



Studio Associato KPMG S.p.A.

Aspetti normativi fiscali

13 Luglio 2004



Premessa

Iter normativo

I documenti rilevanti ai fini delle disposizioni tributarie

I requisiti essenziali delle procedure di digital accounting

Conservazione digitale dei documenti analogici

Conservazione digitale dei documenti informatici

Fatturazione elettronica

Glossario

Premessa (1/2)

L'utilizzazione integrata delle opportunità offerte dall'innovazione tecnologica (eg, firma digitale, documento informatico, attivazione della fatturazione elettronica, uso del protocollo informatico, dell'archiviazione ottica e del web) consentono:

- la progressiva migrazione delle attività amministrative verso soluzioni digitalizzate ed innovative, con piena garanzia dei profili di privacy e di sicurezza
- l'applicazione sistematica – sotto il profilo organizzativo ed applicativo – del concetto di “digital desk” (all'operatore è consentito di gestire il proprio lavoro in modo esclusivamente elettronico, senza ricorso ai tradizionali supporti fisici)
- la gestione informatica/digitale:
 - delle comunicazioni all'interno della stessa funzione aziendale
 - di una porzione delle comunicazioni interno/esterno e v/v
- l'accesso on-line alle informazioni a favore di:
 - operatori di altre funzioni aziendali
 - selezionate categorie di utenti esterni

Premessa (2/2)

Tale processo risultava ostacolato dall'assenza di norme che consentissero la gestione informatica/digitale delle documentazioni aventi rilevanza ai fini tributari

Come è noto, infatti, la disciplina in materia di “archiviazione ottica” esiste ormai dal 1994, ma solo a seguito della recente approvazione del D.M. del 23 gennaio 2004 (riguardante l'archiviazione ottica dei documenti) e del D.Lgs. Del 20 febbraio 2004 n. 52 (riguardante la fatturazione elettronica) è possibile gestire in modo completamente informatizzato i documenti aventi rilevanza ai fini tributari.

L'iter normativo

1994

2004

Gestione cartacea dei documenti

D.Lgs. 10/06/94 n.357: conservazione su supporti informatici dei doc. rilevanti ai fini delle disposizioni civilistiche

D.M. 31/07/98: modalità tecniche di trasmissione telematica delle dichiarazioni/contratti di locazione /esecuzione telematica dei pagamenti

D.M. 8/02/99: regole tecniche per trasmissione e conservazione di doc. informatici

Delibere A.I.P.A. 13/12/01 e 19/02/04: regole tecniche per la riproduzione e conservazione di doc. informatici

D.P.R. 23/01/02: attuazione delle direttiva CCE in materia di firma elettronica

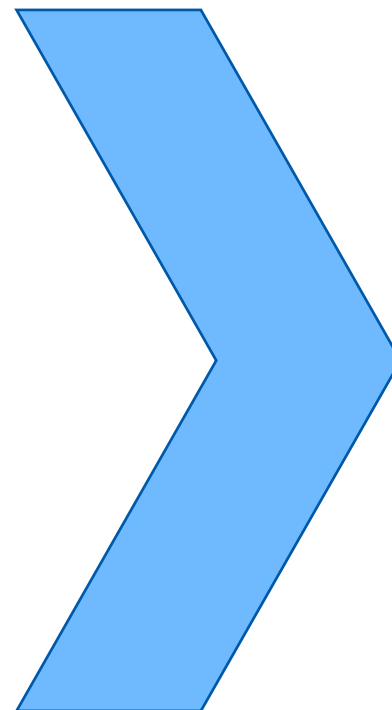
D.M. 23/01/04 e D.Lgs. 20 febbraio 2004 n. 52: modalità di archiviazione elettronica dei documenti Rilevanti ai fini delle disposizioni tributarie e fatturazione elettronica

Gestione informatica dei documenti

I documenti rilevanti ai fini delle disposizioni tributarie

- **Registri IVA acquisti**
- **Registri IVA fatture emesse**
- **Registri IVA vendite**
- **Libro Giornale**
- **Libro Inventari**

- **Registro beni ammortizzabili**
- **Fatture emesse**
- **Fatture ricevute**
- **Documenti di trasporto emessi**
- **Documenti di trasporto ricevuti**
- **Libri sociali**



Il trattamento informatico può essere limitato a una o più tipologie di documenti purchè sia assicurato l'ordine cronologico delle registrazioni e non vi sia soluzione di continuità per ogni periodo d'imposta

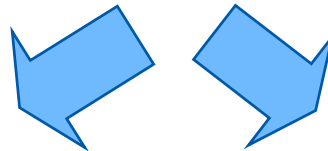
I requisiti essenziali delle procedure di digital accounting

Le procedure adottate per la gestione informatica dei documenti rilevanti ai fini delle disposizioni tributarie devono garantire:

- Autenticità: deve essere possibile risalire all'autore dei documenti informatici
- Integrità: I documenti informatici conservati non possono essere modificati nel tempo e nello spazio

La procedura di archiviazione elettronica dei documenti

La procedura di archiviazione elettronica dei documenti rilevanti ai fini delle disposizioni tributarie si differenzia a seconda della tipologia degli stessi



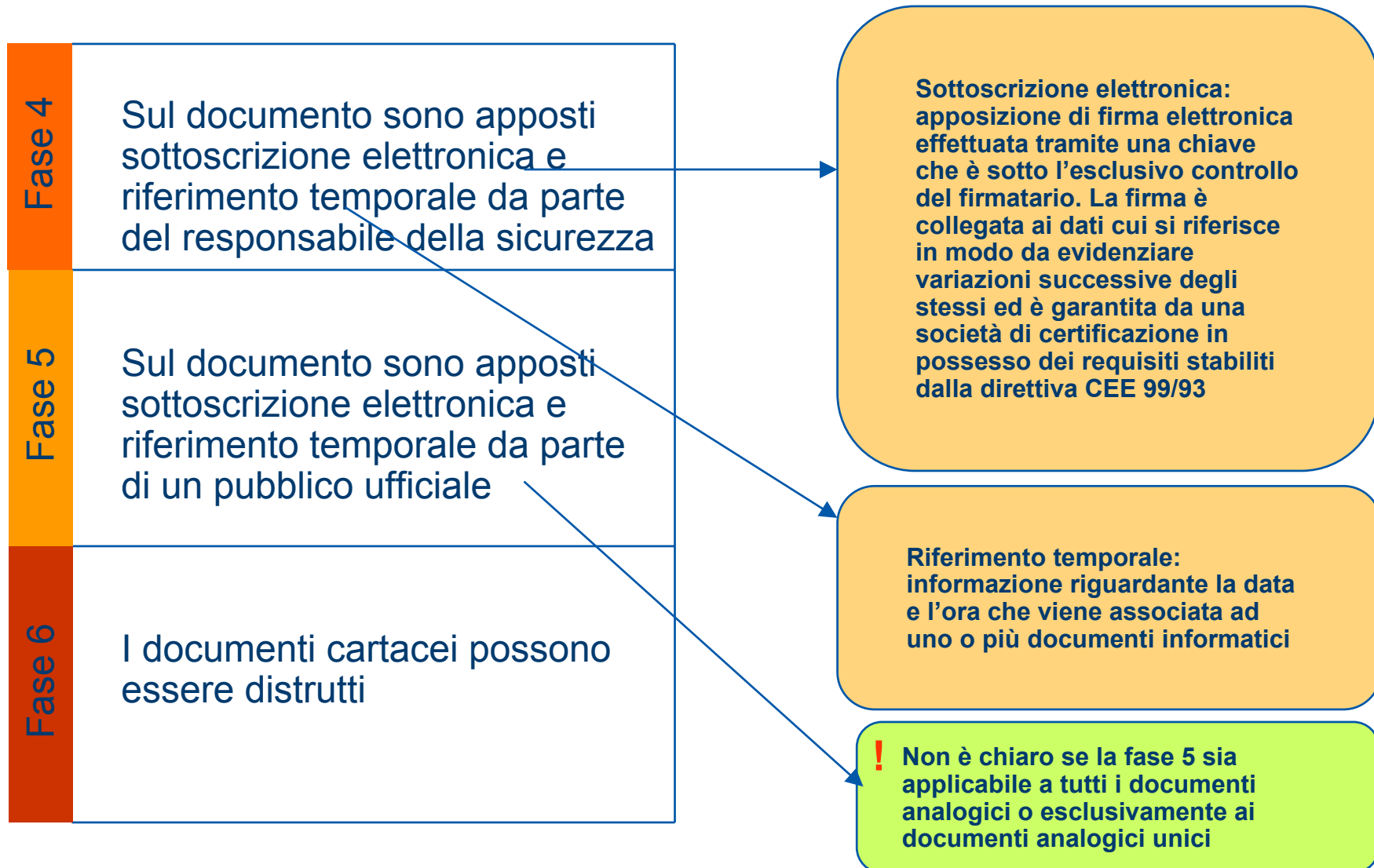
- **Documenti analogici:** insieme di testi, dati e immagini su supporto cartaceo. Sono considerati “unici” nel caso in cui non vi siano copie degli stessi all’interno della struttura aziendale o presso terzi

- **Documenti digitali:** insieme di testi, immagini e dati ottenuti attraverso un processo di elaborazione elettronica

La procedura di archiviazione elettronica dei documenti analogici (1/2)



La procedura di archiviazione elettronica dei documenti analogici (2/2)



La procedura di archiviazione elettronica dei documenti digitali

Fase 1	Nomina del responsabile della conservazione
Fase 2	I documenti (prodotti internamente o ricevuti dall'esterno) vengono elaborati dal sistema gestionale e memorizzati su registri informatici
Fase 3	Sul documento sono apposti sottoscrizione elettronica e riferimento temporale da parte del responsabile della sicurezza

La validità della procedura di archiviazione elettronica dei documenti

- Al fine di riconoscere validità ai documenti conservati è prevista la trasmissione alle competenti agenzie fiscali, entro il mese successivo alla scadenza della dichiarazione dei redditi dell'impronta dell'archivio informatico, della relativa sottoscrizione elettronica e del riferimento temporale
- Le agenzie rendono disponibile per via telematica la ricevuta della comunicazione effettuata ed il relativo numero di protocollo

Impronta: codice di controllo assegnato in modo univoco ad un determinato documento informatico. Consente di verificare che lo stesso non venga successivamente modificato

La procedura fatturazione elettronica

Fase 1

Creazione del documento informatico. Questa fase sarà gestita come avviene attualmente attraverso un gestionale informatico

Fase 2

Trasmissione elettronica del documento con apposizione del riferimento temporale e della sottoscrizione elettronica da parte del responsabile della conservazione

oppure

Trasmissione elettronica dei documenti con sistemi EDI che garantiscono integrità e autenticità dei dati

Fase 3

Archiviazione elettronica del documento digitale come descritto precedentemente



La trasmissione per via elettronica delle fatture è consentita previo accordo con il destinatario

Glossario (1/3)

Firma digitale

La firma digitale rappresenta l'equivalente elettronico di una tradizionale firma apposta su carta.

La firma digitale è il risultato di una procedura informatica e di crittografia basata su un sistema di chiavi asimmetriche a coppia (una chiave privata e una chiave pubblica), in grado di consentire al soggetto inviante e a quello destinatario rispettivamente di rendere manifesta e verificare la provenienza e l'integrità di un documento informatico.

Questo procedimento garantisce:

- La paternità (solo chi è in possesso della chiave privata associata alla chiave pubblica del certificato può effettivamente avere scritto il documento informatico);
- L'integrità (nessuno può averlo modificato).

Peraltro, non è possibile in linea di principio essere completamente sicuri che la coppia di chiavi, ed il certificato relativo, siano effettivamente associati al soggetto inviante: a questo punto interviene la funzione di Certification Authority, autorizzata dall'AIPA ed inserita nell'apposito Elenco Pubblico dei Certificatori, che si fa garante della

- Identità del soggetto tramite apposito certificato.

La legge ha riconosciuto i certificati rilasciati da una Certification Authority autorizzata dall'AIPA anche di potere legale, per cui altra loro caratteristica è:

- La non ripudiabilità (per cui una persona non può rinnegare di avere mandato un documento informatico se a questo ha apposto la propria firma digitale)

Crittografia

Con la crittografia (o cifratura) un messaggio o, più in generale, un qualunque file di dati (testo, immagini, musica ecc.) è trasformato in un insieme di segni e simboli assolutamente privi di significato se non si ha la disponibilità della "chiave" corretta per decifrarlo.

La crittografia è la tecnica fondamentale per la generazione della firma digitale, e viene utilizzata per assicurare la riservatezza, l'autenticazione e il non ripudio delle informazioni archiviate o inviate attraverso reti di computer. Cruciale nella crittografia è la gestione delle chiavi e la garanzia della loro segretezza. Fondamentalmente il problema delle chiavi è affrontato secondo due metodiche:

- A chiave unica, detto anche a chiave privata o simmetrica
- A doppia chiave, detto anche a chiave pubblica o asimmetrica

Glossario (2/3)

Chiavi asimmetriche

Le chiavi asimmetriche sono la coppia di chiavi crittografiche, una pubblica e una privata, correlate tra loro, utilizzate nell'ambito dei sistemi di apposizione e verifica della firma digitale. Una coppia di chiavi può essere attribuita ad un solo titolare.

Chiave privata

La chiave privata è l'elemento della coppia di chiavi asimmetriche, destinato a essere conosciuto dal soggetto titolare, mediante il quale si appone la firma digitale sul documento informatico o si decifra il documento informatico in precedenza cifrato mediante la corrispondente chiave pubblica.

Chiave pubblica

La chiave pubblica è l'elemento della coppia di chiavi asimmetriche destinato a essere reso pubblico, con il quale si verifica la firma digitale apposta sul documento informatico dal titolare delle chiavi asimmetriche o si cifrano i documenti informatici da trasmettere al titolare delle predette.

Documento informatico

Rappresentazione di atti, fatti e dati giuridicamente rilevanti con modalità informatiche.

La formazione e la conservazione dei documenti informatici delle pubbliche amministrazioni devono essere effettuate secondo i seguenti requisiti:

- Identificabilità del soggetto che ha formato il documento informatico e dell'amministrazione di riferimento
- Sottoscrizione, quando prescritta, dei documenti informatici tramite la firma digitale ai sensi del D.P.R. 10 novembre 1997, n. 513;
- Idoneità dei documenti ad essere gestiti mediante strumenti informatici e ad essere registrati mediante il protocollo informatico, ai sensi del D.P.R. 20 ottobre 1998, n. 428;
- Accessibilità ai documenti informatici tramite sistemi informativi autorizzati
- Leggibilità dei documenti
- Interscambiabilità dei documenti

I documenti informatici, muniti dei requisiti sopra detti, sono validi e rilevanti a tutti gli effetti di legge.

Glossario (3/3)

Certification Authority

E' il soggetto che effettua la certificazione, rilascia il certificato della chiave pubblica, lo inserisce in un archivio pubblico, pubblica e aggiorna gli elenchi dei certificati sospesi e revocati.

AIPA

L'Autorità per l'informatica nella Pubblica Amministrazione (AIPA) è un'autorità indipendente istituita dal D.Lgs. n. 39 del 12 febbraio 1993 recante "Norme in materia di sistemi informativi automatizzati delle amministrazioni pubbliche" (come modificato dall'art. 42 della L. 31 dicembre 1996, n. 675).

Il termine "autorità indipendente" indica un'amministrazione pubblica che prende le proprie decisioni in base alla legge, senza dirette interferenze da parte del Governo o del Parlamento.

Elenco pubblico dei certificatori

Per garantire l'identità dei soggetti che utilizzano la firma digitale e per fornire protezione nei confronti di possibili danni derivanti da un esercizio non adeguato delle attività di certificazione, il D.P.R. n. 513/97 (art. 8) richiede che il soggetto certificatore sia in possesso di particolari requisiti e sia incluso in un elenco pubblico, consultabile telematicamente, predisposto, tenuto ed aggiornato a cura dell'Autorità per l'informatica nella Pubblica Amministrazione.

Le Pubbliche Amministrazioni possono anch'esse certificare le chiavi osservando le regole tecniche dettate dall'art. 62 del D.P.C.M. 8 febbraio 1999.

Certificato

Il certificato rappresenta la "credenziale elettronica" con cui l'Autorità di Certificazione attesta la corrispondenza tra una coppia di chiavi e il titolare della stessa.

Il certificato è che una copia della chiave pubblica della coppia "firmata" dall'Autorità di Certificazione con la propria chiave privata, a garanzia dell'autenticità.

La reale procedura di certificazione non si limita alla sola "firma" ma provvede ad inglobarla in una speciale struttura di dati, detta appunto "certificato" la quale contiene tutta una serie di informazioni che, oltre ovviamente a individuare con certezza il soggetto certificatore, qualificano ulteriormente la chiave, nonché il periodo di tempo in cui il certificato stesso può essere utilizzato.