Firme elettroniche e documento informatico: il codice richiede ulteriori integrazioni[1]

Aggiornato al D.Lgs 4 aprile 2006 n. 159

di Alessandro Osnaghi – 24 maggio 2006

Pubblicato in "ASTRID – Rassegna" n. 30 del 2006

1 Premessa

Dal momento dell'introduzione del *documento informatico* con l'art. 15, comma 2 della legge 15 marzo 1997 n. 59 e della *firma digitale* con il DPR 513/1997, seguiti dal DPR 445/2000, poi dal Dlgs 23 gennaio 2002, n. 10 di recepimento della Direttiva 1999/93/CE, fino al Decreto legislativo 7 marzo 2005, n. 82, *Codice della amministrazione digitale*, non si sono mai spente le discussioni sui numerosi aspetti controversi della complessa materia.

Il lavoro di elaborazione e le discussioni hanno coinvolto esperti di materie giuridiche ed amministrative e solo raramente esperti di materie tecniche informatiche. Si tratta tuttavia di dare valenza proprio a strumenti tecnici del tutto nuovi, che sono resi disponibili dall'evoluzione tecnologica, e un confronto tra le due diverse culture, che incontra soprattutto difficoltà di linguaggio, è sicuramente produttivo.

Il recente intervento correttivo del 15 marzo 2006 non sembra tuttavia aver recepito i suggerimenti proposti per rimuovere definitivamente errori, imprecisioni ed ambiguità.

La trattazione che segue rappresenta il punto di vista ed il contributo di chi si preoccupa soprattutto di poter trovare nel *Codice della amministrazione digitale* oltre agli strumenti giuridici, anche gli strumenti tecnici necessari per **abilitare la digitalizzazione e la realizzazione dei sistemi informatici delle amministrazioni,** e propone quelle ulteriori correzioni che consentano di arrivare, dopo tanto tempo e tante discussioni, ad un quadro certo, che è necessario ed urgente per il superamento del documento cartaceo nelle relazioni tra amministrazioni, cittadini ed imprese.

In questa nota non si affrontano i molti altri problemi di contenuto e di impianto che il Codice presenta, e che sono già stati ampiamente dibattuti al momento della sua emanazione, ma vengono discusse, soprattutto da un punto di vista tecnico, le sole tematiche strettamente correlate tra loro del *documento informatico* e *della firma elettronica* e le tematiche dell'accesso in rete ai servizi, cercando di individuare alcune proposte correttive, con l'auspicio che ci sia spazio per accoglierle nell'interesse di un definitivo chiarimento della materia.

[1] Il presente scritto rappresenta una versione rivista e aggiornata della nota pubblicata in ASTRID - RASSEGNA n. 20 del 2005 con il titolo "Firme elettroniche e documento informatico. Proposte di correzione al Codice della PA digitale"

2 La Direttiva 1999/93/CE: le firme elettroniche

Per entrare nel merito della discussione è necessario ricordare che, in tema di *documento informatico* e *firme elettroniche*, il Codice ha modificato o soppresso numerosi articoli del DPR 445/2000 e che ha integralmente abrogato anche il Dlgs 23 gennaio 2002, n. 10, di recepimento della Direttiva 1999/93/CE. Uno dei punti chiave è quindi assicurare che la nuova formulazione del Codice ripristini un quadro di conformità con la Direttiva.

Per quanto riguarda le *firme elettroniche* la Direttiva ha definito due tipologie di strumenti: la ***firma elettronica*** e la ***firma elettronica avanzata*** entrambi recepiti dal Dlgs 23 gennaio 2002, n. 10, con le seguenti definizioni:

> ***firma elettronica****: l'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici,* ***utilizzati come metodo di autenticazione informatica****.*
>
> ***firma elettronica avanzata:*** *la firma elettronica ottenuta attraverso una procedura informatica che garantisce la connessione univoca al firmatario e la sua univoca identificazione, creata con mezzi sui quali il firmatario può conservare un controllo esclusivo e collegata ai dati ai quali si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati.*

Le definizioni della Direttiva, nella versione inglese, sono formulate in linguaggio tecnico ed hanno un preciso significato in questo contesto, ma non sono state tradotte fedelmente nella formulazione italiana, (che dopo varie vicende è approdata alla sostituzione della parola *autenticazione* con la parola *identificazione*). In particolare per quanto riguarda la definizione di ***firma elettronica*** si possono fare due considerazioni:

La prima considerazione è che la definizione italiana di *firma elettronica* (già nella versione del testo del Codice pre intervento correttivo) aveva impropriamente aggiunto alla parola "*autenticazione*" l'aggettivo "*informatica*" che nella versione inglese non c'era[2], creando un equivoco terminologico dovuto al fatto che il Codice ha sentito la opinabile necessità (e su questo punto si tornerà in seguito) di introdurre una propria definizione di *autenticazione informatica*, che non ha nulla a che vedere con il sgnificato della parola autenticazione del testo inglese e che, se applicata qui, rende completamente errata, oltre che incomprensibile, la definizione di *firma elettronica*.

Il legislatore sembra essersi accorto della incongruenza, ma il rimedio al momento proposto è peggiore del male: invece di togliere l'aggettivo "*informatica*" ripristinando il testo inglese, preferisce sostituire alla parola *autenticazione* la parola *identificazione*, come se fosse la stessa cosa. In questo modo si svuota la definizione del suo significato tecnico e, con essa, lo strumento della *firma elettronica*. Se proprio si riteneva di non poter usare la sola parola *autenticazione*, che non è ambigua nel linguaggio tecnico, ma che forse spaventa il giurista (anche se è fin troppo facile osservare che il significato delle parole non è mai indipendente dal contesto e che qui prevale proprio il contesto tecnico), il modo corretto di formulare la definizione è scrivere "*utilizzati come metodo* ***informatico di autenticazione***".

Come si può notare dall'analisi del testo inglese, e anche del Dlgs 23 gennaio 2002, n. 10, che lo riprendeva, la definizione di ***firma elettronica avanzata***[3], viene costruita per estensione delle

---

[2] **Direttiva 1999/93/CE**: **electronic signature** means data in electronic form which are attached to or logically associated with other electronic data and which serve as a **method of authentication**.

[3] **Direttiva 1999/93/CE**: **advanced electronic signature** means an electronic signature which meets the following requirements:
- it is uniquely linked to the signatory;
- it is capable of identifying the signatory;
- it is created using means that the signatory can maintain under his sole control

funzioni strumentali della *firma elettronica*. La differenza tra le due non è di poco conto agli effetti pratici, infatti la definizione di *firma elettronica*, nonostante il nome, non consente di considerarla uno *strumento per apporre una firma*, nel significato pratico comunemente attribuito a questo termine, in quanto non permette di ricondurre i dati cui è applicata ad un soggetto generalmente individuabile e di rendere evidenti le successive modifiche. La *firma elettronica* è solamente uno *strumento informatico di autenticazione* (non quindi di *identificazione*) utilizzabile in uno scambio di dati tra due entità, secondo il significato comunemente attribuito a questo termine nel linguaggio tecnico dell'ICT.

Lo "*strumento per apporre una firma*" previsto dalla Direttiva è solo la ***firma elettronica avanzata***, come chiaramente si evince dalla sua definizione, e infatti il Dlgs 23 gennaio 2002, n. 10 di recepimento aveva introdotto nella normativa italiana questa tipologia di firma **che ora il Codice ha abrogato**, senza tuttavia recuperare uno strumento equivalente**.** È lecito chiedersi per quale motivo si sia sentita la necessità di eliminare proprio la *firma elettronica avanzata*, considerando che senza questo strumento minimo comune di sottoscrizione accettato a livello europeo, la normativa italiana non è più conforme alla Direttiva.

Non si tratta di giocare con le parole e la distinzione non è di poco conto agli effetti pratici perché, in mancanza dello strumento appropriato, ora il Codice è costretto a considerare erroneamente la *firma elettronica* come se fosse uno *strumento per apporre una firma*, come si legge ad esempio all' Art. 21, comma 1, determinando così una grave ambiguità interpretativa: infatti quello che dovrebbe essere liberamente valutabile in giudizio tenuto conto delle sue caratteristiche è un documento informatico cui è apposta una *firma elettronica avanzata*, non una semplice *firma elettronica*.

Avendo abolito la firma elettronica avanzata, il Codice ha portato a livello di norma primaria la definizione della *firma elettronica qualificata*, già introdotta a livello regolamentare all'Art. 1 del DPR, 7 aprile 2003, n. 137, lettera ee), dove viene definita come uno strumento di firma che estende il livello di sicurezza della *firma elettronica avanzata* con la seguente definizione:

> ***firma elettronica qualificata****: la* ***firma elettronica avanzata*** *che sia basata su un* ***certificato qualificato*** *e creata mediante un* ***dispositivo sicuro*** *per la creazione della firma.*

La Direttiva non aveva tuttavia sentito il bisogno di creare, attribuendole un nome, una nuova tipologia di firma e anche il Codice avrebbe potuto evitarlo, dato che la preesistente ***firma digitale*** della normativa italiana già soddisfaceva i requisiti dell'Art. 5,1[4] della Direttiva, che richiede agli Stati Membri di assicurare valore probatorio a una *firma elettronica avanzata* quando basata su un **certificato qualificato** e creata mediante un **dispositivo sicuro** per la creazione della firma.

Il Codice ha eliminato proprio lo strumento, la *firma elettronica avanzata*, che precedentemente, allo scopo di recepire la direttiva, lo stesso legislatore aveva introdotto con una norma primaria e ha invece portato a livello di norma primaria la *firma elettronica qualificata* che aveva giustamente introdotto solo a livello regolamentare essendo già presente nella norma primaria la ***firma digitale.*** Il razionale di questa operazione sinceramente sfugge.

---

it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable.

[4] **Direttiva 1999/93/CE: Art. 5.1: Legal effects of electronic signatures**

1. 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:
(a) 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
(b) are admissible as evidence in legal proceedings.

L'inopinata eliminazione della *firma elettronica avanzata* determina una diffusa incongruenza logica, tecnica e giuridica in tutta la normativa italiana, perché la sua mancanza lascia spazio, quando è necessario essere conformi all'Art. 5,2.[5] della Direttiva, al riferimento alla semplice *firma elettronica*, che come detto non può essere considerata uno *strumento per apporre una firma* ad un documento informatico.

Questa incongruenza risulta ben evidente ad esempio, nella formulazione del già citato Art. 21, comma 1. dove non disponendo della tipologia della *firma elettronica avanzata* si è dovuto utilizzare impropriamente l'unico strumento disponibile, cioè la *firma elettronica*.

ART. 21 (Valore probatorio del documento informatico sottoscritto)

1. *Il documento informatico, cui è apposta una con **firma elettronica**, sul piano probatorio è liberamente valutabile in giudizio, tenuto conto delle sue caratteristiche oggettive di qualità, sicurezza e immodificabilità.*
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.*

Ripristinando nel Codice la *firma elettronica avanzata* non si perde evidentemente la possibilità di disporre, per estensione del suo livello di sicurezza, anche di una *firma elettronica qualificata*, mentre se questo strumento non è definito, si perde sicuramente la possibilità di riferirlo, quando sarebbe necessario e appropriato, negli articoli del Codice**.**

L'eliminazione della firma elettronica avanzata configura a parere dello scrivente, che tuttavia non ha titolo ad esprimersi in materia, un evidente **vulnus al recepimento della Direttiva 1999/93/CE**, che appare disattesa proprio nello strumento minimo comune introdotto per firmare elettronicamente un documento e valido nell'Unione europea.

Anche a prescindere da quest'ultima considerazione è evidente la necessità, pur conservando la *firma elettronica qualificata* a rango primario, di ripristinare la *firma elettronica avanzata* senza la quale non è più utilizzabile nell'articolato uno dei due strumenti tecnici con cui si potrebbe sottoscrivere un *documento informatico* e che è **essenziale per la realizzazione pratica dei sistemi informatici di gestione documentale e non solo di quelli della pubblica amministrazione**.

Per rimediare basterebbe recuperare alla lettera r) e r.bis) dell'Art. 1, comma 1 del Codice, le già citate definizioni all'Art. 2, lettera g) del Dlgs 23 gennaio 2002, n. 10 e all'Art. 1, lettera ee) del DPR 7 aprile 2003, n. 137, di *firma elettronica avanzata* e di *firma elettronica qualificata* rispettivamente.

3 La rappresentazione digitale del documento informatico

Le definizioni relative alle firme elettroniche della Direttiva europea non fanno riferimento a una specifica ***tecnica informatica di apposizione di una firma elettronica*** e neppure alla natura informatica degli "*oggetti*" cui è possibile apporre una firma, ma per **realizzare i sistemi**

[5] **Direttiva 1999/93/CE: Art. 5.2: Legal effects of electronic signatures**
2. Member States shall ensure that an electronic signature is not denied legal effectiveness and admissibility as evidence in legal proceedings solely on the grounds that it is:
- in electronic form, or
- not based upon a qualified certificate, or
- not based upon a qualified certificate issued by an accredited certification-service-provider, or
- not created by a secure signature-creation device

informatici di gestione documentale delle amministrazioni diventa necessario caratterizzare questi strumenti anche tecnicamente e non solamente in termini giuridici.

Nel Codice viene definito il ***documento informatico*** come ***rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti***, definizione che riguarda cosa il "contenuto" del documento rappresenta dal punto di vista giuridico ed amministrativo, mentre è assente una qualsiasi definizione informatica del "contenitore".

Ora, mentre il **sistema informativo** delle amministrazioni è costituito da documenti cartacei, o anche da documenti informatici, il loro **sistema informatico,** non è ovviamente capace di comprendere cosa il documento informatico rappresenti e pertanto non può conoscere il ***documento informatico*** nella sua definizione giuridica, ma solo in quanto codificato e rappresentato da un particolare tipo di *oggetto informatico*, cioè da un insieme di dati strutturati e codificati in forma digitale, che viene generato su un supporto elettronico da specifici programmi informatici.

Un *oggetto informatico* è fruibile attraverso una sua **rappresentazione analogica, direttamente interpretabile da una persona,** che viene generata da un programma informatico capace di tradurne la codifica digitale nella rappresentazione analogica stessa. (Ad esempio, i *file* di tipo .doc o .pdf, che sono prodotti dai programmi di scrittura commerciali, oppure i file di tipo .tif o .jpg che codificano immagini digitali, sono *oggetti informatici*).

La definizione di *documento informatico come "rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti"* è da tempo consolidata nella legislazione italiana, ma ai fini di una corretta gestione informatica sarà necessario stabilire anche quale tipo di *oggetto informatico* ne possa codificare la forma digitale, l'unica trattabile da un sistema informatico. Solo così un sistema informatico potrà gestire e riconoscere un *documento informatico* a prescindere da che cosa esso rappresenti o codifichi dal punto di vista del significato giuridico.

Senza questa distinzione concettuale si determina, come vedremo, una ambiguità terminologica diffusa in tutto il testo del Codice.

La domanda a cui si deve dare una risposta è se un normale *file* (ad esempio un file .doc o .pdf, ecc.) possa essere considerato un *documento informatico* - come ad esempio lascerebbe intendere la discutibile definizione del Decreto 23 gennaio 2004 del Ministero dell'Economia e delle Finanze - o se invece sia necessario o opportuno, anche solo per esigenze tecniche, introdurre una tipologia di *oggetti informatici* che, pur essendo rappresentati ovviamente come *file o insiemi di file*, siano tuttavia dotati di caratteristiche specifiche. In pratica si tratta di individuare una opportuna *trasformazione informatica* che applicata ad un *oggetto informatico* (ad esempio un *file* di tipo .doc) generi un altro *oggetto informatico* usabile come forma digitale di un *documento informatico*.

In analogia col concetto di documento cartaceo, la trasformazione che appare utile applicare ad un *file*, e al suo contenuto, per trasformarlo nella rappresentazione digitale di un *documento informatico* potrebbe essere individuata in una funzione informatica che è capace di creare una **associazione tra il *file* e un *soggetto*** e di **rendere evidenti le modifiche** intervenute dopo l'applicazione della funzione, nonché di rendere possibile a ogni terza parte, che conosca un *attributo pubblico* del *soggetto che ha applicato la trasformazione* di collegare univocamente il *file* al soggetto stesso. (Così come è definita questa funzione non implica che il soggetto che applica la trasformazione al *file* sia una persona). È evidente che un semplice file ad esempio del tipo .doc, in quanto tale, non può essere imputato ad alcun soggetto e non se ne può verificare l'integrità e quindi non lo si potrebbe considerare la rappresentazione digitale un *documento informatico,* almeno nella definizione tecnica data.

La trasformazione descritta corrisponde alle caratteristiche funzionali della ***firma elettronica avanzata***, e pertanto si potrebbe concludere che un semplice *file* diventa un *documento informatico* se gli applichiamo una trasformazione informatica che corrisponde all'apposizione di una *firma elettronica avanzata*. In questa ipotesi, se non si dispone della *firma elettronica avanzata* non si dispone dello strumento tecnico capace di generare un *documento informatico* gestibile in quanto tale da un sistema informatico.

Da questo punto di vista è importante osservare che una semplice *firma elettronica* anche se definita con la formulazione della Direttiva 1999/93/CE, non è tecnicamente utilizzabile per lo scopo che ci si prefigge.

Le considerazioni fin qui svolte portano a concludere che un *documento informatico* può essere gestito come tale da un sistema informatico se alla sua codifica digitale è stata apposta una *firma elettronica avanzata* a maggior ragione, naturalmente, una *firma elettronica qualificata*.

4 Le firme digitali

Oggi l'unica tecnologia praticamente utilizzabile per realizzare una *firma elettronica avanzata* o *qualificata*, e quindi per generare un *file* che codifica la rappresentazione digitale di un *documento informatico*, è la *tecnologia di firma digitale* basata su una coppia di chiavi asimmetriche pubblica e privata. Utilizzando questa tecnologia è possibile a chi possiede la chiave privata trasformare ogni *file* nella rappresentazione digitale di un *documento informatico.*

Pertanto un *documento informatico* è in termini tecnici il risultato dell'applicazione della *tecnologia di firma digitale* ad un *file statico*[6] che diventa quindi univocamente riferito al soggetto titolare di una coppia di chiavi e di cui ogni soggetto terzo, utilizzando la chiave pubblica, può verificare l'attribuzione e l'integrità, naturalmente con il presupposto che la chiave privata sia utilizzabile dal solo titolare della coppia.

L'applicazione della tecnologia di firma digitale è indipendente dal livello di sicurezza con cui è generata e conservata la chiave privata assegnata al titolare, elementi che differenziano la *firma elettronica avanzata* dalla *firma elettronica qualificata*, e pertanto un *documento informatico* può essere generato utilizzando entrambe le tipologie di firma a prescindere dal tipo di certificato e dal tipo di dispositivo usati.

Quando si applica la *tecnologia di firma digitale basata su chiavi asimmetriche* si usa comunemente il termine ***firma (digitale) debole*** per indicare una *firma elettronica avanzata* e il termine ***firma digitale*** *(forte)* per indicare una *firma elettronica qualificata:* entrambi i tipi di firma digitale possono generare la codifica digitale del documento informatico. Si tratta di un aspetto tecnico di estrema importanza implementativa perché in questo modo i sistemi informatici possono gestire i *documenti informatici* in modo uniforme (con le stesse applicazioni software) indipendentemente dalla tipologia di firma utilizzata per crearli.

La ***firma digitale*** *(forte)* mantiene il significato inizialmente introdotto nella normativa italiana, e mantenuto nel Codice, e risultano così chiarite ambiguità, e confusioni terminologiche solo apparenti, che hanno finora contraddistinto questa materia, essendo evidente che il semplice utilizzo di più nomi non significa moltiplicare gli strumenti, ma solo qualificarli meglio.

È qui utile sottolineare ancora una volta che la *firma elettronica* della Direttiva (purtroppo non correttamente recepita dal Codice) implica l'applicazione di trasformazioni informatiche di tipo

[6] Il file statico, è un file che non contiene all'origine elementi che possono modificarne la rappresentazione analogica dopo l'applicazione della sottoscrizione.

diverso dalla *tecnologia di firma digitale basata su chiavi asimmetriche* e pertanto non si presta alla generazione della rappresentazione digitale di un *documento informatico*.

Se non si dispone di una *firma elettronica avanzata* non si dispone proprio dello strumento tecnico minimo capace di generare un *documento informatico* e anche per questa ragione (oltre che per esigenze di conformità alla Direttiva europea) è **necessario introdurre nuovamente nel Codice questa tipologia di firma**.

Il quadro definitivo della relazione tra *firme elettroniche* e *documento informatico* è quindi il seguente:

- ***firma elettronica*:** nel significato della definizione della Direttiva europea, non è uno strumento applicabile per generare un *documento informatico* nella forma proposta;
- ***firma* (digitale) *debole*:** appartiene alla specie delle ***firme elettroniche avanzate*** e genera un ***documento informatico***
- ***firma digitale*:** appartiene alla specie delle ***firme elettroniche qualificate*** e genera un ***documento informatico*** *(qualificato).*

In base a queste considerazioni la *firma elettronica* è uno strumento che **non** si applica alla *gestione di documenti* e deve essere sostituita con la *firma elettronica avanzata* in tutti gli articoli del Codice in cui è riferita, come nel già citato Art, 21, comma 1.

5 Documento informatico e forma scritta

Con riferimento al valore probatorio l'Art. 21 rivela che i *documenti informatici* sono di due tipi, uno **non firmato digitalmente** (perché è apposta una firma elettronica che, come si è detto, non è una forma di sottoscrizione digitale) e uno **firmato digitalmente** cui si riferisce il comma 2. Tutto diventa coerente se si modifica il testo introducendo in luogo della *firma elettronica* che è una **non firma** la **firma elettronica avanzata** nella sua forma di *firma (digitale) debole***.** La *firma elettronica avanzata* diversamente dalla *firma digitale* (che è una firma elettronica qualificata) non ha caratteristiche di sicurezza predefinite a priori e quindi consente al giudice una libera valutazione sulla base di perizie tecniche.

La soluzione di queste ambiguità sta quindi nell'adottare la definizione proposta di *documento informatico* come esistente solo in forma di *oggetto informatico sottoscritto digitalmente* con *firma elettronica avanzata* o con *firma elettronica qualificata*. Alle due tipologie sarebbero associate le previsioni del comma 1 e del comma 2 rispettivamente dell'Art. 21. Infatti l'utilizzo di *certificati qualificati* e di un *dispositivo sicuro* per la sottoscrizione, che distinguono la *firma digitale* dalla *firma (digitale) debole**,*** consentono di discriminare tra valore probatorio e libera valutazione del giudice.

Anche la nuova formulazione dell'Art. 20[7] appare particolarmente ambigua. Il comma 1, non essendo specificata alcuna proprietà della codifica digitale del documento informatico sembra

[7] Art. 20. Documento informatico.

1. Il documento informatico da chiunque formato, la registrazione su supporto informatico e la trasmissione con strumenti telematici conformi alle regole tecniche di cui all'articolo 71sono validi e rilevanti agli effetti di legge, ai sensi delle disposizioni del presente codice;

1-bis. L'idoneità del documento informatico a soddisfare il requisito della forma scritta è liberamente valutabile in giudizio, tenuto conto delle sue caratteristiche oggettive di qualità, sicurezza, integrità ed immodificabilità, fermo restando quanto disposto dal comma 2;

applicarsi a qualsiasi tipo di file. Il comma 1bis, in realtà non stabilisce alcun criterio per soddisfare la forma scritta dato che l'idoneità del documento viene lasciata alla libera valutazione del giudice (il che ovviamente richiede una perizia tecnica probabilmente complessa).

Sembra ragionevole proporre che, per soddisfare la forma scritta, si richieda che il documento possa almeno essere imputabile ad un soggetto e che sia immodificabile.

Si conferma l'esigenza che un documento informatico, per essere gestito in quanto tale da un sistema informatico, debba essere sempre sottoscritto digitalmente, almeno con firma elettronica avanzata, e che l'utilizzo di una firma elettronica avanzata sia il criterio oggettivo minimo per **l'idoneità a soddisfare il requisito della forma scritta**. Se così non fosse dovremmo concludere, ad esempio, che un semplice file .doc potrebbe essere idoneo a soddisfare il requisito della forma scritta.

L'idoneità a soddisfare il requisito della forma scritta diventa così una proprietà intrinseca del *documento informatico*, che attiene al suo essere codificato come *oggetto informatico sottoscritto digitalmente* e può essere attribuita ad entrambe le tipologie di documento informatico.

In questo modo possono essere chiarite alcune ambiguità, ad esempio nell'Art. 45, comma 1, che riguardano la trasmissione dei documenti e che sembrano proporre l'interpretazione che sia il mezzo di trasmissione ad attribuire al *documento informatico* il requisito della forma scritta e che quindi non si tratti di una sua proprietà oggettiva intrinseca e preesistente.

Da questo punto di vista anche l'Art. 47 contiene evidenti ambiguità in quanto utilizza termini quali "*comunicazioni*" e " *provenienza*" o *fonte di provenienza*" non del tutto chiariti se riferiti alla trasmissione di *documenti informatici,* la cui fonte di provenienza non può essere identificata in chi li spedisce, ma in chi li ha sottoscritti digitalmente.

6 L'autenticazione informatica

Per quanto riguarda l'uso dl termine ***autenticazione informatica***[8] il Codice presenta evidenti errori che è necessario correggere. Una volta eliminato dal decreto correttivo il termine dall'Art. 1, lettera q) e lettera r), in cui era usato impropriamente, è opportuno chiedersi se il suo uso sia appropriato nei restanti Art. 54, comma 3 e Art. 64, comma 1 e 2 e indirettamente anche all'Art. 65, comma 1, lettera c, che richiama l'Art. 64, comma 2.

Nell'Art.1, lettera b) al termine ***autenticazione informatica*** si è attribuito il significato di procedimento informatico che consente di verificare che le informazioni presentate da un utente per accedere ad un sistema informatico (le sue credenziali) siano valide. La definizione che viene data fa riferimento ad una imprecisata identità del soggetto nei sistemi informativi e non alla sua identità personale.

Che l'***autenticazione informatica*** non comporti necessariamente l'identificazione dell'utente fa parte dell'esperienza comune. È infatti del tutto normale che per poter accedere ad un sito che eroga servizi si richieda all'utente di procedere alla registrazione, procedura che ha lo scopo di attribuirgli le credenziali da utilizzare per l'autenticazione informatica, ma la registrazione non comporta necessariamente l'accertamento dell'identità dell'utente, che è funzione dal fatto che le credenziali gli siano state attribuite previo accertamento della sua **identità personale**.

[8] b) **autenticazione informatica**: la validazione dell'insieme di dati attribuiti in modo esclusivo ed univoco ad un soggetto, che ne distinguono l'identità nei sistemi informativi, effettuata attraverso opportune tecnologie anche al fine di garantire la sicurezza dell'accesso;

Le informazioni di pubblico dominio devono certamente poter essere accessibili a tutti senza la necessità di venire riconosciuti personalmente, ma questo requisito non deve escludere la possibilità di assegnare all'utente, previa registrazione al servizio, credenziali per *l'autenticazione informatica*, che, pur non collegate alla sua identità personale, consentono di fornire all'utente un servizio personalizzato grazie al fatto che il sistema informatico è messo in condizione di gestirne il profilo di utenza.

Quando si parla di accesso ai servizi o ai dati delle pubbliche amministrazioni non è corretto parlare solo di *autenticazione informatica* che in linea di massima è sempre necessaria o opportuna, ma, in relazione alla tipologia del servizio e alle garanzie da fornire, è necessario specificare se le credenziali da utilizzare per l'autenticazione, di qualunque tipo esse siano, debbano essere associate o meno alla identità personale di chi ne è titolare.

Per questo motivo è opportuno rivedere la formulazione dell'Art. 54 comma 3, e dell'Art. 64, comma 1, 2 e 3, formulandoli come proposto in allegato.

All'Art. 64, comma 1, le credenziali di cui si parla, CIE e CNS, sono effettivamente riconducibili all'identità personale del titolare, ma il testo che ne richiede l'uso "quando è necessaria l'autenticazione informatica" e non l'accertamento dell'identità personale, non consente di individuare in relazione a quali tipologie di servizi queste credenziali **devono** essere usate. Quello che è certo è che appare privo di senso renderle obbligatorie per qualsiasi tipo di servizio.

Anche il comma 2, che fa fronte, sia pure temporaneamente, ad una situazione di potenziale discriminazione tra i cittadini che non dispongono di CIE o CNS, o dell'attrezzatura per usarle, e che consente alle amministrazioni di emettere credenziali di altro tipo, ma senza stabilire alcun criterio, andrebbe riformulato nel senso di richiedere che comunque le credenziali siano associate con certezza ad un soggetto identificato, al fine di impedire violazioni della privacy o di prevenire l'accesso non autorizzato ai servizi.

7 La presentazione di istanze e dichiarazioni

L'analisi dell'Art. 65 (I*stanze e dichiarazioni presentate alle pubbliche amministrazioni per via telematica*) consente una ulteriore riflessione sulla necessità di distinguere tra servizio/autenticazione e documento/firma, che sono funzioni completamente diverse. Per questo motivo l'Art. 65 andrebbe riformulato in modo da renderlo indipendente dall'Art. 64, comma 2, e quindi anche dal comma 3.

La conseguenza ultima della presentazione di una istanza o dichiarazione ad una amministrazione è sempre l'attivazione di un procedimento amministrativo, che tipicamente non ha una conclusione nella sessione (che è il caso dei servizi dell'Art. 64).

Comunque venga costruita l'istanza, fuori linea e inviandola successivamente per posta elettronica certificata o tramite un servizio equivalente, oppure in linea compilando moduli e formulari sul sito di una amministrazione, l'esito non può che essere la produzione di un *documento informatico* che dovrà pervenire al Servizio Protocollo dell'amministrazione, dal quale l'utente si aspetta ad esempio una ricevuta legalmente valida, che indichi il numero di protocollo, anche per consentire il successivo accesso allo stato di avanzamento della pratica.

Il *documento informatico* che rappresenta l'istanza dovrà avere **vita autonoma** nel sistema informatico dell'amministrazione durante tutto il procedimento (gestione documentale, work-flow, ecc.) **indipendentemente dal sistema informatico con cui è stato inizialmente compilato e soprattutto da come l'utente si sia eventualmente autenticato sul sistema stesso.**

L'autonomia del *documento informatico* nel sistema informatico dell'amministrazione si può garantire solo se il documento informatico è sottoscritto con tecnologia di firma digitale a

prescindere dalla forza legale della firma apposta, perché in questo modo il *documento informatico* acquista caratteristiche stabili di non modificabilità e di riconducibilità al sottoscrittore.

Diventa allora evidente che per produrre una istanza **non è necessario autenticarsi** sul sistema che si usa per creare il documento**, ma è sufficiente, esplicitamente o implicitamente, applicare la tecnologia della firma digitale all'istanza**.

Appare quindi improprio ai fini della realizzazione dei sistemi informatici, collegare la presentazione di istanze ad una procedura di autenticazione informatica e non ad una procedura di sottoscrizione di documenti informatici, **a meno che le credenziali presentate in fase di autenticazione non vengano in realtà utilizzate per applicare la tecnologia della firma digitale all'istanza, una volta che sia stata compilata**.

La tipologia di firma digitale da utilizzare è evidentemente da mettere in relazione con la tipologia di istanza o di dichiarazione, ma si dovrà poter utilizzare non solo la **firma digitale,** ma anche la **firma elettronica avanzata**, cioè in pratica la **firma digitale debole**, secondo quanto stabilito da ciascuna amministrazione.

L'uso di CIE o di CNS, previsto all'art. 65, comma 1, lettera b, come strumenti di autenticazione è comunque coerente con questa impostazione, perché in questo caso questi strumenti, non sono principalmente utilizzati per l'accertamento della identità di chi compila l'stanza, ma vengono in realtà usati, anche se non sono dotati di certificati di non ripudio, per apporre una firma digitale debole utilizzando i certificati di autenticazione delle carte.

3 Allegato: Proposte di correzioni al Codice

Vengono riportati nel seguito gli articoli del Codice con indicate in **grassetto rosso** le modifiche proposte. Le cancellazioni sono evidenziate in rosso.

1.1 Correzioni proposte per l'Art. 1, comma 1

Art.1 (Definizioni)

1. Ai fini del presente codice si intende per:

b) autenticazione informatica: la validazione delle informazioni presentate dall'utente al sistema informatico per ottenere l'accesso all'utenza associata[9];

h) chiave privata: l'elemento della coppia di chiavi asimmetriche, utilizzato dal soggetto titolare, mediante il quale **si applica la tecnologia della** *firma digitale* **ad un insieme di dati codificati in forma digitale***;*

i) chiave pubblica: l'elemento della coppia di chiavi asimmetriche destinato ad essere reso pubblico, con il quale si verifica la firma digitale apposta **su un insieme di dati codificati in forma digitale** *dal titolare delle chiavi asimmetriche;*

p) documento informatico: la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti .

q) firma elettronica: l'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo *di identificazione informatica* **informatico di autenticazione**[10]*;*

r) **firma elettronica avanzata***: la firma elettronica ottenuta attraverso una procedura informatica che garantisce la connessione univoca al firmatario, creata con mezzi sui quali il firmatario può conservare un controllo esclusivo e collegata ai dati ai quali si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati;*

r bis) firma elettronica qualificata: la firma elettronica avanzata che sia basata su un certificato qualificato e creata mediante un dispositivo sicuro per la creazione della firma;

s) firma digitale: un particolare tipo di firma elettronica qualificata basata su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici;

---

[9] L'autenticazione informatica è un procedimento informatico che verifica le credenziali presentate dall'utente al sistema e di per se non implica l'identificazione personale dell'utente. Non si può fare l'equazione autenticazione informatica = accertamento dell'identità personale. Questa equazione vale solo se le credenziali, cioè le informazioni che vengono presentate al sistema, sono attribuite previo accertamento dell'identità.

[10] Il concetto di identificazione informatica non è definito e sicuramente inappropriato. Appare in ogni caso un concetto diverso dal termine autenticazione usato nel testo inglese. La sostituzione del termine termine "autenticazione" con "identificazione informatica" rende la **definizione di firma elettronica priva di senso**. Si suggerisce di fare riferimento alla dizione "metodo informatico di autenticazione" per contestualizzare il termine.

s) firma digitale: un particolare tipo di firma elettronica **avanzata, che utilizza un certificato qualificato ed è realizzata mediante un dispositivo sicuro per la creazione della firma e** *basata su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici*[11]*;*

1.2 Correzioni proposte per l'Art. 20

ART. 20 (Documento informatico)

1. *Il documento informatico da chiunque formato, la registrazione su supporto informatico e la trasmissione con strumenti telematici conformi alle regole tecniche di cui all'articolo 71 sono validi e rilevanti a tutti gli effetti di legge, ai sensi delle disposizioni del presente codice.*

1-bis. L'idoneità del documento informatico a soddisfare il requisito della forma scritta è liberamente valutabile in giudizio, tenuto conto delle sue caratteristiche oggettive di qualità, sicurezza, integrità ed immodificabilità, fermo restando quanto disposto dal comma 2.

1 bis. Il documento informatico sottoscritto con firma elettronica avanzata, formato in modo da garantire l'invarianza nel tempo degli atti e fatti rappresentati è idoneo a soddisfare il requisito della forma scritta.

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'identificabilità dell'autore, l'integrità e l'immodificabilità del documento* **e l'invarianza nel tempo degli atti e fatti rappresentati**, *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 nullità, dall'articolo 1350, primo comma, numeri da 1 a 12 del codice civile*

1.3 Correzioni proposte per l'Art. 21

ART. 21 (Valore probatorio del documento informatico sottoscritto)

1. *Il documento informatico, cui è apposta una firma elettronica* **avanzata**, *sul piano probatorio è liberamente valutabile in giudizio, tenuto conto delle sue caratteristiche oggettive di qualità, sicurezza, integrità e immodificabilità* **invarianza nel tempo degli atti e fatti rappresentati (**.

2. *Il documento informatico, sottoscritto con* **cui è apposta una** *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 prova contraria.*

1.4 Correzioni proposte per l'Art. 54

Art. 54 (Contenuto dei siti delle pubbliche amministrazioni)

3. *I dati pubblici contenuti nei siti delle pubbliche amministrazioni sono fruibili in rete gratuitamente e senza necessità di* **accertare l'identità di chi richiede l'accesso.**

[11] Questa seconda definizione di firma digitale è equivalente alla precedente. Adottando questa formulazione che si basa sulla firma elettronica avanzata sarebbe possibile eliminare dal Codice la firma elettronica qualificata che è un termine non utilizzato dalla direttiva europea e usare la sola **firma digitale** evitando di ricorrere sempre alla doppia dizione **firma digitale o altro tipo di firma elettronica qualificata**.

1.5 Correzioni proposte per l'Art. 64

Art. 64 (Modalità di accesso ai servizi erogati in rete dalle pubbliche amministrazioni)

1. *La carta d'identità elettronica e la carta nazionale dei servizi costituiscono strumenti* **di autenticazione informatica** *per l'accesso ai servizi erogati in rete dalle pubbliche amministrazioni per i quali* **sia necessario accertare l'identità dell'utente**.
2. *Le pubbliche amministrazioni possono consentire l'accesso ai servizi in rete da esse erogati,* **per i quali sia necessario accertare l'identità dell'utente,** *anche con strumenti* **di autenticazione informatica** *diversi dalla carta d'identità elettronica e dalla carta nazionale dei servizi, purché tali strumenti consentano di accertare l'identità* **del soggetto cui sono attribuiti**. *L'accesso con carta d'identità elettronica e carta nazionale dei servizi è comunque consentito indipendentemente dalle modalità di accesso predisposte dalle singole amministrazioni.*
3. *Ferma restando la disciplina riguardante le trasmissioni telematiche gestite dal Ministero dell'economia e delle finanze e dalle agenzie fiscali, con decreto del Presidente del Consiglio dei Ministri o del Ministro delegato per l'innovazione e le tecnologie, di concerto con il Ministro per la funzione pubblica e d'intesa con la Conferenza unificata di cui all'articolo 8 del decreto legislativo 28 agosto 1997, n. 281, è fissata la data, comunque non successiva al 31 dicembre 2007, a decorrere dalla quale non è più consentito l'accesso ai servizi erogati in rete dalle pubbliche amministrazioni* **per i quali sia necessario accertare l'identità dell'utente**, *con strumenti diversi dalla carta d'identità elettronica e dalla carta nazionale dei servizi.*

1.6 Correzioni proposte per l'Art. 65

Art. 65 (Istanze e dichiarazioni presentate alle pubbliche amministrazioni per via telematica)

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;*
    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 normativa vigente;*
    c. ovvero se sottoscritte con firma elettronica avanzata nei limiti di quanto stabilito da ciascuna amministrazione ai sensi della normativa vigente;
2. *Le istanze e le dichiarazioni inviate* **a una pubblica amministrazione, o compilate sul suo 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.*
3. *Dalla data di cui all'art, 64, comma 3, non è più consentito l'invio di istanze e dichiarazioni con le modalità di cui al comma 1, lettera c).*

1.7 Trasmissione dei documenti

Art. 45 (Valore giuridico della trasmissione)

1. *I documenti trasmessi da chiunque ad una pubblica amministrazione con qualsiasi mezzo telematico o informatico, ivi compreso il fax, idoneo ad accertarne la fonte di provenienza,* ***soddisfano il requisito della forma scritta*** *e la loro trasmissione non deve essere seguita da quella del documento originale.*
2. *Il documento informatico trasmesso per via telematica si intende spedito dal mittente se inviato al proprio gestore, e si intende consegnato al destinatario se reso disponibile all'indirizzo elettronico da questi dichiarato, nella casella di posta elettronica del destinatario messa a disposizione dal gestore.*

Art. 47 (Trasmissione dei documenti attraverso la posta elettronica tra le pubbliche amministrazioni)

1. *Le comunicazioni di documenti tra le pubbliche amministrazioni avvengono di norma mediante l'utilizzo della posta elettronica; esse sono valide ai fini del procedimento amministrativo una volta che ne sia verificata la provenienza.*
2. *Ai fini della verifica della provenienza le comunicazioni sono valide se:*
    a) *sono sottoscritte con firma digitale o altro tipo di firma elettronica qualificata;*
    b) *ovvero sono dotate di protocollo informatizzato;*
    c) *ovvero è comunque possibile accertarne altrimenti la provenienza, secondo quanto previsto dalla normativa vigente o dalle regole tecniche di cui all'articolo 71;*
    d) *ovvero trasmesse attraverso sistemi di posta elettronica certificata di cui al decreto del Presidente della Repubblica 11 febbraio 2005, n. 68.*

Allegato: Definizioni dalla Raccomandazione CCITT X.800

3.3.7 **authentication**
See ***data origin authentication***, and ***peer entity authentication***.
Note – In this Recommendation the term “authentication” is not used in connection with data integrity; the term “data integrity” is used instead.

3.3.8 **authentication information**
Information used to establish the validity of a claimed identity.

3.3.21 **data integrity**
The property that data has not been altered or destroyed in an unauthorized manner.

3.3.22 **data origin authentication**
The corroboration that the source of data received is as claimed.

3.3.40 **peer-entity authentication**
The corroboration that a peer entity in an association is the one claimed.

5.2.1 ***Authentication Service***
These services provide for the authentication of a communicating peer entity and the source of data as described below.

5.2.1.1 ***Peer entity authentication Service***
This service provides corroboration to the entity that the peer entity is the claimed entity. This service is provided for use at the establishment of, or at times during, the data transfer phase of a connection to confirm the identities of one or more of the entities connected to one or more of the other entities. This service provides confidence, at the time of usage only, that an entity is not attempting a masquerade or an unauthorized replay of a previous connection. One-way and mutual peer entity authentication schemes, with or without a liveness check, are possible and can provide varying degrees of protection.

5.2.1.2 ***Data origin authentication service***
This service provides corroboration to an entity that the source of the data is the claimed peer entity. The data origin authentication service provides the corroboration of the source of a data unit. The service does not provide protection against duplication or modification of data units.