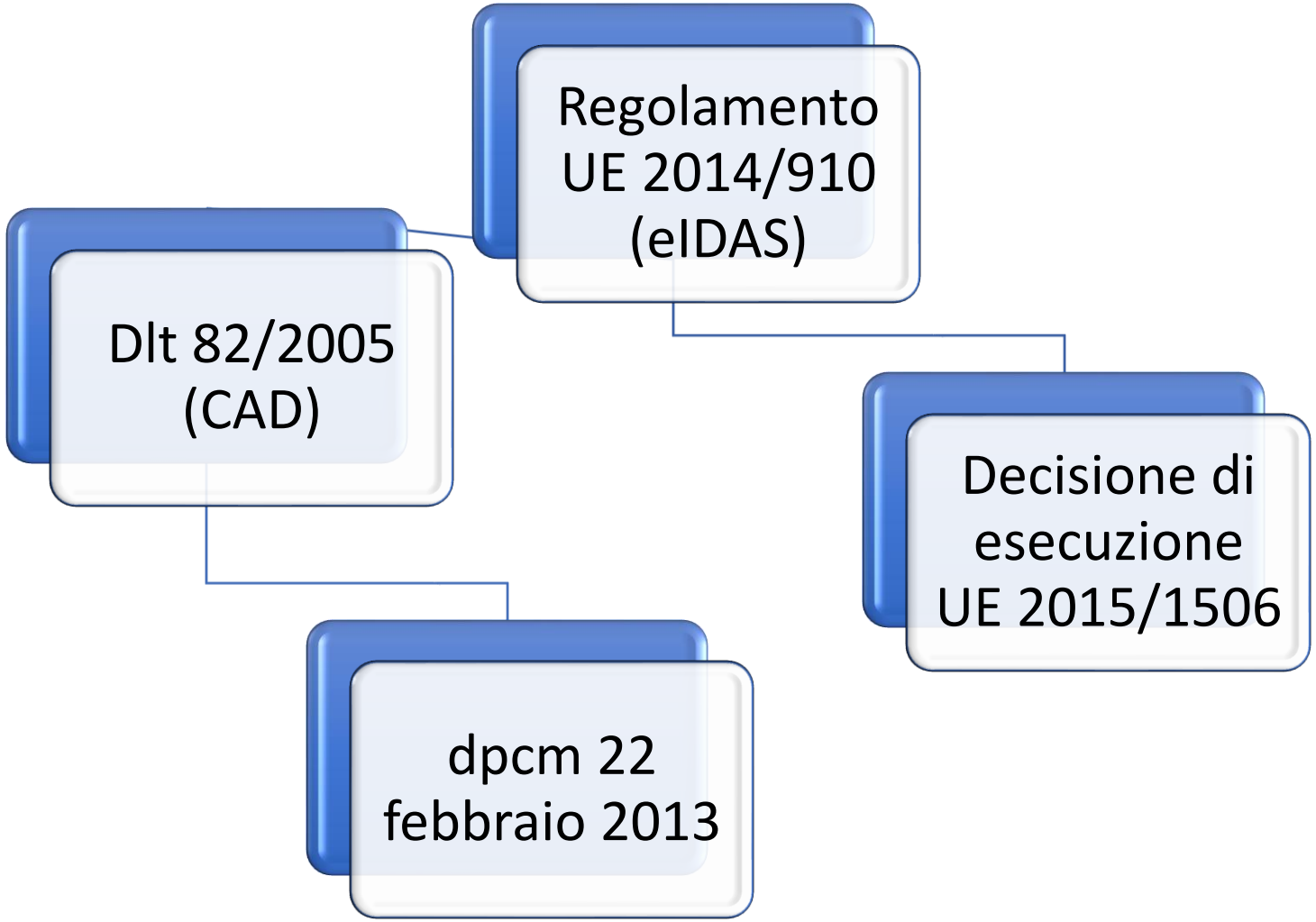
LE FIRME ELETTRONICHE

Napoli, 13 Febbraio 2018 – Sala Metafora

Avv. Roberto Arcella (Gruppo di Lavoro F.I.I.F.)

LE FONTI NORMATIVE



DEFINIZIONI

ART. 3 eIDAS

- (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;
- (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

Art. 26 eIDAS

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**.

DEFINIZIONI

DEFINIZIONE EIDAS

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

DEFINIZIONE CAD ABROGATA (ART. 1 LETT. Q)

«**firma elettroni**ca» : l'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati *come metodo di identificazione informatica*

La firma elettronica perde quindi la funzione *di identificazione informatica* e conserva solo la funzione di «*firma*», vale a dire quella di attribuzione della paternità del documento, conferma o accettazione del contenuto, oltre che per garantire l'origine e, a certe condizioni, l'integrità del documento cui si riferisce

FIRMA PREVIA IDENTIFICAZIONE (dlt 217/2017)

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 immodificabilita' del documento e, in maniera manifesta e inequivoca, la sua riconducibilita' all'autore (ART. 20, COMMA 1 BIS CAD)

Art. 35, comma 2, CAD: «*I documenti informatici devono essere presentati al titolare di firma elettronica, prima dell'apposizione della firma, chiaramente e senza ambiguità, e si deve richiedere conferma della volontà di generare la firma secondo quanto previsto dalle Linee guida*».

Ques

DIFFERENZA TRA «*FIRMA*» E «*SIGILLO*»

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

«**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***

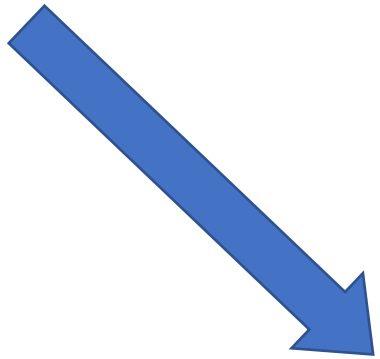
Nel sigillo manca la funzione di «firma» e garantisce solo «origine ed integrità»
I sigilli si riferiscono a persone giuridiche (considerando n. «*Qualora una transazione richieda un sigillo elettronico qualificato di una persona giuridica, è opportuno che sia accettabile anche la firma elettronica qualificata del rappresentante autorizzato della persona giuridica*» e art. 1 n. 29 «*certificato di sigillo elettronico», un attestato elettronico che collega i dati di convalida di un sigillo elettronico a una persona giuridica e conferma il nome di tale persona*»

DEFINIZIONI

C.A.D., art. 1

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 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*

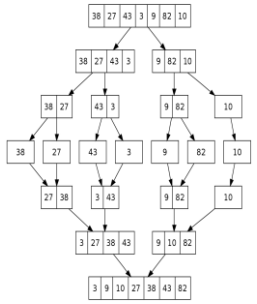
CHIAVE PRIVATA E CHIAVE PUBBLICA



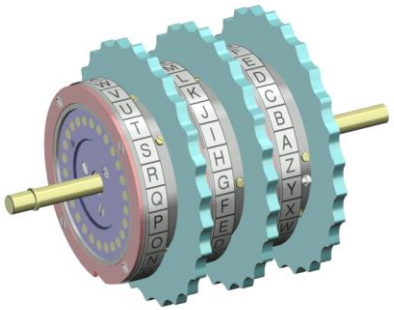
PER FIRMARE

PER VERIFICARE

Apposizione di una firma digitale



Impronta SHA256: ca0e07d71bb268ce844a3f1db4bff61ecbd69bac71db7eb77599e334c4776751



CHIAVE PRIVATA

Documento firmato digitalmente

Alcuni concetti sulla crittografia….

Algoritmo di cifratura: è metodo di calcolo con il quale, dato un messaggio in chiaro, si produce il corrispondente messaggio cifrato.

Chiave di cifratura: è un valore che viene abbinato all'algoritmo per cifrare un documento o un messaggio

Algoritmo a chiave simmetrica (o a chiave segreta): un'unica chiave serve sia per cifrare che per decifrare.

Algoritmo a chiave asimmetrica (o a chiave pubblica): ci sono due chiavi: se una viene usata per cifrare, occorre l'altra per decifrare (e viceversa) una segreta, l'altra pubblica.

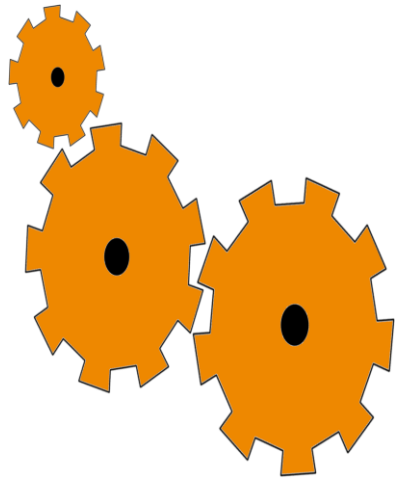
Impronta (digest) di un messaggio: è una stringa di dimensione fissa calcolata a partire dal messaggio originale, ma indipendente dalla dimensione dello stesso

Verifica di una firma digitale

Documento

Impronta crittografata= firma digitale

Certificato con chiave pubblica del sottoscrittore



funzione di hash

Impronta SHA256: ca0e07d71bb268ce844a3f1db4bff61ecbd69bac71db7eb77599e334c4776751

Impronta n. 1

Impronta SHA256: ca0e07d71bb268ce844a3f1db4bff61ecbd69bac71db7eb77599e334c4776751

Impronta n. 2

Trusted list

Art. 34, 3° co., dpcm 22.2.3013

«Le liste pubblicate dei certificati revocati e sospesi, nonché i certificati qualificati eventualmente resi accessibili alla consultazione del pubblico, sono utilizzabili da chi li consulta per le sole finalità di applicazione delle norme che disciplinano la verifica e la validità delle firme elettroniche qualificate e digitali.»

Trusted list

DEFINIZIONI

Art. 25, comma 3 del Regolamento 910/2014

"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"

La firma digitale italiana è, nel contesto europeo, a tutti gli effetti una firma elettronica qualificata.

DEFINIZIONI

eIDAS

Art. 3 n. 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

Art. 3 n. 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

Allegato I

I certificati qualificati di firma elettronica contengono:

a) indicazione del fatto che il certificato è stato rilasciato quale certificato qualificato di firma elettronica;
b) un insieme di dati che indicano il prestatore di servizi fiduciari qualificato che rilascia i certificati e l'indicazione dello Stato membro di rilascio
c) nome o pseudonimo del firmatario
d) i 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

FIIF

DEFINIZIONI

CAD

Art. 28, comma 1 (definizione di Certificati di firma elettronica qualificata): ABROGATO

Art. 28, commi da 2 a 4 bis:

Il certificato **può** contenere inoltre

- **Codice Fiscale** del soggetto
- 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;
- **i limiti d'uso** del certificato, inclusi quelli derivanti da qualifiche e poteri di rappresentanza;
- i 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.

Queste informazioni devono essere **riconoscibili** da parte dei terzi e chiaramente evidenziati nel certificato o (tranne il CF) essere rese disponibili anche in rete (rinvio alle linee guida)

Il certificatore ha l'obbligo di conservare le informazioni di cui ai commi 3 e 4 per almeno VENTI ANNI decorrenti dalla scadenza del certificato di firma.

FIIF

DEFINIZIONI

CAD

Art. 28, comma 1 (definizione di Certificati di firma elettronica qualificata): ABROGATO

Art. 28, commi da 2 a 4 bis:

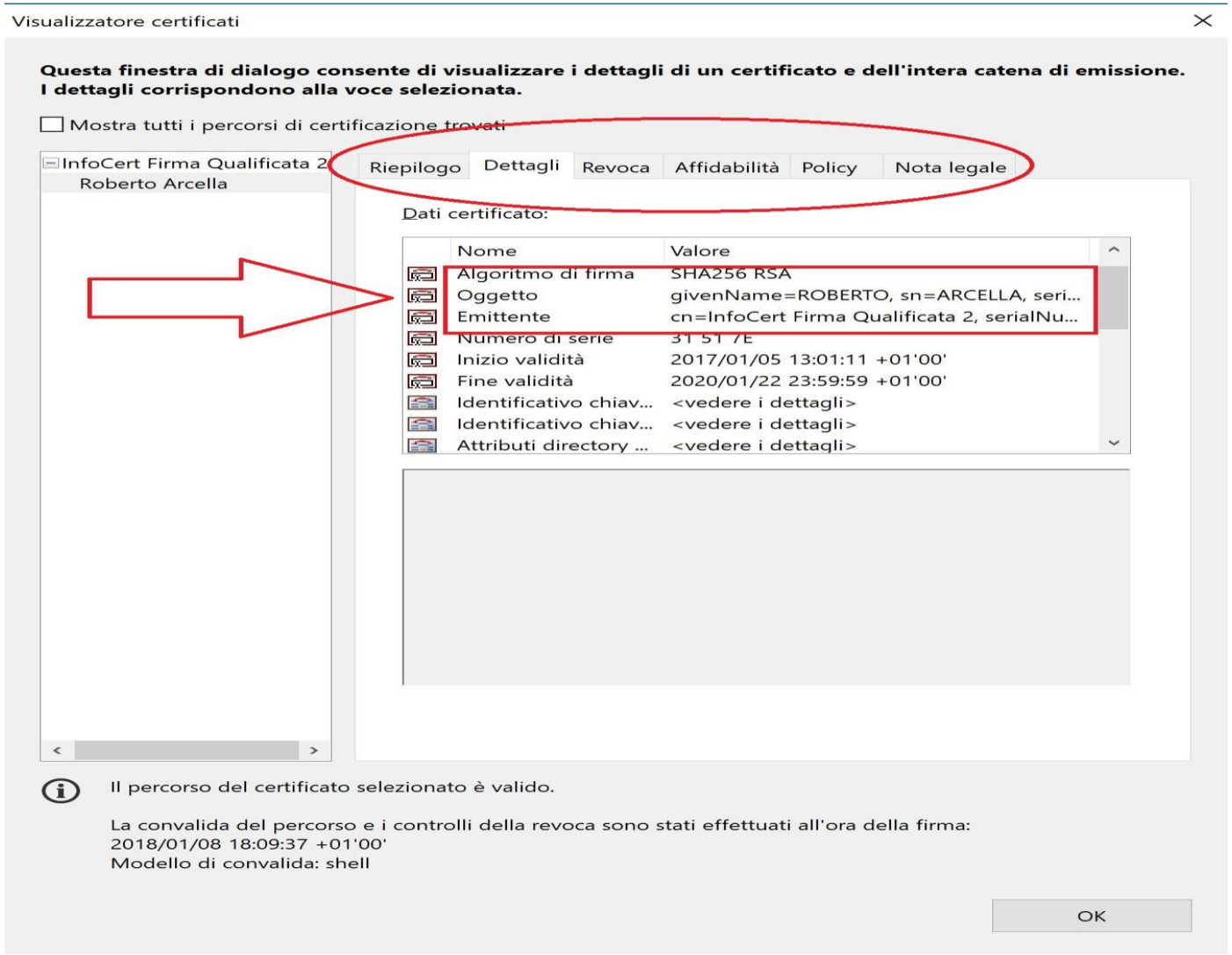
Il certificato **PUÒ** contenere inoltre

- **Codice Fiscale** del soggetto
- 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;
- **i limiti d'uso** del certificato, inclusi quelli derivanti da qualifiche e poteri di rappresentanza;
- i 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.

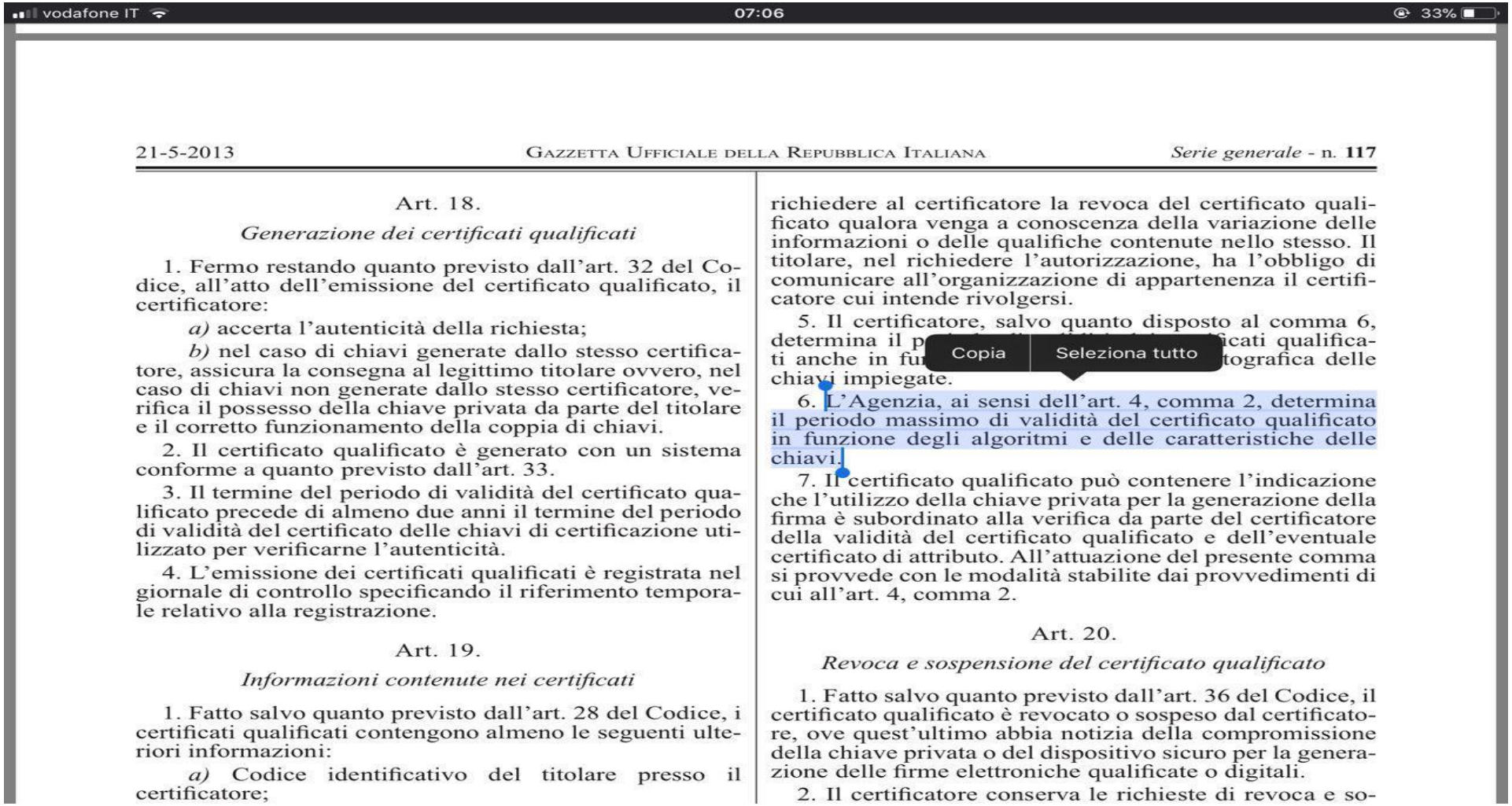
Queste informazioni devono essere **riconoscibili** da parte dei terzi e chiaramente evidenziati nel certificato o (tranne il CF) essere rese disponibili anche in rete (rinvio alle linee guida)

Il certificatore ha l'obbligo di conservare le informazioni di cui ai commi 3 e 4 per almeno VENTI ANNI decorrenti dalla scadenza del certificato di firma.

INFORMAZIONI CONTENUTE NEI CERTIFICATI



PERIODO VALIDITA' DEI CERTIFICATI: PERCHE'?



vodafone IT 07:06 33%

21-5-2013 GAZZETTA UFFICIALE DELLA REPUBBLICA ITALIANA *Serie generale* - n. **117**

Art. 18.

Generazione dei certificati qualificati

1. Fermo restando quanto previsto dall'art. 32 del Codice, all'atto dell'emissione del certificato qualificato, il certificatore:

a) accerta l'autenticità della richiesta;

b) nel caso di chiavi generate dallo stesso certificatore, assicura la consegna al legittimo titolare ovvero, nel caso di chiavi non generate dallo stesso certificatore, verifica il possesso della chiave privata da parte del titolare e il corretto funzionamento della coppia di chiavi.

2. Il certificato qualificato è generato con un sistema conforme a quanto previsto dall'art. 33.

3. Il termine del periodo di validità del certificato qualificato precede di almeno due anni il termine del periodo di validità del certificato delle chiavi di certificazione utilizzato per verificarne l'autenticità.

4. L'emissione dei certificati qualificati è registrata nel giornale di controllo specificando il riferimento temporale relativo alla registrazione.

Art. 19.

Informazioni contenute nei certificati

1. Fatto salvo quanto previsto dall'art. 28 del Codice, i certificati qualificati contengono almeno le seguenti ulteriori informazioni:

a) Codice identificativo del titolare presso il certificatore;

richiedere al certificatore la revoca del certificato qualificato qualora venga a conoscenza della variazione delle informazioni o delle qualifiche contenute nello stesso. Il titolare, nel richiedere l'autorizzazione, ha l'obbligo di comunicare all'organizzazione di appartenenza il certificatore cui intende rivolgersi.

5. Il certificatore, salvo quanto disposto al comma 6, determina il p… …icati qualificati anche in fu… …tografica delle chiavi impiegate.

Copia Seleziona tutto

6. L'Agenzia, ai sensi dell'art. 4, comma 2, determina il periodo massimo di validità del certificato qualificato in funzione degli algoritmi e delle caratteristiche delle chiavi.

7. Il certificato qualificato può contenere l'indicazione che l'utilizzo della chiave privata per la generazione della firma è subordinato alla verifica da parte del certificatore della validità del certificato qualificato e dell'eventuale certificato di attributo. All'attuazione del presente comma si provvede con le modalità stabilite dai provvedimenti di cui all'art. 4, comma 2.

Art. 20.

Revoca e sospensione del certificato qualificato

1. Fatto salvo quanto previsto dall'art. 36 del Codice, il certificato qualificato è revocato o sospeso dal certificatore, ove quest'ultimo abbia notizia della compromissione della chiave privata o del dispositivo sicuro per la generazione delle firme elettroniche qualificate o digitali.

2. Il certificatore conserva le richieste di revoca e so-

EIDAS - NUOVI REQUISITI DI SICUREZZA DEI CERTIFICATI

Art. 51 eIDAS - Disposizioni transitorie

1. I dispositivi per la creazione di una firma sicura la cui conformità sia stata determinata a norma dell'articolo 3, paragrafo 4, della direttiva 1999/93/CE sono considerati dispositivi per la creazione di una firma elettronica qualificata a norma del presente regolamento.

2. I certificati qualificati rilasciati a persone fisiche a norma della direttiva 1999/93/CE sono considerati certificati qualificati di firma elettronica a norma del presente regolamento fino alla loro scadenza.

3. Un prestatore di servizi di certificazione che rilascia certificati qualificati a norma della direttiva 1999/93/CE presenta una relazione di valutazione della conformità all'organismo di vigilanza quanto prima e, comunque, non oltre il 1º luglio 2017. Fino alla presentazione della suddetta relazione di valutazione della conformità e fino a che l'organismo di vigilanza non ne abbia completato la valutazione, il prestatore di servizi di certificazione è considerato un prestatore di servizi fiduciari qualificato a norma del presente regolamento.

4. Se un prestatore di servizi di certificazione che rilascia certificati qualificati a norma della direttiva 1999/93/CE non presenta una relazione di valutazione della conformità all'organismo di vigilanza entro i termini di cui al paragrafo 3, egli non è considerato un prestatore di servizi fiduciari qualificato a norma del presente regolamento a decorrere dal 2 luglio 2017.

EIDAS - NUOVI REQUISITI DI SICUREZZA DEI CERTIFICATI

Art. 62, co. 4, dlt 179/2016

«…I certificati qualificati rilasciati prima dell'entrata in vigore del presente decreto a norma della direttiva 1999/93/CE, sono considerati certificati qualificati di firma elettronica a norma del regolamento eIDAS e dell'articolo 28 del decreto legislativo n. 82 del 2005, come modificato dall'articolo 24 del presente decreto, fino alla loro scadenza».

PERIODO VALIDITA' DEI CERTIFICATI: PERCHE'?

Art. 62, co. 4, dlt 179/2016

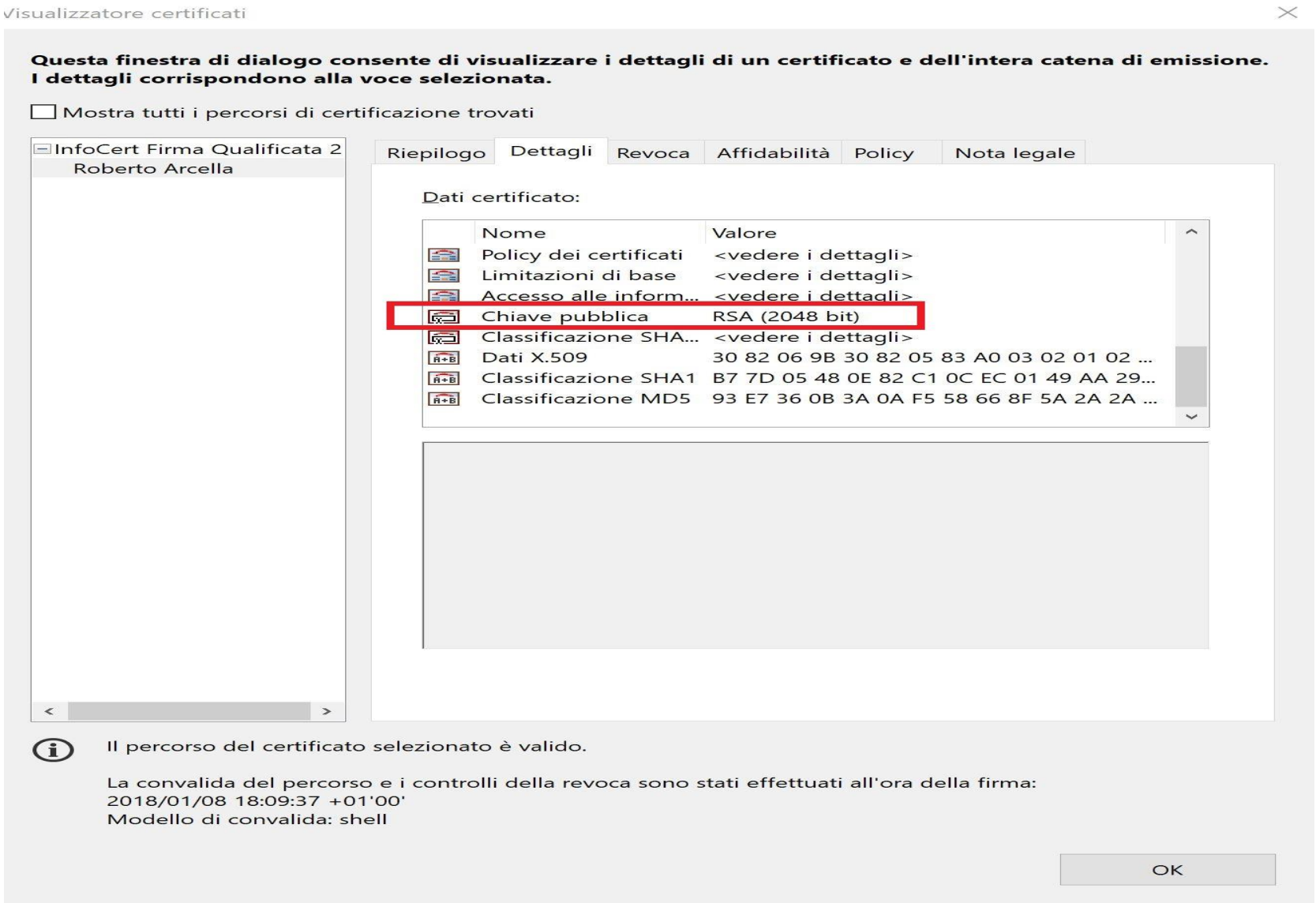
«…I certificati qualificati rilasciati prima dell'entrata in vigore del presente decreto a norma della direttiva 1999/93/CE, sono considerati certificati qualificati di firma elettronica a norma del regolamento eIDAS e dell'articolo 28 del decreto legislativo n. 82 del 2005, come modificato dall'articolo 24 del presente decreto, fino alla loro scadenza».

EIDAS - NUOVI REQUISITI DI SICUREZZA DEI CERTIFICATI

eIDAS, al «considerando» n. 55, richiama lo standard di sicurezza informatica ISO 15408…

«La certificazione della sicurezza delle tecnologie d'informazione basata su norme internazionali, come l'ISO 15408 e i metodi di valutazione e le disposizioni di riconoscimento reciproco connessi, è uno strumento importante per verificare la sicurezza dei dispositivi per la creazione di una firma elettronica qualificata e dovrebbe essere promossa…»

La Decisione di esecuzione (UE) 2015/1506 della Commissione, dell'8 settembre 2015, stabilisce le specifiche relative ai formati delle firme elettroniche avanzate e dei sigilli avanzati che gli organismi del settore pubblico devono riconoscere, di cui all'articolo 27 eIDAS


Visualizzatore certificati
Questa finestra di dialogo consente di visualizzare i dettagli di un certificato e dell'intera catena di emissione.
I dettagli corrispondono alla voce selezionata.
Mostra tutti i percorsi di certificazione trovati
InfoCert Firma Qualificata 2
Roberto Arcella
Riepilogo
Dettagli
Revoca
Affidabilità
Policy
Nota legale
Dati certificato:
Nome
Valore
Policy dei certificati
<vedere i dettagli>
Limitazioni di base
<vedere i dettagli>
Accesso alle inform...
<vedere i dettagli>
Chiave pubblica
RSA (2048 bit)
Classificazione SHA...
<vedere i dettagli>
Dati X.509
30 82 06 9B 30 82 05 83 A0 03 02 01 02 ...
Classificazione SHA1
B7 7D 05 48 0E 82 C1 0C EC 01 49 AA 29...
Classificazione MD5
93 E7 36 0B 3A 0A F5 58 66 8F 5A 2A 2A ...
Il percorso del certificato selezionato è valido.
La convalida del percorso e i controlli della revoca sono stati effettuati all'ora della firma:
2018/01/08 18:09:37 +01'00'
Modello di convalida: shell
OK

Le firme nel C.A.D.
Validita’ ed efficacia

Art. 24. Firma digitale.

1. La firma digitale deve riferirsi in maniera univoca ad un solo soggetto ed al documento o all'insieme di documenti cui è apposta o associata.

2. L'apposizione di firma digitale integra e sostituisce l'apposizione di sigilli, punzoni, timbri, contrassegni e marchi di qualsiasi genere ad ogni fine previsto dalla normativa vigente.

3. **Per la generazione della firma digitale deve adoperarsi un certificato qualificato che, al momento della sottoscrizione, non risulti scaduto di validità ovvero non risulti revocato o sospeso.**

4. Attraverso il certificato qualificato si devono rilevare, secondo le Linee guida, la validità del certificato stesso, nonché gli elementi identificativi del titolare di firma digitale e del certificatore e gli eventuali limiti d'uso. Le linee guida definiscono altresì le modalità, anche temporali, di apposizione della firma.

4-bis. 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. 20. Validità ed efficacia probatoria dei Documenti informatici.

1. *(abrogato)*

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 immodificabilita' del documento e, in maniera manifesta e inequivoca, la sua riconducibilita' all'autore. 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 immodificabilita'. La data e l'ora di formazione del documento informatico sono opponibili ai terzi se apposte in conformità alle Linee guida.

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.

1-quater. Restano ferme le disposizioni concernenti il deposito degli atti e dei documenti in via telematica secondo la normativa, anche regolamentare, in materia di processo telematico.

Art. 2702 c.c.: La scrittura privata fa piena prova, fino a querela di falso, 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

Art. 20, co. 1 bis
(dopo dlt 217/2017)

Tribunale di Roma – sent. 1127/2017 del 23/01/2017

«*…che nella fattispecie oggetto di giudizio deve essere applicato* ***l'art. 21****, secondo comma del Codice dell'Amministrazione Digitale, secondo cui, in relazione al tipo di documento (informatico) e di firma (digitale) in esame nella presente controversia, l'utilizzo del dispositivo di firma "si presume riconducibile al titolare, salvo che questi dia prova contraria"; vi è, quindi, una inversione dell'onere della prova e compete a chi opera il disconoscimento della sottoscrizione per smentire di avere egli sottoscritto…*»

«*…l'onere di provare chi abbia utilizzato il dispositivo di firma digitale, con cui è stato sottoscritto la cessione in argomento, compete proprio all'odierno attore, che era il titolare del dispositivo in questione…*»

«*…detto dispositivo era nella disponibilità del Fiore e che era stato abusivamente utilizzato da quest'ultimo. Inoltre… l'attore ha affermato che, alla data e all'ora della presunta sottoscrizione, egli si trovava presso l'abitazione delle signore Marina e Valentina Pervova, in via Merulana n. 43, ove si era trattenuto sin dalla sera prima e che aveva lasciato soltanto intorno alle ore 11.30 del 13.3.2013; al riguardo ha prodotto copia delle* ***ricevute relative al pagamento*** *del parcheggio situato in via Buonarroti n. 16…*»

Tribunale di Roma – sent. 1127/2017 del 23/01/2017

«*…detto dispositivo era nella disponibilità del Fiore e che era stato abusivamente utilizzato da quest'ultimo. Inoltre… l'attore ha affermato che, alla data e all'ora della presunta sottoscrizione, egli si trovava presso l'abitazione delle signore Marina e Valentina Pervova, in via Merulana n. 43, ove si era trattenuto sin dalla sera prima e che aveva lasciato soltanto intorno alle ore 11.30 del 13.3.2013; al riguardo ha prodotto copia delle* ***ricevute relative al pagamento*** *del parcheggio situato in via Buonarroti n. 16…*»

N.B.: **Art. 32. «***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*»

Art. 21. Ulteriori disposizioni relative ai documenti informatici, sottoscritti con firma elettronica avanzata, qualificata o digitale

1. - 2. *(abrogati)*

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, primo comma, n. 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.

2-ter. Fatto salvo quanto previsto dal decreto legislativo 2 luglio 2010, n. 110, ogni altro atto pubblico redatto su documento informatico è sottoscritto dal pubblico ufficiale a pena di nullità con firma qualificata o digitale. Le parti, i fidefacenti, l'interprete e i testimoni sottoscrivono personalmente l'atto, in presenza del pubblico ufficiale, con firma avanzata, qualificata o digitale ovvero con firma autografa acquisita digitalmente e allegata agli atti.

Art. 21. Ulteriori disposizioni relative ai documenti informatici, sottoscritti con firma elettronica avanzata, qualificata o digitale

1. - 2. *(abrogati)*

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, primo comma, n. 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.

2-ter. Fatto salvo quanto previsto dal decreto legislativo 2 luglio 2010, n. 110, ogni altro atto pubblico redatto su documento informatico è sottoscritto dal pubblico ufficiale a pena di nullità con firma qualificata o digitale. Le parti, i fidefacenti, l'interprete e i testimoni sottoscrivono personalmente l'atto, in presenza del pubblico ufficiale, con firma avanzata, qualificata o digitale ovvero con firma autografa acquisita digitalmente e allegata agli atti.

TIPI DI FIRMA DIGITALE

La firma **CAdES** (CMS Advanced Electronic Signatures) è una firma digitale che può essere apposta su **qualsiasi** tipo di file. Tale modalità di firma genera una **"busta crittografica"** contenente il documento informatico originale e si caratterizza per il suffisso P7M che si aggiunge all'estensione del file (es. citazione.pdf.p7m). In altri termini, nella firma CAdES il documento oggetto di firma digitale viene incapsulato in un contenitore informatico "chiuso" con una firma digitale, che ne garantisce quindi l'autenticità e l'integrità (oltre che il "non ripudio").

La firma **PAdES** (PDF Advanced Electronic Signatures), invece, è una firma che può essere apposta solo su file PDF: in tal caso, l'apposizione di una firma PAdES lascia immutata l'estensione del documento, che continuerà a chiamarsi, nell'esempio di cui sopra, "citazione.pdf". La verifica della firma, inoltre, può essere fatta aprendo semplicemente il documento con il consueto software Acrobat Reader, che deve essere però impostato seguendo le indicazioni riportate di seguito.

XAdES (Xml Advanced Electronic Signatures) nasce per l'apposizione di firma digitale a documenti XML. Può essere incoroporata (embedded) o staccata (detached)

FIIF

GIURISPRUDENZA DI LEGITTIMITA' SULLE FIRME

Cass. n. 5779/2017: notifica copia digitale di atto analogico, assenza di firma su relata e su autentica procura: irrilevanza, trattandosi di copia rispetto all'originale analogico sul quale v'era la firma autografa («*non cagiona incertezza sull'identificazione della parte e del difensore*»)

Cass. n. 6518/2017: assenza firma digitale su relata di notifica («*il difetto della firma non è causa di inesistenza dell'atto - surrogabilità di quella prescrizione attraverso altri elementi capaci di far individuare l'esecutore dell'atto…*»)

FIIF

GIURISPRUDENZA DI LEGITTIMITA' SULLE FIRME

Cass. N. 18758/2017: «alcuna nullità potrebbe essere dichiarata in forza dell'efficacia sanante per raggiungimento dello scopo conseguente al deposito da parte del ricorrente di una puntuale ed articolata memoria di replica al controricorso»

Cass. n. 14338/2017: atto di appello (originale e la copia) privo della firma digitale => la firma digitale è pienamente equiparata, quanto agli effetti, alla sottoscrizione autografa => inesistente la notificazione dell'atto di gravame non solo perché la copia di esso trasmessa via PEC dal difensore dell'appellante era carente della firma digitale, ma, soprattutto, in quanto l'originale del medesimo atto ne era privo

FONDAZIONE ITALIANA PER L'INNOVAZIONE FORENSE

Consiglio Nazionale Forense
presso il Ministero della Giustizia

Grazie per l'attenzione