued, not only upon the lawful request of the owner of the certificate, but also when the request comes from an authorized party, such as the person upon whose authorization the certificate was issued, or a legal authority; certificates are also to be revoked when the CSP becomes aware of certain objective conditions that require revocation, such as the subscriber's disabilities or misbehaviour, independently of any request by the owner or by any authorized entity; (Art 32(3)(g))

> the CSPs do not need prior authorisation to operate (Art 26(1)), but, since they are subject to supervision, in accordance with Directive 1999/93/EC article 3(3), they must inform CNIPA, the supervisory body, before starting their operations (Art 27(3));[12] should it transpire that do not abide by the rules, CNIPA has the power to stop their operations and to require revocation of the certificates that have been issued, although it can grant a period of grace to the certification service provider to resolve the shortcomings, where applicable.

Requirements placed on public administrations

Public administrations (article 34) that wish to issue certificates to be used by their own employees in their official relationships with external entities, be they citizens, companies or even other public administrations, have to meet very specific requirements. Public administrations can only issue qualified certificates, and they must achieve accreditation in accordance with Directive 1999/93/EC article 3(2). The rationale for imposing such conditions rests with the fact that public administrations are required to make use of what is considered to be the 'best of breed' certificates. However, it is important to understand that these requirements complement the provisions set out in article 65(1) that, briefly, requires documents submitted by citizens to public administrations to be digitally signed; alternatively, they can be submitted over the internet, provided that the person submitting the document is identified by using their Electronic Identity Card (CIE) or National Services Card (CNS).

[12] *The CNIPA is the accreditation body, and keeps a list of accredited Certification Service Providers.*

It is possible to suggest that these provisions may limit the free circulation of goods and services within the European Union.[13] However, it can be argued, given the objective standing of a public administration, that a Member State can and should provide appropriate security measures, including cyber-measures, to protect its public administrations and therefore the state, as explicitly allowed by article 3(7) of Directive 1999/93/EC. On the other hand, given the increasing number of accreditation schemes being implemented in the EU Member States, this is more a theoretical than an actual hindrance to free competition.

Article 34 also enables a public administration to issue certificates to external entities (other administrations, citizens, companies), although these certificates can only be used between the person or legal entity with a certificate and the administration that issued the certificate. A public administration can agree that a commercial CSP issues the certificates on its behalf, provided the latter has been accredited in accordance with article 3(2) of Directive 1999/93/EC. Public administrations are encouraged to make use of commercial CSPs, because another specific rule of law (DPR 445/2000, art. 64(1)) requires them to assess the cost and benefits each time they intend to implement any new IT procedure, although for the same reason, public administrations can adopt, for their internal use, any solution they choose, without any limit (article 34(2)).

By 1 January 2008, all public administrations must be equipped with procedures and software applications suitable to verify digital signatures, as set out in article 34(5):

> 'Entro ventiquattro mesi dalla data di entrata in vigore del presente codice le pubbliche amministrazioni devono dotarsi di idonee procedure informatiche e strumenti software per la verifica delle firme digitali secondo quanto previsto dalle regole tecniche di cui all'articolo 71.'
>
> 'Within twenty-four months from the date of entry into force of this code, the public administrations must have adequate procedures and software tools for the verification of digital signatures as set out in the technical requirements laid down in Article 71.'

The technical requirements will be specified in technical decrees to be issued at a later date. Unfortunately, the Code does not provide any sanctions for administrations that do not provide such services, but this would have been impolitic. Moreover, there are also the provisions of article 40(1), that 'Public administrations *that have adequate technological resources* .....', which means the politicians have toned down the provisions, because a provision had in fact been in force in the Italian legislation since March 1998 (Regolamento attuativo DPR 513/97, (G.U. nº 60 13/3/1998) (DPR No 513 of 10 November 1997, published in the Official Journal on 13/3/1998), (Articles 20 and subsequent ones) that bound all public administration to adopt the electronic signature, but without success.

Adopting the signature

Article 35 of the Code mandates that any secure signature creation device and procedure used to issue an electronic signature (without any distinction) must enable the document to be submitted to the signer's examination before the signature is generated, except where an automatic signing procedure is in use. In the latter case, however, this procedure must be activated upon the explicit instructions of the signing party, and their will is to be made evident for each automatically signed document, as provided in article 35(3):

> 'Il secondo periodo del comma 2 non si applica alle firme apposte con procedura automatica. L'apposizione di firme con procedura automatica è valida se l'attivazione della procedura medesima è chiaramente riconducibile alla volontà del titolare e lo stesso renda palese la sua adozione in relazione al singolo documento firmato automaticamente.'
>
> 'The second sentence of paragraph 2 shall not apply with signatures affixed by an automatic procedure. The affixing of signatures by an automatic procedure is valid if the same procedure is clearly attributable to the will of the owner and the same as to reveal its adoption in relation to each single document signed automatically.'

This provision of the Italian Code appears to be reasonable and practical, especially when an organization needs to sign a batch of invoices, by way of example. However, the requirement that the signing procedure must be activated upon the explicit act of will

[13] *Jos Dumortier, Stefan Kelm, Hans Nilsson, Georgia Skouma and Patrick Van Eecke The legal and market aspects of electronic signatures; Stefan Kelm, ' On the implementation of the 1999 European Directive on electronic signatures' , Digital Evidence and Signature Law Review, 2 (2005) 7 - 15.*

by the signer is, it seems, tantamount to giving the signer responsibility for each signature in any event.

Secure signature-creation devices

Requirements are provided for in article 35 in respect of secure signature-creation devices (SSCDs) and procedures used to issue electronic signatures, as specified in Annex III of Directive 1999/93/EC. Moreover, article 35(4), (5) and (6) require that the SSCDs used to issue Qualified Electronic Signatures must be certified as meeting the requirements set out in Annex III of Directive 1999/93/EC by national bodies of the European Union Member States. Member States must notify the European Commission and other Member States of the names of their respective national bodies. This is not a problem for smart cards and similar devices.

There is some doubt about Hardware Security Modules (HSM), which are high performance hardware signing devices used by Certification Authorities, Time Stamping Authorities and others. It is difficult to see how HSM manufacturers will commit to spending a remarkable amount of money (in the order of magnitude of some hundred thousand euros) to achieve certification for a device that would only sell in very small quantities. If such devices are sold in such limited numbers, it has to be wondered what their resale cost will be. This could be a real hindrance to the diffusion of digital signatures.[14]

Storage of digital documents

Articles 42, 43 and 44 refer to the storage of digital documents. The term 'storage' is a useful term, but is can also mean 'archive'. However, it is necessary to make a distinction between what can be termed an 'operational' archive, for the purpose of making documents immediately retrievable by many persons simultaneously, and 'conservation' storage for the purposes of auditing, possibly for many years. In fact they have different requirements.

Operational storage

The basic requirement of an 'operational' archive is to enable the fast retrieval of documents by many people simultaneously, to facilitate daily operational requirements; the security measures need only be sufficient to ensure the documents are not lost or altered by accident: there is no need to grant them legal validity.

Conservation storage

The purpose of 'conservation' storage is to ensure in the long term that the digital document is the 'original' document, or an exact copy of the paper document; the length of time taken to retrieve the document is less important: the aim is to is support auditors in fulfilling their duties. It is only an added bonus if it is possible to achieve dynamic and multiple access for this form of storage.

The Code addresses the second type of storage, and it is remarkable that another law already in force, the Deliberazione CNIPA n. 11/2004, specifically addresses this subject by laying down the technical and organisational rules on how this is to be implemented. The main provisions are as follows:

> There are no additional requirements to the storage of electronic documents signed with an electronic signature (article 3).
>
> Analogue documents (paper, microfilm) can be stored electronically under the sole responsibility of the organisation (article 4(1)).
>
> The only exceptions are what are termed 'unique' analogue documents, that is, analogue documents of which no copy exists and the content of which cannot be derived from other existing documents. The storage of these unique analogue documents requires an additional qualified signature by a public officer (notary, public administration official, and the like), asserting that the stored object accurately represent the analogue original (article 4(2)).
>
> When the storage media is closed, a qualified electronic signature is to be issued by the person appointed by the organisation performing the storage and, where the cases of the previous items occur, by a public officer, plus a Time Stamp Token (articles 3(1), 4(1), 4(2)).
>
> No additional mechanism or procedure is required, although organisations are free to adopt additional measures. In fact, the validity of the storage must be guaranteed by the organisation's security measures. This is an important point, since it makes clear that the security of the storage measures in place rely on the organisation's structure and procedures, and that additional technical measures are just an additional

[14] *The author agrees with the comments by Stefan Kelm in relation to this issue, ' On the implementation of the 1999 European Directive on electronic signatures' , Digital Evidence and Electronic Signature Law Review.*

feature, not an essential element (article 8).

With respect to the acts of notaries, article 39 of the Code provides that all documents that must be retained, including notary acts, can be kept in electronic format, provided that they meet the requirements specified in relevant technical Decrees:

> 'I libri, i repertori e le scritture, ivi compresi quelli previsti dalla legge sull'ordinamento del notariato e degli archivi notarili, di cui sia obbligatoria la tenuta possono essere formati e conservati su supporti informatici in conformità alle disposizioni del presente codice e secondo le regole tecniche stabilite ai sensi dell'articolo 71.'

> 'The books, directories and books, including those provided by law upon the Notaries and notarial archives, which are mandatory to retain can be formed and stored electronically in accordance with the provisions of this Code and in accordance with the technical rules established under Article 71.'

On a final note, while in a number of other jurisdictions detailed requirements are provided relating to the media documents in digital format can be stored, Italy has adopted a pragmatic approach to the issue, as set out in article 6(1) of Deliberazione CNIPA n. 11/2004, which states:

> '1. Il documento conservato deve essere reso leggibile in qualunque momento presso il sistema di conservazione sostitutiva e disponibile, a richiesta, su supporto cartaceo.'

> '1. The document that is stored must be made legible at any time at the place of conservation and must be made available, upon request, on paper.'

It is simple: the organisation must exhibit the document, and if it is not able to, then it will incur any sanctions provided for by the relevant legislation. The organization does not have the excuse that it adopted the relevant hardware and software as required by law, and it is not their fault that the document cannot be retrieved. In Italy, it is for the organisation to ensure they can exhibit the document.

Posta Elettronica Certificata

Registered e-mail is a further facility that is addressed in article 48, by specifying the Posta Elettronica Certificata (PEC), that means precisely "registered e-mail". The organisational requirements of the PEC are set out in the Decreto del Presidente della Repubblica 11 febbraio 2005, n.68 "Regolamento recante disposizioni per l'utilizzo della posta elettronica certificata, a norma dell'articolo 27 della legge 16 gennaio 2003, n. 3. (G.U. 28 marzo 2005, n. 97)" (Decree by the President of the Republic No 68 of 11 February 2005 (Gazzetta Ufficiale No 97 of 28 March 2005)), specifically mentioned by the Code, while the technical requirements are set out in an additional, specific Presidenza Del Consiglio Dei Ministri, Dipartimento Per L'Innovazione e Le Technologie Decreto 2 novembre 2005 Regole tecniche per la formazione, la trasmissione e la validazione, anche temporale, della posta elettronica certificata (tutti i requisiti tecnico-funzionali che devono essere rispettati dalle piattaforme utilizzate per erogare il servizio) (G.U. del 15 novembre 2005, n. 266) (Decree by the President of the Counsel of Ministers issued on 2 November 2005 (Gazzetta Ufficiale No 266 of 15 November 2005)).

The purpose of PEC is to apply the mechanisms of the ordinary paper registered mail to e-mail, with the additional requirement that users must register themselves at their own PEC provider.

When sending an e-mail using the PEC, the sender is electronically authenticated and is provided with a receipt signed by the PEC provider; this receipt states that the provider accepted a certain e-mail at a certain moment from the specific sender. Moreover, since the recipient's server is supposed to be able to reliably identify who the actual recipient is that has rightful access to the relevant mail box, the sender will also be provided with a receipt stating that a certain e-mail was deposited in the correct recipient's mail box at a certain moment in time. This provides the sender with a means to lawfully uphold an assertion that, effective at a certain moment, an e-mail was available in the mailbox for the intended recipient, or for an authorized delegate. The sender is not at fault if the recipient fails to open the mailbox to open the e-mail. An interesting aspect of the receipt, is that it bears the entire e-mail that was sent, unless otherwise required by the sender. This provides a great advantage over the postal mail, because in the latter case a recipient can claim that they received the envelope by registered mail, but the envelope did not contain anything.

The service does not extend to inform the sender if the e-mail was opened. Similarly, PEC does not address confidentiality or authenticity of the documents sent: it is for the sender to decide to encrypt, or to encrypt and sign the document.

In particular, article 47(2), provides that communications between public administrations can be carried out by e-mail, provided their origin is verified. It is also provided that the origin of the e-mail can be ascertained when a digital signature or a qualified electronic signature is used; when the Protocollo Informatico keeps track of the e-mails; in any other case where it is possible to ascertain the origin of the e-mail, and when PEC is used. All public administrations were required set up a PEC mail box from 1 September 2006 (Art. 47(3) of the Code).

Electronic identity and authentication cards

Italy is one of the countries where identity cards have been in force for a very long time. In 1999, Italy began planning the introduction of an Electronic Identity Card, called Carta d’Identità Elettronica. Given the complexity of the project, there have been a number of pilot phases and such like, and the legal, organisational and technical aspects have been addressed by a number of laws and decrees.

Now, article 66 of the Code addresses the two types of identity or authentication cards: the ‘Electronic Identity Card’ (CIE) and the ‘National Services Card’ (CNS). In summary, the CIE is a smart card that purports to meet two requirements: face to face identification and on-line authentication. The CIE is produced by the Italian Mint.[15]

The reader will note that, in addition to the usual data and photograph of the purported holder of the card, an optical memory band is present on the rear. The purpose of this optical band is to implement security measures suitable to prevent counterfeiting by modifying the data. On the left part of the optical memory band, there is an embedded hologram, which is created when the card is prepared for the individual, that reproduces the document number and the photograph of the holder of the document that is printed in colour on the front of the card. This feature, like the hologram, is visible under a specific light source. The chip has the usual function of an authentication card: it has a signing capability that is supported by an authentication certificate issued by the Ministry of the Interior. This means that the issuing of a CIE certificate is controlled by the relevant Ministry service, the Sistema di Sicurezza per il Circuito di Emissione (Issuing Circuit Security System). As of March 2007, in accordance with the official CIE site, the Municipalities involved in issuing the CIE totalled 3 million, out of population of almost 57 million.

In the effort to speed up ‘e-Democracy’, the Carta Nazionale dei Servizi (CNS) (National Services Card) was launched, after years of tests and efforts to achieve interoperability. On 2 March 2004 the President of the Republic signed a Decree[16] that set out the regulations for issuing the CNS. This was followed on 9 December 2004 by a joint Decree by the Minister of the Interior, the Minister of Economy and Finance and the Minister for Innovation and Technology, published in the Gazzetta Ufficiale No 296 of 18 December 2004,[17] providing security and technical rules related to the technologies and the materials to be used to produce the CNS. The National Services Card (CNS) is a smart card intended as a means of on-line authentication. Since it does not have the purpose of serving as a face to face identity document, it only has a microchip with similar characteristics to those of the CIE. The CNS does not have a photograph of the holder and has no specific requirements on the card, thus paving the way to enable it to be issued at a faster rate. Moreover, the CNS can be issued by any public administration that acquires the relevant authentication certificates from any accredited certification service provider. This does not mean that the CNS is accepted only by the issuing administration: rather, it must be accepted by any administration, thus speeding up the means of on-line authentication.

There are some interesting problems surrounding the validity of the process of confirming the identity of the person to whom a card is issued. Article 65(1) of the Code provides as follows:

> ‘1. Le istanze e le dichiarazioni presentate alle pubbliche amministrazioni per via telematica ai sensi dell’articolo 38, commi 1 e 3, del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, sono valide:
>
> a. se sottoscritte mediante la firma digitale, il cui certificato è rilasciato da un certificatore accreditato;

[15] *Istituto Poligrafico Zecca dello Stato (IPZS), an image of the card is available on-line at http://www.ipzs.it/scheda_sicurezza_CI_eng.jsp.*

[16] *Decreto Del Presidente Della Repubblica 2 marzo 2004, n. 117 Regolamento concernente la diffusione della carta nazionale dei servizi, a norma dell'articolo 27, comma 8, lettera b), della L. 16 gennaio 2003, n. 3. (G.U. 6 maggio 2004, n. 105) (Decree by the President of the Republic 2 March 2004, No 117 Regulations regarding the national services card diffusion, as per article 27, paragraph 8, letter b), of law 16 January 2003, No 3 (Gazzetta Ufficiale No 105 of 6 May 2004)).*

[17] *Decreto 9 dicembre 2004 del Ministro dell’ interno, del Ministro per l’ innovazione e le tecnologie e del Ministro dell’ economia e finanze (avviso in G.U. 18 dicembre 2004, n. 296), Le regole tecniche e di sicurezza relative alle tecnologie e ai materiali utilizzati per la produzione della Carta nazionale dei servizi.*

b. ovvero, quando l'autore è identificato dal sistema informatico con l'uso della carta d'identità elettronica o della carta nazionale dei servizi, nei limiti di quanto stabilito da ciascuna amministrazione ai sensi della normative vigente;

c. ovvero quando l'autore è identificato dal sistema informatico con i diversi strumenti di cui all'articolo 64, comma 2, nei limiti di quanto stabilito da ciascuna amministrazione ai sensi della normativa vigente e fermo restando il disposto dell'articolo 64, comma 3.'

'1. Claims and statements submitted to the government electronically in accordance with Article 38, paragraphs 1 and 3 of the Decree of the President of the Republic on December 28, 2000, n. 445 are valid:

a. if signed by a digital signature, whose certificate is issued by an accredited certificate authority;

b. or, when the author is identified by the computer system with the use of an electronic identity card or national card services to the extent determined by each administration in accordance with regulations in force;

c. or when the author is identified by the computer system with the different instruments referred to in Article 64, paragraph 2, to the extent determined by each administration to law and without prejudice to the provisions of Article 64, paragraph 3.'

The provisions of article 65(1)(a) are straightforward, but the provisions of 65(1)(b) and 65(1)(c) pose some difficulty. Article 65(1)(b) enables an electronic document that is not signed to be valid, provided that the identity of the person submitting the document or claim is verified. Some questions that arise from this sub-section include what 'valid' means, and the period of time the validity lasts. For instance, an official in a public administration may have verified the identity of the person submitting the document or claim, but it cannot be guaranteed that the document that is submitted will never be modified by anyone. Should the document be modified, it is debatable whether the document will still be valid. The provisions in items (b) and (c) are open to criticism. At best, all that can be asserted is the authenticity of the person performing the submission (assuming, for the sake of argument, that the person using the password is the person to whom the card has been issued), not of the document that is submitted.

It is suggested that this criticism is reinforced by the provisions of article 65(2), which provide as follows:

> 'Le istanze e le dichiarazioni inviate o compilate su sito secondo le modalità previste dal comma 1 sono equivalenti alle istanze e alle dichiarazioni sottoscritte con firma autografa apposta in presenza del dipendente addetto al procedimento; resta salva la facoltà della pubblica amministrazione di stabilire i casi in cui è necessaria la sottoscrizione mediante la firma digitale.'
>
> 'applications and declarations submitted in the manner provided for in paragraph 1 shall be equivalent to the demands and declarations signed with signature affixed in the presence of the employee assigned to the proceedings; the faculty of public administration may determine when a subscription is required by the use of a digital signature.'

It is interesting to note that this requirement was already present in Decreto legislativo 23 gennaio 2002, n. 10 Attuazione della direttiva 1999/93/CE relativa ad un quadro comunitario per le firme elettroniche (G.U. n. 39 del 15 febbraio 2002) (Legislative Decree No 10/2002), which was repealed when the Code came into force on 1 January 2006.

Enforceability

The Code extends the enforceability of previous technical decrees, based on previous rules of law, until new ones, as required by the Code, come into force. The Code itself became effective 1 January 2006, and the changes applied as a result of the Dlgs 159/2006 did not affect this validity date.

Franco Ruggieri is an independent consultant in respect of the practical implementation of digital signatures. He co-operated with ETSI ESI (since 2001), and the CEN El-sign workshop (now closed) 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 di Ruggieri Franco & C s.a.s.
franco.ruggieri@fastwebnet.it