MASTER
in diritto delle nuove tecnologie
e informatica giuridica

Modulo 4 – Firme elettroniche e E-commerce

Documento informatico e firme elettroniche
Il commercio elettronico

Claudio Di Cocco

MASTER in diritto delle nuove tecnologie e informatica giuridica

ALMA MATER RESEARCH INSTITUTE FOR HUMAN-CENTERED ARTIFICIAL INTELLIGENCE

REGOLAMENTO (UE) N. 910/2014

Articolo 1. Oggetto

Allo scopo di garantire il buon funzionamento del mercato interno perseguendo al contempo un adeguato livello di sicurezza dei mezzi di identificazione elettronica e dei servizi fiduciari, il presente regolamento:

- a) fissa le condizioni a cui gli Stati membri riconoscono i mezzi di **identificazione elettronica** delle persone fisiche e giuridiche che rientrano in un regime notificato di identificazione elettronica di un altro Stato membro,
- b) stabilisce le norme relative ai servizi fiduciari, in particolare per le transazioni elettroniche; e
- c) istituisce un quadro giuridico per le **firme elettroniche**, i sigilli elettronici, le **validazioni temporali elettroniche**, **i documenti elettronici**, i **servizi elettronici di recapito certificato** e i servizi relativi ai **certificati di autenticazione di siti web**.

MASTER in diritto delle nuove tecnologie e informatica giuridica

REGOLAMENTO (UE) N. 910/2014

Articolo 2. Ambito di applicazione

1. Il presente regolamento si applica ai regimi di identificazione elettronica che sono stati notificati da uno Stato membro, nonché ai prestatori di servizi fiduciari che sono stabiliti nell'Unione.

2. Il presente regolamento non si applica alla prestazione di servizi fiduciari che sono utilizzati esclusivamente nell'ambito di **sistemi chiusi** contemplati dal diritto nazionale o da accordi conclusi tra **un insieme definito di partecipanti**.

3. Il presente regolamento non pregiudica il diritto nazionale o unionale legato alla **conclusione e alla validità di contratti** o di altri vincoli giuridici o procedurali relativi alla **forma**.

MASTER in diritto delle nuove tecnologie e informatica giuridica

15

REGOLAMENTO (UE) N. 910/2014

Articolo 3 Definizioni.

1) «**identificazione elettronica**», il processo per cui si fa uso di dati di identificazione personale in forma elettronica che rappresentano un'unica persona fisica o giuridica, o un'unica persona fisica che rappresenta una persona giuridica;

2) «**mezzi di identificazione elettronica**», un'unità materiale e/o immateriale contenente dati di identificazione personale e utilizzata per l'autenticazione per un servizio online;

3) «**dati di identificazione personale**», un insieme di dati che consente di stabilire l'identità di una persona fisica o giuridica, o di una persona fisica che rappresenta una persona giuridica;

9) «**firmatario**», una **persona fisica** che crea una firma elettronica;

10) «**firma elettronica**», dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati elettronici e utilizzati dal firmatario per firmare;

MASTER in diritto delle nuove tecnologie e informatica giuridica

16

REGOLAMENTO (UE) N. 910/2014

Articolo 3 Definizioni.

11) «**firma elettronica avanzata**», una firma elettronica che soddisfi i requisiti di cui all'articolo 26;

12) «**firma elettronica qualificata**», una firma elettronica avanzata creata da un dispositivo per la creazione di una firma elettronica qualificata e basata su un certificato qualificato per firme elettroniche;

13) «**dati per la creazione di una firma elettronica**», i dati unici utilizzati dal firmatario per creare una firma elettronica;

14) «**certificato di firma elettronica**», un attestato elettronico che collega i dati di convalida di una firma elettronica a una persona fisica e conferma almeno il nome o lo pseudonimo di tale persona;

15) «**certificato qualificato di firma elettronica**», un certificato di firma elettronica che è rilasciato da un prestatore di servizi fiduciari qualificato ed è conforme ai requisiti di cui all'allegato I;

MASTER in diritto delle nuove tecnologie e informatica giuridica

REGOLAMENTO (UE) N. 910/2014

Articolo 3 Definizioni.

16) «**servizio fiduciario**», un servizio elettronico fornito normalmente dietro remunerazione e consistente nei seguenti elementi:

a) creazione, verifica e convalida di firme elettroniche, sigilli elettronici o validazioni temporali elettroniche, servizi elettronici di recapito certificato e certificati relativi a tali servizi; oppure

b) creazione, verifica e convalida di certificati di autenticazione di siti web; o

c) conservazione di firme, sigilli o certificati elettronici relativi a tali servizi;

17) «**servizio fiduciario qualificato**», un servizio fiduciario che soddisfa i requisiti pertinenti stabiliti nel presente regolamento;

19) «**prestatore di servizi fiduciari**», una persona fisica o giuridica che presta uno o più servizi fiduciari, o come prestatore di servizi fiduciari qualificato o come prestatore di servizi fiduciari non qualificato;

20) «**prestatore di servizi fiduciari qualificato**», un prestatore di servizi fiduciari che presta uno o più servizi fiduciari qualificati e cui l'organismo di vigilanza assegna la qualifica di prestatore di servizi fiduciari qualificato;

MASTER in diritto delle nuove tecnologie e informatica giuridica

REGOLAMENTO (UE) N. 910/2014

Articolo 3 Definizioni.

21) «**prodotto**», un hardware o software o i loro componenti pertinenti, destinati a essere utilizzati per la prestazione di servizi fiduciari;

22) «**dispositivo per la creazione di una firma elettronica**», un software o hardware configurato utilizzato per creare una firma elettronica;

23) «**dispositivo per la creazione di una firma elettronica qualificata**», un dispositivo per la creazione di una firma elettronica che soddisfa i requisiti di cui all'allegato II;

24) «**creatore di un sigillo**», una persona giuridica che crea un sigillo elettronico;

25) «**sigillo elettronico**», dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati in forma elettronica per garantire l'origine e l'integrità di questi ultimi;

REGOLAMENTO (UE) N. 910/2014

Articolo 3 Definizioni.

33) «**validazione temporale elettronica**», dati in forma elettronica che collegano altri dati in forma elettronica a una particolare ora e data, così da provare che questi ultimi esistevano in quel momento;

34) «**validazione temporale elettronica qualificata**», una validazione temporale elettronica che soddisfa i requisiti di cui all'articolo 42;

35) «**documento elettronico**», qualsiasi contenuto conservato in forma elettronica, in particolare testo o registrazione sonora, visiva o audiovisiva;

REGOLAMENTO (UE) N. 910/2014

Articolo 3 Definizioni.

36) «**servizio elettronico di recapito certificato**», un servizio che consente la trasmissione di dati fra terzi per via elettronica e fornisce prove relative al trattamento dei dati trasmessi, fra cui prove dell'avvenuto invio e dell'avvenuta ricezione dei dati, e protegge i dati trasmessi dal rischio di perdita, furto, danni o di modifiche non autorizzate;

37) «**servizio elettronico di recapito qualificato certificato**», un servizio elettronico di recapito certificato che soddisfa i requisiti di cui all'articolo 44;

38) «**certificato di autenticazione di sito web**», un attestato che consente di autenticare un sito web e collega il sito alla persona fisica o giuridica a cui il certificato è rilasciato; […]

MASTER in diritto delle nuove tecnologie e informatica giuridica

REGOLAMENTO (UE) N. 910/2014

CAPO II

IDENTIFICAZIONE ELETTRONICA

Articolo 6 Riconoscimento reciproco

1. Ove il diritto o la prassi amministrativa nazionale richiedano l'impiego di un'identificazione elettronica mediante mezzi di identificazione e autenticazione elettroniche per accedere a un servizio prestato da un organismo del **settore pubblico** online in uno Stato membro, **i mezzi di identificazione elettronica rilasciati in un altro Stato membro sono riconosciuti** nel primo Stato membro ai fini dell'autenticazione transfrontaliera di tale servizio online, purché soddisfino le seguenti condizioni:

a) i mezzi di identificazione elettronica sono rilasciati nell'ambito di un regime di identificazione elettronica compreso nell'elenco pubblicato dalla Commissione a norma dell'articolo 9;

b) […]

MASTER in diritto delle nuove tecnologie e informatica giuridica

REGOLAMENTO (UE) N. 910/2014

CAPO III SERVIZI FIDUCIARI

Articolo 13 Responsabilità e onere della prova

1. Fatto salvo il paragrafo 2, i prestatori di servizi fiduciari sono responsabili di danni causati, con dolo o per negligenza, a qualsiasi persona fisica o giuridica in seguito a un mancato adempimento degli obblighi di cui al presente regolamento.

L'onere di dimostrare il dolo o la negligenza di un prestatore di servizi fiduciari non qualificato ricade sulla persona fisica o giuridica che denuncia il danno di cui al primo comma.

Si presume il dolo o la negligenza di un prestatore di servizi fiduciari qualificato, salvo se questi dimostra che il danno di cui al primo comma si è verificato senza suo dolo o negligenza.

2. Se i prestatori di servizi fiduciari informano debitamente e preventivamente i loro clienti delle **limitazioni d'uso dei servizi** da essi forniti e se tali limitazioni sono riconoscibili da parte di terzi, non sono responsabili dei danni che derivano dall'utilizzo di servizi oltre i limiti indicati.

3. I paragrafi 1 e 2 si applicano conformemente alle norme nazionali in materia di responsabilità.

MASTER in diritto delle nuove tecnologie e informatica giuridica

REGOLAMENTO (UE) N. 910/2014

Articolo 24 Requisiti per i prestatori di servizi fiduciari qualificati

1. Allorché rilascia un certificato qualificato per un servizio fiduciario, un prestatore di servizi fiduciari qualificato verifica, mediante mezzi appropriati e conformemente al diritto nazionale, l'identità e, se del caso, eventuali attributi specifici della persona fisica o giuridica a cui il certificato qualificato è rilasciato.

Le informazioni di cui al primo comma sono verificate dal prestatore di servizi fiduciari qualificato **direttamente o ricorrendo a un terzo** conformemente al diritto nazionale:

a) mediante la presenza concreta della persona fisica o di un rappresentante autorizzato della persona giuridica; o

b) a distanza, mediante mezzi di identificazione elettronica, con cui prima del rilascio del certificato qualificato è stata garantita una presenza concreta della persona fisica o di un rappresentante autorizzato della persona giuridica e che soddisfano i requisiti fissati all'articolo 8 riguardo ai livelli di garanzia «significativo» o «elevato»; o

c) mediante un certificato di una firma elettronica qualificata o di un sigillo elettronico qualificato rilasciato a norma della lettera a) o b); o

d) mediante altri metodi di identificazione riconosciuti a livello nazionale che forniscono una garanzia equivalente sotto il profilo dell'affidabilità alla presenza fisica. La garanzia equivalente è confermata da un organismo di valutazione della conformità.

MASTER in diritto delle nuove tecnologie e informatica giuridica

REGOLAMENTO (UE) N. 910/2014

SEZIONE 4 Firme elettroniche

Articolo 25 Effetti giuridici delle firme elettroniche

1. A una firma elettronica **non possono essere negati gli effetti giuridici e l'ammissibilità come prova in procedimenti giudiziali per il solo motivo della sua forma elettronica o perché non soddisfa i requisiti per firme elettroniche qualificate**.

2. Una **firma elettronica qualificata** ha effetti giuridici **equivalenti** a quelli di una firma autografa.

3. Una firma elettronica qualificata basata su un certificato qualificato rilasciato in uno Stato membro è riconosciuta quale firma elettronica qualificata in tutti gli altri Stati membri.

MASTER in diritto delle nuove tecnologie e informatica giuridica

25

REGOLAMENTO (UE) N. 910/2014

SEZIONE 4 Firme elettroniche

Articolo 26 Requisiti di una firma elettronica avanzata

Una firma elettronica avanzata soddisfa i seguenti requisiti:

a) è connessa unicamente al firmatario;

b) è idonea a identificare il firmatario;

c) è creata mediante dati per la creazione di una firma elettronica che il firmatario può, con un elevato livello di sicurezza, utilizzare sotto il proprio esclusivo controllo; e

d) è collegata ai dati sottoscritti in modo da consentire l'identificazione di ogni successiva modifica di tali dati.

Articolo 27 Firme elettroniche nei servizi pubblici

MASTER in diritto delle nuove tecnologie e informatica giuridica

26

REGOLAMENTO (UE) N. 910/2014

SEZIONE 4 Firme elettroniche

Articolo 29 Requisiti relativi ai dispositivi per la creazione di una firma elettronica qualificata

1. I dispositivi per la creazione di una firma elettronica qualificata soddisfano i requisiti di cui all'allegato II. […]

Articolo 30 Certificazione dei dispositivi per la creazione di una firma elettronica qualificata

1. La conformità dei dispositivi per la creazione di una firma elettronica qualificata con i requisiti stabiliti all'allegato II è certificata da appropriati organismi pubblici o privati designati dagli Stati membri. […]

Articolo 31 Pubblicazione di un elenco di dispositivi per la creazione di una firma elettronica qualificata certificati

Articolo 32 Requisiti per la convalida delle firme elettroniche qualificate

Articolo 33 Servizio di convalida qualificato delle firme elettroniche qualificate

Articolo 34 Servizio di conservazione qualificato delle firme elettroniche qualificate

REGOLAMENTO (UE) N. 910/2014

SEZIONE 5 Sigilli elettronici

Articolo 35 Effetti giuridici dei sigilli elettronici

1. A un sigillo elettronico non possono essere negati gli effetti giuridici e l'ammissibilità come prova in procedimenti giudiziali per il solo motivo della sua forma elettronica o perché non soddisfa i requisiti per i sigilli elettronici qualificati.

2. Un sigillo elettronico qualificato gode della presunzione di integrità dei dati e di correttezza dell'origine di quei dati a cui il sigillo elettronico qualificato è associato.

3. Un sigillo elettronico qualificato basato su un certificato qualificato rilasciato in uno Stato membro è riconosciuto quale sigillo elettronico qualificato in tutti gli altri Stati membri.

REGOLAMENTO (UE) N. 910/2014

SEZIONE 6 VALIDAZIONE TEMPORALE ELETTRONICA

Articolo 41 Effetti giuridici della validazione temporale elettronica

1. Alla validazione temporanea elettronica non possono essere negati gli effetti giuridici e l'ammissibilità come prova in procedimenti giudiziali per il solo motivo della sua forma elettronica o perché non soddisfa i requisiti della validazione temporanea elettronica qualificata.

2. Una validazione temporale elettronica qualificata gode della presunzione di accuratezza della data e dell'ora che indica e di integrità dei dati ai quali tale data e ora sono associate.

3. Una validazione temporale elettronica rilasciata in uno Stato membro è riconosciuta quale validazione temporale elettronica qualificata in tutti gli Stati membri.

Articolo 42 Requisiti per la validazione temporale elettronica qualificata

REGOLAMENTO (UE) N. 910/2014

SEZIONE 7 Servizi elettronici di recapito certificato

Articolo 43 Effetti giuridici di un servizio elettronico di recapito certificato

1. Ai dati inviati e ricevuti mediante un servizio elettronico di recapito certificato non sono negati gli effetti giuridici e l'ammissibilità come prova in procedimenti giudiziali per il solo motivo della loro forma elettronica o perché non soddisfano i requisiti del servizio elettronico di recapito certificato qualificato.

2. **I dati inviati e ricevuti** mediante servizio elettronico di recapito certificato **qualificato** godono della **presunzione** di **integrità** dei dati, dell'**invio** di tali dati da parte del mittente identificato, della loro **ricezione** da parte del destinatario identificato e di **accuratezza** della data e dell'ora dell'invio e della ricezione indicate dal servizio elettronico di recapito certificato qualificato.

Articolo 44 Requisiti per i servizi elettronici di recapito certificato qualificati

REGOLAMENTO (UE) N. 910/2014

SEZIONE 8 Autenticazione dei siti web

Articolo 45 Requisiti per i certificati qualificati di autenticazione di siti web

1. I certificati qualificati di autenticazione di siti web soddisfano i requisiti di cui all'allegato IV. […]

CAPO IV DOCUMENTI ELETTRONICI

Articolo 46 Effetti giuridici dei documenti elettronici*

A un **documento elettronico** non sono negati gli effetti giuridici e l'ammissibilità come prova in procedimenti giudiziali per il solo motivo della sua forma elettronica.

**(Unica disposizione in materia presente nel regolamento; n.d.r.)*

REGOLAMENTO (UE) N. 910/2014

Norme per attuazione eIDAS

1. **Interoperabilità**

Interoperabilità dei regimi nazionali di identificazione elettronica notificati alla Commissione => requisiti tecnici e operativi => regolamento (UE) 2015/1501.

2. **Livelli di garanzia dei mezzi di identificazione**

Interpretazione uniforme dei livelli di garanzia dei mezzi di identificazione personale (basso, significativo ed elevato) => regolamento (UE) 2015/1502.

3. **Elenchi di fiducia**

Elenchi di fiducia con informazioni relative ai prestatori di servizi fiduciari e ai servizi fiduciari da questi erogati => decisione (UE) 2015/1505.

4. **Formati riconoscibili di firma elettronica e sigillo elettronico**

Individuazione dei formati riconoscibili dagli Stati (principio del riconoscimento reciproco) => decisione (UE) 2015/1506.

5. **Valutazione di sicurezza dei dispositivi**

Norme per la valutazione di sicurezza dei dispositivi per la creazione di una firma e di un sigillo qualificati => decisione di esecuzione (UE) 2016/650.

[…]

Decreto Legislativo 7 marzo 2005, n. 82
Codice dell'amministrazione digitale

Abroga:
a) D.P.R. 10 novembre 1997, n. 513
b) il D.Lgs. 10/2002, Attuazione della direttiva 1999/93/CE relativa alle firme elettroniche;
c) gli articoli 1, comma 1, lettere t), u), v), z), aa), bb), cc), dd), ee), ff), gg), hh), ii), ll), mm), nn), oo); 2, comma 1, ultimo periodo, 6; 8; 9; 10; **11**; 12; 13; **14**; 17; 20; 22; 23; 24; 25; 26; 27; 27-bis; 28; 28-bis; 29; 29-bis; 29-ter; 29-quater; 29-quinquies; 29-sexies; 29-septies; 29-octies; 36, commi 1, 2, 3, 4, 5 e 6; 51; **del D.P.R. 445/2000 Documentazione amministrativa**;
[…]

MASTER in diritto delle nuove tecnologie e informatica giuridica

33

Decreto Legislativo 7 marzo 2005, n. 82
Codice dell'amministrazione digitale

Entrato in vigore il **1 gennaio 2006**.

Modificato più volte, da ultimo con il D.Lgs. 30 dicembre 2010, n. 235, D.L. 13 agosto 2011, n. 138 (L. 148/2011), il D.L. 6 dicembre 2011, n. 201 (L. 214/2011), D.L. 9 febbraio 2012, n. 5, convertito, con modificazioni, dalla L. 4 aprile 2012, n. 35, D.L. 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla L. 17 dicembre 2012, n. 221, D.Lgs. 14 marzo 2013, n. 33, D.L. 21 giugno 2013, n. 69, convertito, con modificazioni, dalla L. 9 agosto 2013, n. 98, dalla L. 9 agosto 2013, n. 98, D.L. 24 giugno 2014, n. 90, convertito, con modificazioni, dalla L. 11 agosto 2014, n. 114, L. 27 dicembre 2013, n. 147, L. 23 dicembre 2014 n. 190, D.Lgs. 18 maggio 2015, n. 102, D.L. 19 giugno 2015, n. 78, convertito, con modificazioni, dalla L. 6 agosto 2015, n. 125, D.L. 27 giugno 2015, n. 83, convertito, con modificazioni, dalla L. 6 agosto 2015, n. 132, D.Lgs. 26 agosto 2016, n. 179, D.Lgs. 13 dicembre 2017, n. 217 (in vigore dal 27/01/2018), L. 16 novembre 2018, n. 130, L. 11 febbraio 2019, n. 12, D.L. 16 luglio 2020, n. 76 , convertito, con modificazioni, dalla L. 11 settembre 2020, n. 120.

* Nel proseguo, se non indicato diversamente, gli articoli citati si riferiscono al Codice dell'amministrazione digitale-CAD.

MASTER in diritto delle nuove tecnologie e informatica giuridica

34

Documenti informatici e firme elettroniche

Art. 2. Finalità e ambito di applicazione.
3. Le disposizioni del presente Codice e le relative Linee guida concernenti il documento informatico, le firme elettroniche e i servizi fiduciari di cui al Capo II, la riproduzione e conservazione dei documenti di cui agli articoli 43 e 44, il domicilio digitale e le comunicazioni elettroniche di cui all'articolo 3-bis e al Capo IV, l'identità digitale di cui agli articoli 3-bis e 64 **si applicano anche ai privati**, ove non diversamente previsto.

Documenti informatici e firme elettroniche

Documento informatico: il documento elettronico che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti; (art. 1).

Documento analogico: la rappresentazione non informatica di atti, fatti o dati giuridicamente rilevanti (art. 1).

Documenti informatici e firme elettroniche

01000100 01101111 01100011 01110101 01101101 01100101 01101110 01110100 01101111
00100000 01101001 01101110 01100110 01101111 01110010 01101101 01100001 01110100
01101001 01100011 01101111 00111010 00100000 01101001 01101100 00100000 01100100
01101111 01100011 01110101 01101101 01100101 01101110 01110100 01101111 00100000
01100101 01101100 01100101 01110100 01110100 01110010 01101111 01101110 01101001
01100011 01101111 00100000 01100011 01101000 01100101 00100000 01100011 01101111
01101110 01110100 01101001 01100101 01101110 01100101 00100000 01101100 01100001
00100000 01110010 01100001 01110000 01110000 01110010 01100101 01110011 01100101
01101110 01110100 01100001 01111010 01101001 01101111 01101110 01100101 00100000
01101001 01101110 01100110 01101111 01110010 01101101 01100001 01110100 01101001
01100011 01100001 00100000 01100100 01101001 00100000 01100001 01110100 01110100
01101001 00101100 00100000 01100110 01100001 01110100 01110100 01101001 00100000
01101111 00100000 01100100 01100001 01110100 01101001 00100000 01100111 01101001
01110101 01110010 01101001 01100100 01101001 01100011 01100001 01101101 01100101
01101110 01110100 01100101 00100000 01110010 01101001 01101100 01100101 01110110
01100001 01101110 01110100 01101001 00100000 00100000 00101000 01100001 01110010
01110100 00101110 00100000 00110001 00101001 00101110 00001010

Documento informatico: il documento elettronico che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti (art. 1).

LE FIRME ELETTRONICHE

Reg. UE 910/2014

*10) «**firma elettronica**», dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati elettronici e utilizzati dal firmatario per firmare;*

*11) «**firma elettronica avanzata**», una firma elettronica che soddisfi i requisiti di cui all'articolo 26;*

Articolo 26 - Requisiti di una firma elettronica avanzata

Una firma elettronica avanzata soddisfa i seguenti requisiti:

a) è connessa unicamente al firmatario;

b) è idonea a identificare il firmatario;

c) è creata mediante dati per la creazione di una firma elettronica che il firmatario può, con un elevato livello di sicurezza, utilizzare sotto il proprio esclusivo controllo; e

d) è collegata ai dati sottoscritti in modo da consentire l'identificazione di ogni successiva modifica di tali dati.

*12) «**firma elettronica qualificata**», una firma elettronica avanzata creata da un dispositivo per la creazione di una firma elettronica qualificata e basata su un certificato qualificato per firme elettroniche;*

LE FIRME ELETTRONICHE

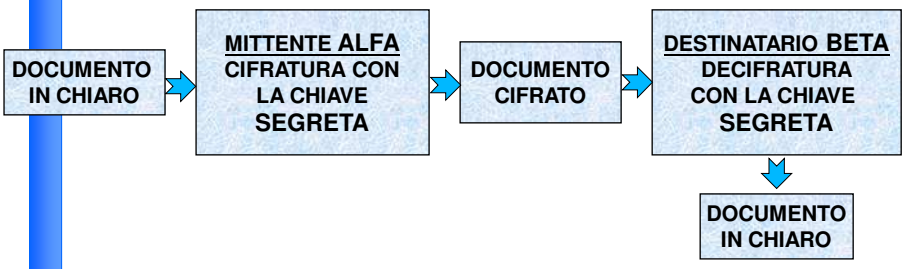
s) **firma digitale:** un particolare tipo di firma qualificata basata su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare di firma elettronica tramite la chiave privata e a un soggetto terzo tramite la chiave pubblica, rispettivamente, di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

aa) **titolare di firma elettronica**: la persona **fisica** cui è attribuita la firma elettronica e che ha accesso ai dispositivi per la sua creazione nonché alle applicazioni per la sua apposizione della firma elettronica;

LE FIRME ELETTRONICHE
LA CRITTOGRAFIA

- La **crittografia** è una tecnica che permette, mediante l'uso di un algoritmo matematico, di trasformare un messaggio leggibile da tutti in una forma illeggibile e decifrabile esclusivamente dal soggetto che possiede la chiave di decifrazione
- **Crittografia "simmetrica"**: se si utilizza una sola chiave segreta per criptare e decriptare il messaggio.
- **Crittografia "asimmetrica"**: se si utilizzano due chiavi per criptare e decriptare il messaggio.

Trasmissione di un documento con crittografia a CHIAVE SIMMETRICA (c.d. chiave segreta)



Il sistema si basa sull'utilizzo di un'unica chiave crittografica, utilizzata sia per cifrare sia per decifrare.

La debolezza del sistema consiste nella unicità della chiave e nella necessità di un canale sicuro da utilizzare per trasmettere la chiave stessa agli utilizzatori.

MASTER in diritto delle nuove tecnologie e informatica giuridica

41

La tecnologia di firma digitale
Crittografia "asimmetrica"

La **firma digitale** rientra nella più ampia categoria delle firme elettroniche e si basa sulle moderne tecniche di crittografia "asimmetrica".

La crittografia asimmetrica prevede l'utilizzo di **due chiavi**:
- una **privata** (o diretta), che dovrà rimanere segreta;
- una **pubblica** (o inversa), destinata invece a essere diffusa.

Sistema di chiavi asimmetriche a coppia:

- il mittente firma il documento informatico con la propria chiave privata (nota solo a lui);
- il destinatario legge il documento con la chiave pubblica del mittente.

Questo meccanismo garantisce:

integrità, **non modificabilità** e **paternità** del documento.

MASTER in diritto delle nuove tecnologie e informatica giuridica

42

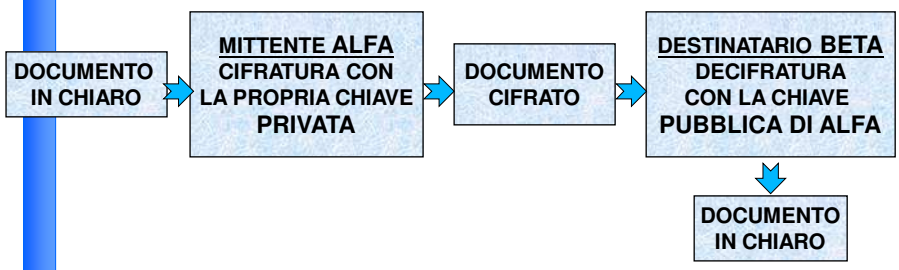
Segue: La crittografia a chiavi asimmetriche

Le **caratteristiche della crittografia asimmetrica** sono:

- ciascuna chiave può essere indifferentemente utilizzata per cifrare e decifrare un documento;
- la chiave utilizzata per cifrare un documento non può essere utilizzata per decifrare lo stesso documento;
- la conoscenza di una delle due chiavi non fornisce alcuna informazione sull'altra chiave.

MASTER in diritto delle nuove tecnologie e informatica giuridica

Trasmissione di un documento con crittografia a CHIAVI ASIMMETRICHE - I -

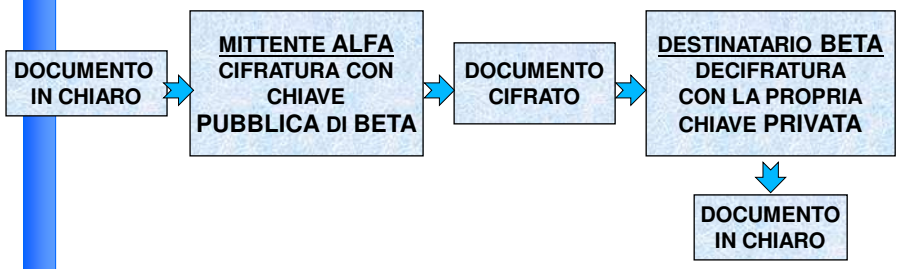


Il sistema garantisce al destinatario Beta che il messaggio ricevuto sia stato inviato proprio dal mittente Alfa, unico soggetto a possedere la chiave privata utilizzata per cifrare.

Il documento è però decifrabile da chiunque utilizzando la chiave pubblica di Alfa.

MASTER in diritto delle nuove tecnologie e informatica giuridica

Trasmissione di un documento con crittografia a CHIAVI ASIMMETRICHE - II -

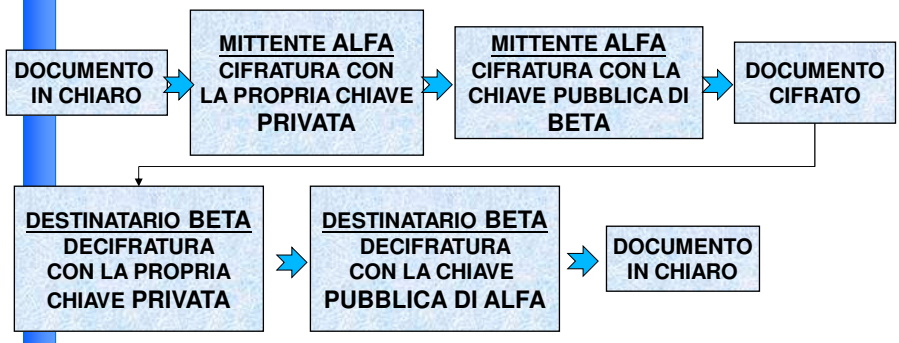


Il sistema garantisce al mittente Alfa che il messaggio inviato sarà decifrabile unicamente dal legittimo destinatario Beta, unico soggetto a possedere la chiave inversa a quella utilizzata per cifrare.

Il destinatario Beta non è invece in grado di verificare la paternità del documento inviatogli.

45

Trasmissione di un documento con crittografia a CHIAVI ASIMMETRICHE - III -



Il sistema garantisce:

- al mittente Alfa che il messaggio inviato sarà decifrabile unicamente dal legittimo destinatario Beta (unico soggetto a possedere la chiave inversa necessaria).

- al destinatario Beta che il messaggio ricevuto è stato inviato proprio dal mittente Alfa (unico soggetto a possedere la chiave inversa utilizzata per cifrare).

Sono dunque assicurate sia la segretezza, sia la paternità del documento.

46

Documenti informatici e firme elettroniche

Funzione di hash: una funzione matematica che genera, a partire da una evidenza informatica, una impronta in modo tale che risulti di fatto impossibile, a partire da questa, ricostruire l'evidenza informatica originaria e generare impronte uguali a partire da evidenze informatiche differenti (art. 1 D.P.C.M. 22/02/2013, Regole tecniche).

Documenti informatici e firme elettroniche

Funzione di hash

Esempio di hash con MD5

Testo in chiaro: *Nel mezzo del cammin di nostra vita*

Hash (impronta o digest):
cb9d3598141c8445a3ba97d73139697a

Se aggiungo una sola lettera…

aa62c6ca68d53b5171652222312b0e1f

Documenti informatici e firme elettroniche

-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

Nel mezzo del cammin di nostra vita mi ritrovai per una selva oscura,
ché la diritta via era smarrita. Ahi quanto a dir qual era cosa dura
esta selva selvaggia e forte che nel pensier rinova la paura! Tant'è
amara che poco è più morte; ma per trattar del ben ch'i' vi trovai,
dirò de l'altre cose ch'i' v'ho scorte.
(Dante Alighieri, Inferno, Canto I 1-9)

-----BEGIN PGP SIGNATURE-----
Version: PGPfreeware 5.0i for non-commercial use
Charset: noconv

iQA/AwUBNm4ma89U6Euy1WZmEQICzACfRayMn71r9fxHzJ3dFtUg
zL2AU/sAoOZg
cPsxL+oATnMhgVe/sKvavV21
=WJN8
-----END PGP SIGNATURE-----

MASTER in diritto delle nuove tecnologie e informatica giuridica

Documenti informatici e firme elettroniche

Il procedimento di firma digitale

Creazione e invio del doc. informatico firmato digitalmente

Creazione doc. in chiaro → **Applicazione della funzione di HASH** → **Si ottiene una impronta o *digest* (riassunto di 128 bit)** →

Si applica la firma (chiave privata) all'impronta (cifrazione) => si ottiene un'evidenza informatica (firma = impronta cifrata) →

Si crea una "busta" (file .p7m) =
+ testo in chiaro
+ impronta (digest)
+ firma (impronta cifrata)
+ certificato
+ chiave pubblica

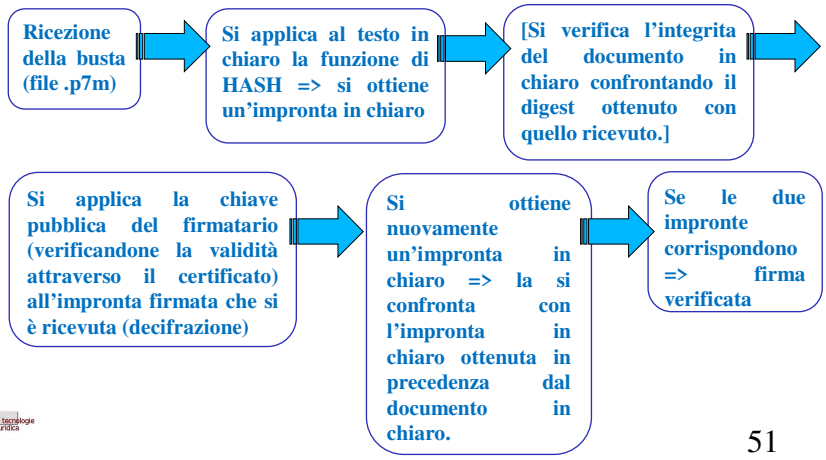
→ **Invio della "busta" al destinatario**

MASTER in diritto delle nuove tecnologie e informatica giuridica

Documenti informatici e firme elettroniche

Il procedimento di firma digitale

Verifica del doc. informatico firmato digitalmente



MASTER in diritto delle nuove tecnologie e informatica giuridica

51

Documenti informatici e firme elettroniche

La firma qualificata/digitale applicata ad un documento

- è **una stringa alfanumerica**, derivante dall'applicazione della chiava privata all'impronta (*digest*) generata dalla funzione di hash;
- la firma qualificata/digitale **cambia a seconda** sia del **firmatario** sia del **testo da firmare**
  - lo stesso testo, sottoscritto da soggetti diversi, genera firme diverse;
  - testi diversi, sottoscritti dal medesimo soggetto, generano firme diverse.

MASTER in diritto delle nuove tecnologie e informatica giuridica

52

I certificati

Le firme qualificate e digitali da sole non possono garantire l'identità del firmatario.

È necessario l'intervento di prestatori di servizi fiduciari che verifichino e attestino la corrispondenza biunivoca tra l'**identità** di un soggetto e la titolarità della firma elettronica.

I certificati

Reg. UE 910/2014

14) «**certificato di firma elettronica**», un attestato elettronico che collega i dati di convalida di una firma elettronica a una persona fisica e conferma almeno il nome o lo pseudonimo di tale persona;

15) «**certificato qualificato di firma elettronica**», un certificato di firma elettronica che è rilasciato da un prestatore di servizi fiduciari qualificato ed è conforme ai requisiti di cui all'allegato I;

REGOLAMENTO (UE) N. 910/2014

SEZIONE 4 Firme elettroniche

Articolo 28 Certificati qualificati di firme elettroniche

1. I certificati qualificati di firme elettroniche soddisfano i requisiti di cui all'allegato I.
2. I certificati qualificati di firme elettroniche non sono soggetti a requisiti obbligatori oltre ai requisiti di cui all'allegato I.
3. I certificati qualificati di firme elettroniche possono includere attributi specifici aggiuntivi non obbligatori. Tali attributi non pregiudicano l'interoperabilità e il riconoscimento delle firme elettroniche qualificate.
4. Qualora un certificato qualificato di firme elettroniche sia stato revocato dopo l'iniziale attivazione, esso decade della propria validità dal momento della revoca e la sua situazione non è ripristinata in nessuna circostanza.
5. Fatte salve le condizioni seguenti, gli Stati membri possono fissare norme nazionali in merito alla sospensione temporanea di un certificato qualificato di firma elettronica:
a) in caso di temporanea sospensione di un certificato qualificato di firma elettronica, il certificato perde la sua validità per il periodo della sospensione;
b) il periodo di sospensione è indicato chiaramente nella banca dati dei certificati e la situazione di sospensione è visibile, durante il periodo di sospensione, dal servizio che fornisce le informazioni sulla situazione del certificato.
6. […]

MASTER in diritto delle nuove tecnologie e informatica giuridica

55

REGOLAMENTO (UE) N. 910/2014

ALLEGATO I

REQUISITI PER I CERTIFICATI QUALIFICATI DI FIRMA ELETTRONICA

I certificati qualificati di firma elettronica contengono:

a) un'indicazione, almeno in una forma adatta al trattamento automatizzato, del fatto che il certificato è stato rilasciato quale certificato qualificato di firma elettronica;

b) un insieme di dati che rappresenta in modo univoco il prestatore di servizi fiduciari qualificato che rilascia i certificati qualificati e include almeno lo Stato membro in cui tale prestatore è stabilito e

- per una persona giuridica: il nome e, se del caso, il numero di registrazione quali figurano nei documenti ufficiali,
- per una persona fisica: il nome della persona;

c) è chiaramente indicato almeno il nome del firmatario, o uno pseudonimo, qualora sia usato uno pseudonimo;

MASTER in diritto delle nuove tecnologie e informatica giuridica

56

REGOLAMENTO (UE) N. 910/2014

d) i dati di convalida della firma elettronica che corrispondono ai dati per la creazione di una firma elettronica;

e) l'indicazione dell'inizio e della fine del periodo di validità del certificato;

f) il codice di identità del certificato che deve essere unico per il prestatore di servizi fiduciari qualificato;

g) la firma elettronica avanzata o il sigillo elettronico avanzato del prestatore di servizi fiduciari qualificato che rilascia il certificato;

h) il luogo in cui il certificato relativo alla firma elettronica avanzata o al sigillo elettronico avanzato di cui alla lettera g) è disponibile gratuitamente;

i) l'ubicazione dei servizi a cui ci si può rivolgere per informarsi sulla validità del certificato qualificato;

j) qualora i dati per la creazione di una firma elettronica connessi ai dati di convalida della firma elettronica siano ubicati in un dispositivo per la creazione di una firma elettronica qualificata, un'indicazione appropriata di questo fatto, almeno in una forma adatta al trattamento automatizzato.

MASTER in diritto delle nuove tecnologie e informatica giuridica

57

CAD

Art. 28. Certificati di firma elettronica qualificata

2. In aggiunta alle informazioni previste nel Regolamento eIDAS nel certificato di firma elettronica qualificata può essere inserito il codice fiscale. Per i titolari residenti all'estero cui non risulti attribuito il codice fiscale, si può indicare il codice fiscale rilasciato dall'autorità fiscale del Paese di residenza o, in mancanza, un analogo codice identificativo univoco.

3. Il certificato di firma elettronica qualificata può contenere, ove richiesto dal titolare di firma elettronica o dal terzo interessato, le seguenti informazioni, se pertinenti e non eccedenti rispetto allo scopo per il quale il certificato è richiesto:

a) **le qualifiche specifiche del titolare di firma elettronica**, quali l'appartenenza ad ordini o collegi professionali, la qualifica di pubblico ufficiale, l'iscrizione ad albi o il possesso di altre abilitazioni professionali, nonché poteri di rappresentanza;

b) **i limiti d'uso del certificato**, inclusi quelli derivanti dalla titolarità delle qualifiche e dai poteri di rappresentanza di cui alla lettera a) ai sensi dell'articolo 30, comma 3;

c) **limiti del valore degli atti unilaterali e dei contratti** per i quali il certificato può essere usato, ove applicabili;

c-bis) **uno pseudonimo**, qualificato come tale. […]

MASTER in diritto delle nuove tecnologie e informatica giuridica

58

CAD

Art. 32. Obblighi del titolare e del prestatore di servizi di firma elettronica qualificata

1. 1. Il titolare del certificato di firma è tenuto ad assicurare la **custodia** del dispositivo di firma o degli strumenti di autenticazione informatica per l'utilizzo del dispositivo di firma da remoto, 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.

2. Il prestatore di servizi di firma elettronica qualificata è tenuto ad adottare tutte le misure organizzative e tecniche idonee ad evitare danno a terzi.

3. Il prestatore di servizi di firma elettronica qualificata che rilascia certificati qualificati deve comunque:

a) provvedere con certezza **alla identificazione della persona** che fa richiesta della certificazione;

b) **rilasciare e rendere pubblico il certificato elettronico** nei modi o nei casi stabiliti dalle Linee guida, nel rispetto del decreto legislativo 30 giugno 2003, n. 196, e successive modificazioni;

[…];

CAD

[Segue Art. 32]

c) specificare, nel certificato qualificato su richiesta dell'istante, e con il consenso del terzo interessato, i poteri di rappresentanza o altri titoli relativi all'attività professionale o a cariche rivestite, previa verifica della documentazione presentata dal richiedente che attesta la sussistenza degli stessi;

d) attenersi alle Linee guida;

e) informare i richiedenti in modo compiuto e chiaro, sulla procedura di certificazione e sui necessari requisiti tecnici per accedervi e sulle caratteristiche e sulle limitazioni d'uso delle firme emesse sulla base del servizio di certificazione;

[f) non rendersi depositario di dati per la creazione della firma del titolare;]

g) procedere alla tempestiva pubblicazione della **revoca** e della **sospensione** del certificato elettronico in caso di richiesta da parte del titolare di firma elettronica qualificata o del terzo dal quale derivino i poteri del titolare di firma elettronica qualificata medesimo, di perdita del possesso o della compromissione del dispositivo di firma o degli strumenti di autenticazione informatica per l'utilizzo del dispositivo di firma, di provvedimento dell'autorità, di acquisizione della conoscenza di cause limitative della capacità del titolare di firma elettronica qualificata, di sospetti abusi o falsificazioni, secondo quanto previsto dalle Linee guida;

CAD

[Segue Art. 32]

h) garantire un servizio di revoca e sospensione dei certificati elettronici sicuro e tempestivo nonché garantire il funzionamento efficiente, puntuale e sicuro degli elenchi dei certificati di firma emessi, sospesi e revocati;

i) assicurare la precisa determinazione della data e dell'ora di rilascio, di revoca e di sospensione dei certificati elettronici;

j) tenere registrazione, anche elettronica, di tutte le informazioni relative al certificato qualificato dal momento della sua emissione almeno per venti anni anche al fine di fornire prova della certificazione in eventuali procedimenti giudiziari;

k) non copiare, né conservare, le chiavi private di firma del soggetto cui il prestatore di servizi di firma elettronica qualificata ha fornito il servizio di certificazione;

l) predisporre su mezzi di comunicazione durevoli tutte le informazioni utili ai soggetti che richiedono il servizio di certificazione, tra cui in particolare gli esatti termini e condizioni relative all'uso del certificato, compresa ogni limitazione dell'uso, l'esistenza di un sistema di accreditamento facoltativo e le procedure di reclamo e di risoluzione delle controversie; dette informazioni, che possono essere trasmesse elettronicamente, devono essere scritte in linguaggio chiaro ed essere fornite prima dell'accordo tra il richiedente il servizio ed il prestatore di servizi di firma elettronica qualificata;

MASTER in diritto delle nuove tecnologie e informatica giuridica

61

CAD

[Segue Art. 32]

m) utilizzare sistemi affidabili per la gestione del registro dei certificati con modalità tali da garantire che soltanto le persone autorizzate possano effettuare inserimenti e modifiche, che l'autenticità delle informazioni sia verificabile, che i certificati siano accessibili alla consultazione del pubblico soltanto nei casi consentiti dal titolare del certificato e che l'operatore possa rendersi conto di qualsiasi evento che comprometta i requisiti di sicurezza. Su richiesta, elementi pertinenti delle informazioni possono essere resi accessibili a terzi che facciano affidamento sul certificato;

m-bis) garantire il corretto funzionamento e la continuità del sistema e comunicare immediatamente a AgID e agli utenti eventuali malfunzionamenti che determinano disservizio, sospensione o interruzione del servizio stesso.

4. Il prestatore di servizi di firma elettronica qualificata è responsabile dell'identificazione del soggetto che richiede il certificato qualificato di firma anche se tale attività è delegata a terzi.

[…]

MASTER in diritto delle nuove tecnologie e informatica giuridica

62

CAD

Art. 29. Qualificazione e accreditamento

1. I soggetti che intendono fornire servizi fiduciari qualificati o svolgere l'attività di gestore di posta elettronica certificata o di gestore dell'identità digitale di cui all'articolo 64 presentano all'AgID domanda di qualificazione, secondo le modalità fissate dalle Linee guida. I soggetti che intendono svolgere l'attività di conservatore di documenti informatici presentano all'AgID domanda di accreditamento, secondo le modalità fissate dalle Linee guida.

2. Il richiedente deve trovarsi nelle condizioni previste dall'articolo 24 del Regolamento eIDAS, deve avere natura giuridica di società di capitali e deve disporre dei requisiti di onorabilità, tecnologici e organizzativi, nonché delle garanzie assicurative e di eventuali certificazioni, adeguate rispetto al volume dell'attività svolta e alla responsabilità assunta nei confronti dei propri utenti e dei terzi. I predetti requisiti sono individuati, nel rispetto della disciplina europea, con decreto del Presidente del Consiglio dei ministri, sentita l'AgID. […].

CAD

Art. 30. Responsabilità dei prestatori di servizi fiduciari qualificati, dei gestori di posta elettronica certificata, dei gestori dell'identità digitale e di conservatori

1. I prestatori di servizi fiduciari qualificati, i gestori di posta elettronica certificata, i gestori dell'identità digitale e i conservatori di documenti informatici, iscritti nell'elenco di cui all'articolo 29, comma 6, che cagionano danno ad altri nello svolgimento della loro attività, **sono tenuti al risarcimento, se non provano di avere adottato tutte le misure idonee a evitare il danno**.

[2. Abrogato]

3. Il prestatore di servizi di firma digitale o di altra firma elettronica qualificata **non è responsabile dei danni derivanti dall'uso di un certificato qualificato che ecceda i limiti eventualmente posti dallo stesso** ai sensi dell'articolo 28, comma 3, a condizione che limiti d'uso e di valore siano chiaramente riconoscibili secondo quanto previsto dall'articolo 28, comma 3-bis.

Valore giuridico ed efficacia probatoria dei documenti informatici

Valore giuridico in senso stretto (o valore formale) = la capacità del documento informatico di costituire "forma scritta".

Efficacia (o valore) probatorio = la valenza del documento informatico in riferimento alla sua capacità di costituire prova nel processo.

MASTER in diritto delle nuove tecnologie e informatica giuridica

65

Documento informatico sottoscritto con firma elettronica avanzata, qualificata o digitale.

Valore giuridico ed efficacia probatoria

1-bis. Il documento informatico soddisfa il requisito della **forma scritta** e ha **l'efficacia prevista dall'articolo 2702 del Codice civile** quando vi è apposta una **firma digitale, altro tipo di firma elettronica qualificata o una firma elettronica avanzata** o, comunque, **è formato, previa identificazione informatica del suo autore**, **attraverso un processo avente i requisiti fissati dall'AgID ai sensi dell'articolo 71** con modalità tali da garantire la **sicurezza, integrità e immodificabilità** del documento e, in maniera manifesta e inequivoca, la sua riconducibilità all'autore.

1-ter. L'utilizzo del dispositivo di firma elettronica qualificata o digitale **si presume** riconducibile al titolare di firma elettronica, **salvo** che questi dia **prova contraria**. (art. 20)

MASTER in diritto delle nuove tecnologie e informatica giuridica

66

Valore giuridico ed efficacia probatoria dei documenti informatici

Art. 2702 c.c. (**Efficacia della scrittura privata**).

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 è legalmente considerata come riconosciuta (Cod. Proc. Civ. 214, 215).

Valore giuridico ed efficacia probatoria dei documenti informatici

Art. 2702 c.c. (**Efficacia della scrittura privata**).

Elementi essenziali «scrittura privata»:

1) **la cosa** destinata a recepire i segni grafici che formano la scrittura;
2) il **testo**;
3) la **sottoscrizione**.

Documento informatico sottoscritto con firma elettronica avanzata, qualificata o digitale.

Valore giuridico ed efficacia probatoria

2-bis. Salvo il caso di sottoscrizione autenticata, le scritture private di cui all'articolo 1350, primo comma, numeri da 1 a 12, del codice civile, se fatte con documento informatico, sono sottoscritte, **a pena di nullità**, con **firma elettronica qualificata o con firma digitale**.

Gli atti di cui all'articolo 1350, numero 13), del codice civile redatti su documento informatico o formati attraverso procedimenti informatici sono sottoscritti, **a pena di nullità**, con **firma elettronica avanzata, qualificata o digitale** ovvero sono formati con le ulteriori modalità di cui all'articolo 20, comma 1-bis, primo periodo. (art. 21 CAD)

69

Valore giuridico ed efficacia probatoria dei documenti informatici

Art. 1350 c.c. (Atti che devono farsi per iscritto).

Devono farsi per atto pubblico [c.c. 2699] o per scrittura privata [c.c. 2702], sotto pena di nullità:
1) i contratti che trasferiscono la proprietà di beni immobili;
2) i contratti che costituiscono, modificano o trasferiscono il diritto di usufrutto su beni immobili, il diritto di superficie, il diritto del concedente e dell'enfiteuta;
3) i contratti che costituiscono la comunione di diritti indicati dai numeri precedenti;
4) i contratti che costituiscono o modificano le servitù prediali, il diritto di uso su beni immobili e il diritto di abitazione;
5) gli atti di rinunzia ai diritti indicati dai numeri precedenti;
6) i contratti di affrancazione del fondo enfiteutico;
[...]
13) gli altri atti specialmente indicati dalla legge.

70

Documento informatico non sottoscritto e sottoscritto con firma elettronica c.d. semplice

Valore giuridico ed efficacia probatoria

1-bis. […] In tutti gli altri casi, l'idoneità del documento informatico a soddisfare il requisito della **forma scritta** e il suo **valore probatorio** sono **liberamente valutabili in giudizio**, in relazione alle caratteristiche di sicurezza, integrità e immodificabilità.

La data e l'ora di formazione del documento informatico sono opponibili ai terzi se apposte in conformità alle Linee guida. (art. 20 CAD).

Art. 23-quater. Riproduzioni informatiche

1. All'articolo 2712 del codice civile dopo le parole: «riproduzioni fotografiche» è inserita la seguente: «, informatiche».

71

Valore giuridico ed efficacia probatoria dei documenti informatici

Documento informatico non sottoscritto.

Efficacia probatoria

Art. 2712 c.c. (Riproduzioni meccaniche).

Le riproduzioni fotografiche, **informatiche** o cinematografiche, le registrazioni fonografiche e, in genere, ogni altra rappresentazione meccanica di fatti e di cose formano **piena prova** dei fatti e delle cose rappresentate, se colui contro il quale sono prodotte non ne disconosce la conformità ai fatti e alle cose medesime.

72

Valore giuridico ed efficacia probatoria dei documenti informatici

Documento informatico non sottoscritto.

Si noti come l'efficacia probatoria sia disciplinata in modo differente da due diverse norme => art. 2712 c.c. e art. 20 CAD.

- Per alcuni autori si tratta di una "anomalia" sulla quale ci si augura il legislatore intervenga quanto prima.

- Per altri l'art. 20 CAD disciplinerebbe il «documento», l'art. 2712 c.c. le «riproduzioni».

MASTER in diritto delle nuove tecnologie e informatica giuridica

73

Forma scritta e clausole vessatorie

Art. 1341. (Condizioni generali di contratto).
Le condizioni generali di contratto predisposte da uno dei contraenti sono efficaci nei confronti dell'altro, se al momento della conclusione del contratto questi le ha conosciute o avrebbe dovuto conoscerle usando l'ordinaria diligenza.

In ogni caso non hanno effetto, se non sono specificatamente approvate per iscritto, le condizioni che stabiliscono, a favore di colui che le ha predisposte: limitazioni di responsabilità, facoltà di recedere dal contratto o di sospenderne l'esecuzione, ovvero sanciscono a carico dell'altro contraente decadenze, limitazioni alla facoltà di opporre eccezioni, restrizioni alla libertà contrattuale nei rapporti coi terzi, tacita proroga o rinnovazione del contratto, clausole compromissorie o deroghe alla competenza dell'autorità giudiziaria.

MASTER in diritto delle nuove tecnologie e informatica giuridica

74

Forma scritta e clausole vessatorie

Art. 1341. (Condizioni generali di contratto).
«specificatamente approvate per iscritto» => significa in forma scritta e con approvazione specifica

NON è equivalente a «specifica sottoscrizione per iscritto».

Scrittura => certezza all'atto (requisito di forma).

Sottoscrizione => approvazione specifica
(funzione della sottoscrizione => indicativa (individua l'autore) + dichiarativa (volontà di assumere paternità => effetti)

MASTER in diritto delle nuove tecnologie e informatica giuridica

75

Valore giuridico ed efficacia probatoria dei documenti informatici

L'apposizione a un documento informatico di una **firma digitale** o di un altro tipo di firma elettronica **qualificata** basata su un certificato elettronico revocato, scaduto o sospeso **equivale a mancata sottoscrizione**, salvo che lo stato di sospensione sia stato annullato.

La revoca o la sospensione, comunque motivate, hanno effetto dal momento della pubblicazione, salvo che il revocante, o chi richiede la sospensione, non dimostri che essa era già a conoscenza di tutte le parti interessate. (art. 24).

MASTER in diritto delle nuove tecnologie e informatica giuridica

76

Copie analogiche, copie informatiche e duplicati

Art. 1 CAD

i-bis) **copia informatica di documento analogico**: il documento informatico avente contenuto identico a quello del documento analogico da cui è tratto;

i-ter) **copia per immagine su supporto informatico di documento analogico**: il documento informatico avente contenuto e forma identici a quelli del documento analogico da cui è tratto;

i-quater) **copia informatica di documento informatico**: il documento informatico avente contenuto identico a quello del documento da cui è tratto su supporto informatico con diversa sequenza di valori binari;

i-quinquies) **duplicato informatico**: il documento informatico ottenuto mediante la memorizzazione, sullo stesso dispositivo o su dispositivi diversi, della medesima sequenza di valori binari del documento originario;

Copie analogiche, copie informatiche e duplicati

CAD

Art. 22. Copie informatiche di documenti analogici

3. Le copie per immagine su supporto informatico di documenti originali formati in origine su supporto analogico nel rispetto delle Linee guida hanno la stessa efficacia probatoria degli originali da cui sono tratte se la loro conformità all'originale non è espressamente disconosciuta.

Art. 23. Copie analogiche di documenti informatici

2. Le copie e gli estratti su supporto analogico del documento informatico, conformi alle vigenti regole tecniche, hanno la stessa efficacia probatoria dell'originale se la loro conformità non è espressamente disconosciuta. Resta fermo, ove previsto l'obbligo di conservazione dell'originale informatico.

Copie analogiche, copie informatiche e duplicati

Art. 1 CAD

Art. 23-bis. Duplicati e copie informatiche di documenti informatici

1. I duplicati informatici hanno il medesimo valore giuridico, ad ogni effetto di legge, del documento informatico da cui sono tratti, se prodotti in conformità alle Linee guida.

2. Le copie e gli estratti informatici del documento informatico, se prodotti in conformità alle vigenti Linee guida, hanno la stessa efficacia probatoria dell'originale da cui sono tratte se la loro conformità all'originale, in tutti le sue componenti, è attestata da un **pubblico ufficiale** a ciò autorizzato o se la conformità non è espressamente disconosciuta. Resta fermo, ove previsto, l'obbligo di conservazione dell'originale informatico.

Regole tecniche

3. Le **regole tecniche** per la formazione, per la trasmissione, la conservazione, la copia, la duplicazione, la riproduzione e la validazione dei documenti informatici, nonché quelle in materia di generazione, apposizione e verifica di qualsiasi tipo di firma elettronica, sono stabilite con le **Linee guida**. (art. 20)

Le regole tecniche AGID

https://www.agid.gov.it/it/linee-guida

- Linee Guida sulla formazione, gestione e conservazione dei documenti informatici [e relativi allegati, n.d.r.]

https://www.agid.gov.it/sites/default/files/repository_files/linee_guida_sul_documento_informatico_.pdf

- Linee guida contenenti le Regole Tecniche e Raccomandazioni afferenti la generazione di certificati elettronici qualificati, firme e sigilli elettronici qualificati e validazioni temporali elettroniche qualificate

https://www.agid.gov.it/sites/default/files/repository_files/regole_tecniche_e_raccomandazioni_v1.1_0.pdf

- D.P.C.M. 22 febbraio 2013 - Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali, ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma 3, lettera b), 35, comma 2, 36, comma 2, e 71.

[…]

Valore giuridico ed efficacia probatoria dei documenti informatici

Firma autenticata (art. 25).

1. Si ha per riconosciuta, ai sensi dell'articolo 2703 del codice civile, la firma elettronica o qualsiasi altro tipo di firma elettronica avanzata **autenticata** dal notaio o da altro pubblico ufficiale a ciò autorizzato.

2. **L'autenticazione** della firma elettronica, anche mediante l'acquisizione digitale della sottoscrizione autografa, o di qualsiasi altro tipo di firma elettronica avanzata 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 dell'eventuale certificato elettronico utilizzato e del fatto che il documento sottoscritto non è in contrasto con l'ordinamento giuridico.

Valore giuridico ed efficacia probatoria dei documenti informatici

Segue: Firma autenticata.

3. L'apposizione della firma digitale 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.
[...].

Atto pubblico informatico → D.Lgs. 110/2010 → D.L. 18 ottobre 2012, n. 179, convertito con modificazioni nella legge 17 dicembre 2012, n. 221.

Validazione temporale del documento informatico

Reg. UE 910/2014

33) «**validazione temporale elettronica**», dati in forma elettronica che collegano altri dati in forma elettronica a una particolare ora e data, così da provare che questi ultimi esistevano in quel momento;

34) «**validazione temporale elettronica qualificata**», una validazione temporale elettronica che soddisfa i requisiti di cui all'articolo 42;

Validazione temporale del documento informatico

Si ottiene mediante la creazione (attraverso un'apposita coppia di chiavi) e l'applicazione al documento informatico - da parte di un **certificatore** - di una c.d. **marca temporale** (*time stamping*).

La data e l'ora di formazione del documento informatico sono opponibili ai terzi se apposte in conformità alle Linee guida. (art. 20).

Validazione temporale del documento informatico

Marca temporale
(art. 1, DPCM 22.2.2013)

- **marca temporale**: il riferimento temporale che consente la validazione temporale e che dimostra l'esistenza di un'evidenza informatica in un tempo certo;

- **riferimento temporale**: evidenza informatica, contenente la data e l'ora, che viene associata ad uno o più documenti informatici;

- **evidenza informatica**: una sequenza di simboli binari (bit) che può essere elaborata da una procedura informatica.

Validazione temporale del documento informatico

Validazione temporale con marca temporale
(art. 47, DPCM 22.2.2013)

1. Una **evidenza informatica** è sottoposta a validazione temporale mediante generazione e applicazione di una marca temporale alla relativa impronta. […]

Precisione dei sistemi di validazione temporale
(art. 51, DPCM 22.2.2013)

1. Il riferimento temporale assegnato ad una marca temporale **coincide con il momento della sua generazione**, con una differenza non superiore ad un minuto secondo rispetto alla scala di tempo UTC(IEN), di cui al decreto del Ministro dell'industria, del commercio e dell'artigianato 30 novembre 1993, n. 591.
2. Il riferimento temporale contenuto nella marca temporale è specificato con riferimento al Tempo Universale Coordinato (UTC).

MASTER in diritto delle nuove tecnologie e informatica giuridica

87

Validazione temporale del documento informatico

Richiesta di marca temporale
(art. 54, DPCM 22.2.2013)

1. Il certificatore stabilisce, pubblicandole nel manuale operativo, le procedure per l'invio della richiesta di marca temporale.
2. **La richiesta contiene l'evidenza informatica alla quale applicare la marca temporale**.
3. L'evidenza informatica può essere sostituita da una o più impronte, calcolate con funzioni di hash scelte dal certificatore tra quelle stabilite ai sensi dell'art. 4, comma 2.
4. La generazione delle marche temporali garantisce un tempo di risposta, misurato come differenza tra il momento della ricezione della richiesta e l'ora riportata nella marca temporale, **non superiore al minuto primo**.

MASTER in diritto delle nuove tecnologie e informatica giuridica

88

Validazione temporale del documento informatico

Valore delle firme elettroniche qualificate e digitali nel tempo
(art. 62, DPCM 22.2.2013)

1. Le firme elettroniche qualificate e digitali, **ancorché sia scaduto, revocato o sospeso il relativo certificato qualificato** del sottoscrittore, sono valide **se** alle stesse è associabile un riferimento temporale opponibile ai terzi che collochi la generazione di dette firme rispettivamente in un momento **precedente** alla scadenza, revoca o sospensione del suddetto certificato.

Conservazione del documento informatico

Art. 43. Conservazione ed esibizione dei documenti

1. Gli obblighi di conservazione e di esibizione di documenti si intendono soddisfatti a tutti gli effetti di legge a mezzo di documenti informatici, se le relative procedure sono effettuate in modo tale da garantire la conformità ai documenti originali e sono conformi alle Linee guida.

1-bis. Se il documento informatico è conservato per legge da uno dei soggetti di cui all'articolo 2, comma 2, cessa l'obbligo di conservazione a carico dei cittadini e delle imprese che possono in ogni momento richiedere accesso al documento stesso ai medesimi soggetti di cui all'articolo 2, comma 2. Le amministrazioni rendono disponibili a cittadini ed imprese i predetti documenti attraverso servizi on-line accessibili previa identificazione con l'identità digitale di cui all'articolo 64 ed integrati con i servizi di cui agli articoli 40-ter e 64-bis.

2. Restano validi i documenti degli archivi, le scritture contabili, la corrispondenza ed ogni atto, dato o documento già conservati mediante riproduzione su supporto fotografico, su supporto ottico o con altro processo idoneo a garantire la conformità dei documenti agli originali ai sensi della disciplina vigente al momento dell'invio dei singoli documenti nel sistema di conservazione.

3. I documenti informatici, di cui è prescritta la conservazione per legge o regolamento, possono essere archiviati per le esigenze correnti anche con modalità cartacee e sono conservati in modo permanente con modalità digitali, nel rispetto delle Linee guida.

[…]

Valore giuridico ed efficacia probatoria dei documenti informatici

Art. 45. Valore giuridico della trasmissione.

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.

Domicilio digitale

n-ter) **domicilio digitale**: un indirizzo elettronico eletto presso un servizio di posta elettronica certificata o un servizio elettronico di recapito certificato qualificato, come definito dal regolamento (UE) 23 luglio 2014 n. 910 del Parlamento europeo e del Consiglio in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE, di seguito "Regolamento eIDAS", valido ai fini delle comunicazioni elettroniche aventi valore legale; [art. 1 CAD]