ANORC

TAVOLI DI LAVORO
2018/2019

FIRME E SIGILLI

COORDINATORE

Giovanni Manca

CON LA PARTECIPAZIONE DI

ARUBA PEC · ASI Agenzia Spaziale Italiana · VENETO AGRICOLTURA · CREDEM · CREDEMTEL · EURONOVATE

witness Group · HiT Internet Technologies · InfoCert Gruppo Tecnoinvestimenti · LAND · Namirial SpA

SOMMARIO

Obiettivi del documento 1

1. Introduzione 2

2. Il regolamento 910/2014 (eIDAS) 2

2.1 Identificazione ed autenticazione 2

2.2 La firma elettronica 3

2.3 Il sigillo elettronico 3

2.4 La conservazione di firme e sigilli 3

3 Identità, firme e sigilli nel CAD 4

3.1 CIE, CNS, SPID 4

3.2 Presentazione di istanze e dichiarazioni telematiche 5

3.3 Applicazione dell'art. 20, comma 1-bis 6

4 La firma elettronica avanzata (FEA) in Italia ed Europa 9

4.1 Basi normative 9

4.2 Le varie tipologie di FEA 10

4.3 La FEA basata sulla grafometria 11

4.4 La verifica della sottoscrizione grafometrica 12

4.4.1 Le strutture dati ISO/IEC 19794-7 (2014) 12

4.4.2 Non solo i dati delle firme: i dati di contesto 13

4.4.3 Verifica e conservazione digitale a norma 13

4.4.4 Lo stato dell'arte 13

5. Il sigillo elettronico qualificato 15

5.1 Fondamenti tecnici e tecnologici 15

5.2 Basi legali 18

5.3 Gli standard europei di riferimento 22

6. Scenari di utilizzo per il sigillo elettronico 23

6.1 Considerazioni sulla creazione dei sigilli 23

6.2 Conservazione digitale 23

6.3 Fatturazione elettronica 24

6.4 Protocollo e repertori informatici 29

6.5 Sanità elettronica 30

6.6 Utilizzi in scenari specifici 31

7. Scenari di utilizzo per la FEA e per la FES (Firma Elettronica Semplice) 33

7.1 Firme Elettroniche Semplici 35

7.2 Firma Elettronica Avanzata (FEA) 36
7.3 Come valutare la scelta? 36
7.4 Sanità elettronica 37
7.5 Articolo 60 del DPCM 22 febbraio 2013 39
8. Interoperabilità delle firme e dei sigilli nel regolamento eIDAS 40
9. Considerazioni finali 43
10. Bibliografia e Linkografia 44
Appendice 45
A.1 Esempi di sigillo elettronico qualificato 45
Allegato I 60
1. Riferimenti al sigillo elettronico nel regolamento eIDAS. 60

Giovanni Manca

Ingegnere, Vicepresidente di ANORC e Coordinatore Tdl "Firme e Sigilli"

Giovanni Manca, laureato in Ingegneria Elettronica, da circa 35 anni svolge attività di consulenza sulle tematiche di servizi digitali, dematerializzazione e sicurezza ICT.

Ha partecipato ai principali progetti pubblici e privati di identità digitale, sicurezza e dematerializzazione documentale con una attività anche di stesura di norme primarie e di regole tecniche.

In particolare, tra l'altro ha contribuito al progetto Tessera Sanitaria – Carta Nazionale dei Servizi (TS-CNS), alla definizione normativa e tecnica della cosiddetta firma remota, a progetti di dematerializzazione in pubbliche amministrazioni, banche e assicurazioni con particolare rilievo per la firma grafometrica e la firma elettronica avanzata.

In tempi più recenti cura lo sviluppo del procedimento digitale in supporto a importanti strutture sanitarie, del Digital Transaction Management (DTM) e dei nuovi servizi elettronici di recapito certificato stabiliti nel regolamento europeo 910/2014 (eIDAS).

In applicazione del regolamento europeo sulla protezione (679/2016 – GDPR) dei dati personali cura la progettazione e la messa in opera dei sistemi di sicurezza ICT presso alcune aziende locali.

Nell'ultimo biennio ha pubblicato oltre ottanta articoli e pubblicazioni sui temi dell'innovazione tecnologica digitale sia nazionale che europea.

Attualmente è Vicepresidente di ANORC (Associazione Nazionale per Operatori e Responsabili della Conservazione) dopo esserne stato Presidente nel biennio 2016-2018.

Svolge attività di docenza presso numerosi Master Universitari di primo e secondo livello e nell'ambito dell'alta formazione.

Obiettivi del documento

Una vignetta "storica" pubblicata nel 1993 sulla rivista "The New Yorker" e ripresa alcuni anni dopo ai tempi del primo grande sviluppo del web mostrava un cane su una sedia davanti a una scrivania con un personale computer che dice a un altro cane: "Su Internet nessuno sa che sei un cane".
Oggi con lo sviluppo dell'Intelligenza Artificiale possiamo integrare questa frase con "su Internet nessuno sa che sei un robot".
Queste affermazioni introducono il principio che nel mondo cosiddetto cibernetico l'identità ovviamente digitale costituisce la base per ogni attività, a maggior ragione se la propria identità digitale deve essere la base per conferire valore legale alle proprie attività nella rete.

In questo documento sono affrontate, a vari livelli di approfondimento, le tematiche della prova di identità rispetto alla fruizione di documenti informatici (non solo file, ma anche record e quindi anche dati in memoria fisica e logica).
Si parlerà poi della sottoscrizione informatica, del suo valore legale a livello europeo (regolamento UE 910/2014 – eIDAS) associata alla fattispecie operativa del motivo per il quale si firma un documento ovvero la funzione della sottoscrizione.
L'identità viene inquadrata in un contesto di strumenti per l'identità, come la Carta d'Identità Elettronica (CIE), la Carta Nazionale dei Servizi (CNS) e ovviamente lo SPID (Servizio Pubblico di Identità Digitale).
Con il regolamento eIDAS è stato introdotto anche il sigillo elettronico allo scopo di garantire la certezza dell'origine e l'integrità dei dati ai quali il sigillo è applicato.
Il sigillo (come vedremo) è praticamente identico alla firma dal punto di vista tecnologico ma differente sul piano giuridico. Il fatto che nel Codice dell'amministrazione digitale (Decreto legislativo 7 marzo 2005, n. 82 e successive modificazioni – CAD) non si parla di sigillo elettronico impone di fare una serie di analisi e valutazioni su questa fattispecie al fine di profilarne il valore giuridico e l'efficacia probatoria coordinandole a livello nazionale, il tutto considerando che eIDAS come regolamento europeo si pone ad un rango normativo superiore della Legislazione nazionale (nei limiti dei trattati comunitari) e del CAD in particolare.
In questo contesto si faranno anche valutazioni sulla Firma Elettronica Avanzata (FEA) e su quella Semplice (FES) cercando di individuare i contesti di utilizzo più consoni a ciascuna fattispecie di sottoscrizione.
Per completare le attività, vista anche la gioventù del sigillo elettronico saranno illustrati alcuni casi d'uso di possibile utilizzo del sigillo stesso. Nell'ambito del ciclo di vita di questa pubblicazione, alcuni casi d'uso saranno immediatamente applicabili, altri che saranno indicati come significativamente utili richiederanno un aggiornamento normativo.
Il tema dell'identità deve essere analizzato anche dal punto di vista del regolamento europeo 679/2016 sulla protezione dei dati personali (GDPR) visto che la fruizione e gestione di documenti informatici deve essere conforme anche a queste specifiche regole.
Infine, saranno indicati anche degli scenari dove l'utilizzo del sigillo elettronico risulterebbe seducente ma poi, in verità, è ampiamente fuori dai scopi o addirittura sbagliato.

1. Introduzione

L'impatto delle norme comunitarie sul sistema nazionale delle firme elettroniche è iniziato con la direttiva 99/93/CE che poi dopo qualche passaggio intermedio nel recepimento fu definitivamente collocata nel primo codice dell'amministrazione digitale (D.Lgs. 7 marzo 2005, n. 82). Questa direttiva si occupava solo di firme elettroniche e non è riuscita mai a creare un quadro comunitario trans nazionale e trans settoriale tale da far decollare il sistema digitale europeo.
Dopo alcune analisi poco incoraggianti sullo stato dell'arte in materia, la commissione europea nel giugno del 2012 presentò uno schema di regolamento che dopo gli iter normativi standard comunitari porto al definitivo regolamento europeo 910/2014 (indicato spesso anche come eIDAS (electronic IDentification Authentication and Signature).
La scelta di fare un regolamento deriva dal fatto che questo strumento normativo è di rango superiore alla normativa nazionale e quindi i recepimenti nazionali non sono più necessari e il quadro comunitario dovrebbe risultare omogeneo e coordinato.
Oltre alle firme elettroniche il regolamento stabilisce regole di principio (le norme comunitarie sono tecnologicamente neutre) per l'identificazione elettronica e i *trust services* (tradotti come servizi fiduciari) per le transazioni elettroniche nel mercato interno.
Nel prossimo capitolo, visti gli scopi del presente documento vengono sintetizzati i principali aspetti e cioè gli schemi di identificazione, le regole sulle firme elettroniche e sulla nuova fattispecie denominata sigillo elettronico per poi fornire qualche sintetica informazione sulla conservazione di firme e sigilli elettronici.
Non parleremo di validazione temporale e servizi di recapito certificato, anch'essi presenti nel regolamento eIDAS perché al di fuori degli obiettivi del presente documento.
Per chiudere questo paragrafo, comunque è utile richiamare il considerando 2 del regolamento che ne evidenzia la finalità principale, cioè fornire:
"*una base comune per interazioni elettroniche sicure fra cittadini, imprese e autorità pubbliche, in modo da migliorare l'efficacia dei servizi elettronici pubblici e privati, nonché dell'eBusiness e del commercio elettronico, nell'Unione europea*".
È utile ricordare che il regolamento eIDAS pur mantenendo la neutralità tecnologica getta le basi per i meccanismi di realizzazione dei servizi fiduciari con particolare attenzione al mutuo riconoscimento e all'interoperabilità. Con atti di esecuzione o atti delegati la Commissione stabilisce quali standard ETSI o CEN debbano essere utilizzati per gli elementi in gioco come i certificati digitali, le firme elettroniche qualificate o le certificazioni di sicurezza dei dispositivi di firma qualificata.

2. Il regolamento 910/2014 (eIDAS)

2.1 Identificazione ed autenticazione

Il regolamento eIDAS distingue tra identificazione ed autenticazione elettronica. La prima viene definita come il procedimento di utilizzo dei dati personali identificativi in forma elettronica al fine di rappresentare in modo univoco una persona fisica o giuridica, o la persona fisica che rappresenta una persona giuridica; l'autenticazione è invece definita come il processo elettronico che consente di confermare l'identificazione elettronica di una persona fisica o giuridica, o l'origine e l'integrità dei dati in forma elettronica.

In questo scenario l'Italia ha scelto di notificare alla Commissione il Sistema Pubblico di Identità Digitale (SPID) e questa notifica, superate con successo le attività di analisi della Commissione stessa e degli Stati membri è stata pubblicata nella Gazzetta comunitaria e quindi entro il settembre 2019 (un anno dopo la pubblicazione) SPID potrà essere utilizzato anche per l'identificazione in rete ai fini dell'accesso ai servizi pubblici nel mercato interno.
A gennaio 2019 è iniziato il procedimento di notifica per la Carta d'Identità Elettronica che si dovrebbe concludere entro maggio 2019.

2.2 La firma elettronica

Come già detto la direttiva 99/93/CE si occupava solo di firme elettroniche e negli anni ha creato una serie di situazioni nazionali ben consolidate. In questo senso il regolamento eiDAS non introduce significative modifiche rispetto al quadro normativo previgente. Ci sono piccole variazioni nella definizione di firma elettronica che non è più uno strumento di identificazione come stabilito nella direttiva, vista la presenza di specifiche regole per l'identificazione in rete.
Viene confermata la neutralità tecnologica della firma elettronica avanzata (che pur avendo lo stesso nome ha efficacia giuridica diversa da quella italiana come stabilito nel CAD). Nulla cambia per la firma elettronica qualificata che è equivalente ad una sottoscrizione autografa. È l'ordinamento nazionale del singolo Stato membro a stabilire il valore della firma autografa per esempio nella forma scritta. Il regolamento eIDAS introduce il sigillo elettronico che rappresenta forte analogia con la firma elettronica ma che indubbiamente è una nuova fattispecie.

2.3 Il sigillo elettronico

Il regolamento eIDAS definisce il sigillo elettronico come un insieme di dati in forma elettronica acclusi, o connessi tramite associazione logica, ad altri dati in forma elettronica, per garantirne la provenienza e l'integrità. Appare evidente che viene introdotta una fattispecie giuridica che garantisce l'integrità del documento, anche quando è senza firma. L'analisi affrettata del sigillo lo potrebbe far considerare come la sottoscrizione di una persona giuridica; questo non è scontato e dipende dagli ordinamenti nazionali. Per esempio, in Italia nulla dice la normativa nazionale sul sigillo ma la sottoscrizione della persona giuridica non è esplicitamente nel nostro ordinamento.
A titolo esemplificativo in appendice sono mostrati tre esempi di *dump* in formato ASN.1 di certificati qualificati per il sigillo elettronico in cui la chiave privata risiede in un dispositivo per la creazione di un sigillo elettronico qualificato.

2.4 La conservazione di firme e sigilli

La conservazione di firma e sigilli è stabilita in modo estremamente sintetico negli articoli 34 e 40 del regolamento eIDAS. Il regolamento parla di fattispecie qualificate e l'obiettivo è quello di estendere l'affidabilità della firma (e del sigillo) elettronica qualificata oltre il periodo di validità tecnologica. Quindi questa conservazione è differente da quella digitale che è ben nota e ampiamente attuata in Italia per la conservazione digitale di documenti informatici. Differenti sono gli obiettivi e quindi differenti sono i percorsi tecnologici realizzativi.

3 Identità, firme e sigilli nel CAD

3.1 CIE, CNS, SPID

L'identità digitale è definita nel Codice dell'Amministrazione Digitale all'art. 1 come "*la rappresentazione informatica della corrispondenza tra un utente e i suoi attributi identificativi, verificata attraverso l'insieme dei dati raccolti e registrati in forma digitale secondo le modalità fissate nel decreto attuativo dell'articolo 64*". A sua volta, il novellato art. 64 regola aspetti strettamente legati al Sistema Pubblico di Identità Digitale (SPID), riducendo – a prima vista – il tema dell'identità digitale all'ambito dei rapporti con la pubblica amministrazione. Questa interpretazione è avvalorata dalla necessità sentita dal legislatore di specificare, al comma 2-quinques dell'articolo in discorso, che SPID può essere utilizzato – secondo modalità dettate da apposito Decreto – anche da "*soggetti privati*".

Come noto, il sistema SPID è un insieme aperto di soggetti pubblici e privati che identificano gli utenti per garantire un accesso sicuro ai servizi in rete: il modello architetturale e l'accreditamento sono delineate dal DPCM 24 ottobre 2014. Inoltre, nel 2017 AgID ha definito le regole, tecniche, formali ed economiche con cui i *service provider* privati possono entrare a far parte del sistema SPID.

Nel contesto nazionale, quindi, l'identità digitale è oggi descritta come un sistema di autenticazione verso i servizi della Pubblica Amministrazione e/o dei soggetti privati: lo strumento di autenticazione può essere l'identità SPID oppure – per quanto dettato dal comma 2-nonies – uno a scelta tra la Carta Nazionale dei Servizi (CNS) e la Carta d'Identità Elettronica (CIE). Tuttavia, questi strumenti, sin dalla novella del 2016, hanno perso gran parte del loro fascino verso il legislatore, che ha fatto della normativa di settore un volano per il solo SPID.

Ulteriore indizio del favore di cui gode SPID è rappresentato dal fatto che si tratta del primo strumento di *e-identification* notificato ai sensi dell'art. 9 del Regolamento eIDAS: mentre altri Stati Membri hanno notificato documenti d'identità per così dire tradizionali (si veda ad esempio la Germania con la propria carta d'identità elettronica), l'Italia ha mostrato un certo spirito innovativo nel promuovere uno strumento identificativo completamente digitale.

La preponderanza di SPID era rafforzata dal comma – oggi abrogato – 2-septies dell'articolo in discorso che prevedeva: come "*un atto giuridico può essere attuato da un soggetto identificato mediante SPID, nell'ambito di un sistema informatico avente i requisiti fissati nelle regole tecniche adottate ai sensi dell'articolo 71, attraverso processi idonei a garantire, in maniera manifesta e inequivoca, l'acquisizione della sua volontà. 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*". Il legislatore aveva previsto una modalità di sottoscrizione in cui l'uso identificativo di SPID sosteneva un processo di firma composito, oggi – forse – confluito nell'art. 20 comma 1-bis.

3.2 Presentazione di istanze e dichiarazioni telematiche

All'art. 65 del CAD il legislatore ha previsto nel dettaglio le modalità telematiche con cui presentare validamente le istanze e dichiarazione ai sensi dell'articolo 38, commi 1 e 3, del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445. L'articolo risulta assolutamente opportuno in un contesto che tende alla digitalizzazione della Pubblica Amministrazione e pone come priorità il *digital first* nei rapporti con lo Stato.

La forma delle istanze, come prevista dal primo comma dell'articolo in discorso, è di vario tipo e cerca – con mezzi digitali e ibridi – di andare incontro alla necessità di rendere agile e comunque legittima la comunicazione verso la PA, non solo di quei soggetti già avvezzi al digitale e quindi muniti degli strumenti informatici adeguati, ma anche di tutti quei Cittadini che ancora non hanno abbracciato completamente la dematerializzazione.

Le istanze e dichiarazioni sono validamente presentate alla Pubblica Amministrazione se:

a) "*Sottoscritte mediante una delle forme di cui all'art. 20*": al netto della complessità sistematica di questa norma (ampiamente discussa nel paragrafo successivo), in questo caso il Cittadino che abbia una firma Qualificata, Digitale, Avanzata o "Ibrida" potrà validamente sottoscrivere l'istanza e presentarla con lo strumento elettronico che più preferisce;

b) "*l'istante o il dichiarante è identificato attraverso il sistema pubblico di identità digitale (SPID), nonché attraverso uno degli altri strumenti di cui all'art. 64 comma 2-novies, nei limiti ivi previsti*". In questo caso, la validità dell'istanza non verte sulla sua corretta sottoscrizione (o integrità) ma sull'identificazione del soggetto, che deve avvenire con SPID, con la CIE o con la CNS;

c) "*sottoscritte e presentate unitamente alla copia del documento d'identità*". Limitando l'applicabilità del comma al contesto informatico, ed escludendo una sottoscrizione elettronica "forte" già prevista dalla lettera a), si potrebbe desumere che qui la validità dell'istanza verte sulla sua presentazione: sottoscritta, con firma elettronica semplice o con firma autografa, e poi presentata, con il mezzo preferito dal Cittadino, unitamente a copia (informatica) del documento d'identità;

d) "*trasmesse dall'istante o dal dichiarante dal proprio domicilio digitale purché le relative credenziali di accesso siano state rilasciate previa identificazione del titolare, anche per via telematica secondo modalità definite con Linee guida, e ciò sia attestato dal gestore del sistema nel messaggio o in un suo allegato. In tal caso, la trasmissione costituisce elezione di domicilio speciale ai sensi dell'articolo 47 del Codice civile. Sono fatte salve le disposizioni normative che prevedono l'uso di specifici sistemi di trasmissione telematica nel settore tributario*". In questa previsione, prima della novella del 2017, riviveva la Posta Elettronica Certificata identificata (c.d. "PEC-ID"): ad oggi, invece, questa lettera sembra essere l'unica previsione in cui il Cittadino possa eleggere domicilio digitale, sempre che – appunto – la PEC da cui invia i propri messaggi rispetti le regole sulla PEC-ID.

Le istanze così presentate hanno – verso la PA – un altissimo valore giuridico e probatorio in quanto a norma del successivo comma 2: "*sono equivalenti alle istanze e alle dichiarazioni sottoscritte con firma autografa apposta in presenza del dipendente addetto al procedimento*".
Considerata l'eterogeneità della ratio di ciascun processo di invio e presentazione delle istanze, sarebbe utile, sia per l'Interprete che per il Cittadino, mantenere una linea unitaria sulle esigenze che stanno alla base della validità delle istanze: le quattro lettere brevemente analizzate, invece, sembrano contenere quattro ratio diverse. Da quanto esposto, gli sforzi del legislatore si potrebbero concentrare su due aspetti cardine e fondamentali: da una parte la certezza di provenienza e integrità dell'istanza, dall'altra della sicurezza del mezzo elettronico di invio e ricezione. Entrambi i criteri possono facilmente essere soddisfatti con strumenti conosciuti: firme elettroniche qualificate, Posta Elettronica Certificata e quando operativi i Servizi Elettronici di Recapito Certificato di natura postale.

3.3 Applicazione dell'art. 20, comma 1-bis

L'articolo 20 è stato fortemente innovato dall'ultima novella del Codice. In particolare, l'intervento legislativo ne ha modificato la rubrica, da semplice "*documento informatico*" in "*validità ed efficacia probatoria dei documenti informatici*" lasciando presagire un maggiore dettaglio normativo sulla formazione e validità del documento elettronico: infatti, si è assistito a un'inversione della centralità regolatoria rispetto al passato, che vedeva preponderante il successivo art. 21.
Per comprendere l'applicazione della norma in analisi è necessario premettere alcuni ragionamenti volti a individuarne scopo e perimetro di usabilità. Non è chiaro, infatti, se l'art. 20 faccia oggi riferimento a strumenti di *firma* ovvero a strumenti di *formazione* del documento informatico.
Se ci si attiene a un'interpretazione strettamente letterale, la rubrica dell'art. 20 è chiara nel circoscrivere l'operatività della norma alla "*validità ed efficacia probatoria dei documenti informatici*": a prima vista, quindi, è chiaro che gli strumenti di cui all'art. 20 servono all'utente a *formare* i documenti. Tuttavia, l'articolo in discorso descrive, al comma 1-bis, una serie di strumenti elettronici utilizzati per sottoscrivere (Firma Elettronica Qualificata, Digitale e Avanzata), sostituendo il ruolo definitorio che sino alla novella del 2017 era riservato al successivo art. 21.
Le incertezze aumentano se si allarga la visione interpretativa scegliendo un approccio sistematico: per esempio, l'art. 65 sopra brevemente commentato alla lettera a) del suo primo comma parla di istanze valide se "*sottoscritte mediante una delle forme di cui all'articolo 20*". L'interprete e soprattutto l'utente non possono che essere gettati nello sconforto nel non avere certezza se il processo elettronico che stanno seguendo porti alla *formazione* ovvero alla *firma* di un documento. La confusione di scopo è alimentata anche dallo stesso art. 21, che al comma 2-bis affianca strumenti di *sottoscrizione* a strumenti di *formazione*: i documenti elettronici hanno forma scritta se sono *sottoscritti* con un tipo di firma sicura (qualificata, digitale o avanzata) ovvero se sono *formati* "*a norma dall'art. 20, comma 1-bis, primo periodo"*. Nel tentativo di riconoscere rango di forma scritta al documento informatico – forse nel rispetto dell'art. 46 eIDAS[1] – si rischia di creare disallineamento sugli strumenti informatici posti alla base delle transazioni giuridiche digitali.

[1] A norma del quale: "*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*".

Del resto, la formazione di un documento non è la sua sottoscrizione: la firma elettronica è chiaramente definita in eIDAS come lo strumento che il firmatario usa per *firmare* il documento e non *formarlo*.
Da queste considerazioni deriva che l'applicazione dell'art. 20 comma 1-bis risulta già complessa nel momento stesso della sua genesi.
Dovendo individuare dei casi di applicazione dell'articolo in oggetto, occorre a fronte di quanto appena detto, differenziare:

a) Nel caso in cui si ritenga che il documento generato a norma dell'art. 20 comma 1-bis sia semplicemente *formato*, si potrebbe salvare l'utilità dell'articolo riconducendone l'applicabilità a un valore strettamente probatorio, e cioè quello previsto dall'art. 2702 del Codice Civile. Tuttavia, questa ricostruzione non convince: basterebbe, infatti, leggere il Codice Civile per rendersi conto che la norma – nel riportare l'efficacia probatoria del documento – si riferisce alle "*dichiarazioni di chi l'ha sottoscritto*". È chiaro, quindi, che risulta complesso sostenere – a meno di non limitarsi a leggere il solo CAD – l'utilità sistematica di interpretare l'art. 20 in discorso come una modalità di *formazione* del documento elettronico.
b) Sembra, invece, più corretto ritenere che l'art. 20 in oggetto descriva un quinto tipo di firma per così dire "ibrido": in questo caso l'ambito applicativo risulta molto più chiaro. Una soluzione in cui il documento "*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*", infatti, potrà rispondere a quei processi di sottoscrizione che non richiedono l'uso di una Firma Elettronica Qualificata (o Digitale) né di una Firma Elettronica Avanzata (ancora imbrigliata nelle maglie del DPCM 22 febbraio 2013). All'interprete europeo non resterà che capire come mai a livello nazionale esisteranno cinque tipi di firma elettronica, quando il regolamento eIDAS ne prevede già tre che soddisfano le diverse esigenze di certezza giuridica e tecnologica.

In definitiva, l'articolo in discorso sembra prevedere un quinto tipo di firma, tecnologicamente vincolato dalle specifiche Linee Guida di AgID. La confusione che questo approccio potrebbe portare sul mercato europeo è – forse – bilanciata dalla possibilità di sfruttare (al netto di quanto verrà previsto dalle Linee Guida de qua) strumenti identificativi innovati che esulino da quanto previsto oggi dal DPCM 22 febbraio 2013 in tema di identificazione del firmatario. Strumenti nativi digitali, come SPID, o ibridi, come la CIE e il CNS, potrebbero essere utilizzati per risolvere uno dei quattro scopi (quello identificavo appunto) della firma: in questo contesto, l'Identity provider SPID si ritroverebbe a ricoprire un ruolo fondamentale nel riconoscimento del firmatario, lasciando al service provider l'onere di costruire un processo di firma sicuro e rispettoso del CAD.
In ogni scenario, comunque, ipotizzando che l'autore sia stato identificato mediante SPID e tramite questo acceda con la sua identità in un sistema informatico dove produce la forma e il contenuto del documento informatico, a doverosa copertura dei principali scopi della firma (dichiarativo e probatorio) e applicando le specifiche Linee Guida AgID, il procedimento in questione dovrebbe garantire piena paternità del contenuto del documento e la riconducibilità all'autore. Del resto,

proprio su quest'ultimo tema, la definizione e costruzione del processo è resa sfidante dallo stesso CAD, con previsioni atte ad assicurarne efficacia e forma "manifesta ed inequivoca".
A fronte di tale condivisibile intento difficilmente ci si potrà esimere dal porsi come obiettivo la formazione di un documento informatico di per sé "parlante" e auto consistente. Inoltre, è necessario evitare qualsiasi rischio che conduca alla costituzione di processi di firma che, già irrigiditi dalla laboriosità della loro genesi e probabilmente confinati in ambiti limitati (unicità dell'autore - sottoscrittore), risultino anche prevedibilmente chiusi (mancanza di interoperabilità).
Tutti temi importanti e a volte antitetici, come quelli della sicurezza, della semplicità e della diffusione di un servizio, che portano a pensare a un auspicabile coinvolgimento, esteso e centrale, dell'Identity provider, anche in qualità di soggetto *super partes*, nel governo del processo e nell'assicurazione dei suoi intenti.
Comunque, in ogni scenario, si avrebbe certamente maggiore chiarezza, soprattutto a livello Europeo, se la normativa nazionale si limitasse a descrivere il valore giuridico e probatorio delle soluzioni di firma già previste da eIDAS, in modo da permettere lo sviluppo dei rapporti digitali da e per il territorio nazionale, senza creare ghetti in cui vigono previste soluzioni di firma nazionali e inaccessibili ai Cittadini europei.

4 La firma elettronica avanzata (FEA) in Italia ed Europa

4.1 Basi normative

Da un punto di vista strettamente normativo, la Firma Elettronica Avanzata è oggi definita dal combinato disposto degli artt. 3 numero 11) e 26 dal Regolamento eIDAS come la firma elettronica (semplice) che sia:

a) connessa unicamente al firmatario;

b) idonea a identificare il firmatario;

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

A fronte di una definizione unitaria[2] esistono tuttavia regole implementative differenti. Se da una parte a livello europeo le soluzioni di FEA sono tecnologicamente neutre, richiedendo solo il soddisfacimento dei criteri sopra enunciati, a livello nazionale vige ancora il DPCM 22 febbraio 2013 che analiticamente regola il processo di formazione della firma in discorso.

Il titolo V del DPCM, oltre a richiamare i principi sopra elencati, detta alcune norme che non trovano corrispondenza nel Regolamento europeo. Un primo aspetto peculiare delle regole tecniche nazionali è la previsione di due diversi soggetti nella costruzione di soluzioni di FEA: un soggetto Realizzatore, che concretamente disegna e mette a disposizione la soluzione tecnica, e un soggetto Erogatore, che utilizza concretamente la soluzione di FEA nei rapporti con le proprie controparti. Comunque, bisogna tenere in conto che la FEA in eIDAS e quella nel nostro ordinamento tecnico sono differenti in termini di efficacia probatoria e efficacia giuridica e quindi trovare analogie tra le due fattispecie non è corretto.

È utile rilevare come l'onere di conservazione previsto dall'art. 57 possa risultare eccessivo, soprattutto a fronte degli oneri di minimizzazione imposti dal nuovo Regolamento sulla protezione dei dati personali (GDPR), l'onere di conservare copia del documento per 20 anni dalla sottoscrizione: sarebbe più coerente prevedere un obbligo di conservazione scaglionato, sulla base della prescrizione prevista per gli atti in concreto sottoscritti.

Il valore giuridico e probatorio delle FEA è, in linea con eIDAS, regolamentato a livello nazionale: il CAD, agli artt. 20-21, riconosce un rango elevato alla Firma Avanzata, in quanto

a) Può essere utilizzata per sottoscrivere tutti gli atti che ex art. 1350 n.13 del Codice Civile richiedono forma scritta (*ad substantiam*) a pena di nullità dello stesso.
b) Ha il valore probatorio di cui all'art. 2702 nell'ambito del soddisfacimento della forma scritta (*ad probationem*) e fa piena prova fino a querela di falso delle dichiarazioni sottoscritte.

[2] Il CAD richiama espressamente quanto disposto dal Regolamento eIDAS: "*Ai fini del presente Codice, valgono le definizioni di cui all'articolo 3 del Regolamento eIDAS*" (Cfr. art. 1 comma 1-bis CAD).

4.2 Le varie tipologie di FEA

In generale, la FEA gode di grande libertà, sempre che si rispettino i 4 criteri elencati al paragrafo precedente: un processo che permetta di garantire paternità della firma e integrità di quanto sottoscritto rientra, almeno per quanto disposto dal Regolamento eIDAS, nell'alveo della FEA. A livello nazionale, invece, sarà necessario seguire quanto dettato dall'art. 56 del DPCM 22 febbraio 2013 e l'identificazione dovrà essere fatta a norma dell'art. 57 dello stesso provvedimento: con un documento d'identità in corso di validità.

Nonostante questa libertà di forme, la Firma Elettronica Avanzata oggi ha due principali accezioni: una grafometrica e una basata su un certificato elettronico avanzato per firme elettroniche.

La firma grafometrica verrà analizzata nel paragrafo che segue, mentre per quanto riguarda la firma basata su certificato si può dire che sia una soluzione tecnologica che sfrutta i certificati di firma senza però raggiungere il livello di Firma Elettronica Qualificata (QES). Questo approccio da una parte permette di superare i vincoli normativi e tecnici di un servizio Qualificato, ma dall'altra erode il valore giuridico e probatorio della firma stessa, che non è più *de jure* riconosciuta in tutti e 28 gli Stati Membri e soprattutto non è equiparata – a livello europeo – alla firma autografa. Al netto di queste differenze, la FEA può basarsi su:

a) Certificati elettronici non qualificati
b) Certificati elettronici qualificati ma creata da un dispositivo per la creazione di una firma elettronica non qualificata

In entrambi i casi il firmatario sarà titolare di un certificato di firma che – tecnologicamente e giuridicamente – permette di ricondurre quel particolare documento al suo titolare. Da un punto di vista di usabilità, invece, il processo di firma dipenderà dalle scelte intraprese dall'Erogatore in accordo con il Realizzatore, se presente. La flessibilità tecnologica della FEA, infatti, permette di costruire esperienze di firme diversificate, basandosi di volta in volta sugli strumenti adeguati all'esigenza del mercato e agli strumenti tecnologici in possesso del firmatario. Non si esclude, quindi, che si possa avere una FEA remota, al pari della Firma Elettronica Qualificata remota, magari gestita da APP.

4.3 La FEA basata sulla grafometria

Come noto, la firma grafometrica è un particolare tipo di firma che prevede l'apposizione di un tratto grafico su un apposito tablet che è in grado di raccogliere le informazioni biometriche della firma e di allegarle logicamente al documento elettronico. In particolare, la firma grafometrica richiama l'operatività di una firma autografa, in quanto il tratto viene vergato manualmente, con il vantaggio di conservare anche le preziose informazioni[3] che permettono di ricondurre al firmatario la sottoscrizione, tra gli altri[4]:

1) Forma del tratto
2) Pressione del tratto
3) Posizione della sottoscrizione
4) Tempo del tratto
5) Elementi in volo
6) Pressione zero (sperimentalmente si rileva che il passaggio "soffice" ovvero senza premere della penna sulla superficie del dispositivo di scrittura viene rilevato come pressione zero).

La presenza di un hardware specifico, alimentato da apposito software, permette la raccolta, conservazione ed esibizione, quando necessario, delle prove che costituiscono la firma e della sua riconducibilità univoca all'autore.

In merito alla realizzazione di firme elettroniche di tipo grafometrico, si cita il GDL 001-2014 di AIFAG, in cui sono stati analizzati gli aspetti tecnici di realizzazione di tali firme. Anche da quello studio, è emerso che per raggiungere l'interoperabilità è opportuno utilizzare la standardizzazione perla costruzione del pacchetto di firma definendone eventualmente, uno o più profili. A tal scopo, è stato avviato un successivo GDL AIFAG, di cui si parlerà nel dettaglio in seguito.

Questo particolare tipo di firma ha il grosso vantaggio di rendere meno brusca la transazione dal mondo cartaceo a quello elettronico: l'esperienza di firma per l'utente è molto simile a quella della firma autografa e il suo valore giuridico e probatorio è relativamente alto. Infatti, seppur non assuma il massimo valore giuridico e probatorio tipico della Firma Qualificata, questa soluzione di firma rientra nell'alveo della FEA, garantendo la possibilità di sottoscrivere atti che richiedono – ex art. 1350 n. 13 del Codice Civile – forma scritta a pena di nullità e godendo della piena efficacia probatoria della scrittura privata ex art. 2702 Codice Civile.

La firma grafometrica ha esercitato grande fascino in tutte le esperienze di firma elettronica che richiedono la presenza fisica del firmatario, come ad esempio la firma di documentazione a uno sportello. Tuttavia, oltre alle obbligazioni di cui al DPCM 22 febbraio 2013 più volte citato, la soluzione di firma grafometrica deve:

1) Rispettare i vincoli imposti dalle norme sulla protezione dei dati personali (regolamento europeo GDPR e coordinamento nazionale con la il decreto 101/2018) seguendo le regole del Provvedimento generale prescrittivo in tema di biometria del 12 novembre 2014 del Garante privacy nazionale.

[3] Sull'uso dei dati biometrici a questo scopo si veda il "Provvedimento generale prescrittivo in tema di biometria" del 12 novembre 2014 come successivamente rettificato il 15 gennaio 2015.
[4] Per un'analisi estesa delle soluzioni tecnologiche si veda anche: "Buone prassi per l'analisi forense di firme grafometriche – AGI – AIFAG"

2) Prevedere la figura di una terza parte fidata, che mantenga parte del controllo sulla chiave privata usata per cifrare i dati biometrici del firmatario, che possono essere accessibili solo nei casi di procedure giudiziarie

4.4 La verifica della sottoscrizione grafometrica

Nel luglio del 2016 si scriveva dei risultati del Gruppo di lavoro AIFAG (Associazione Italiana Firma elettronica avanzata biometrica e Grafometrica) presentati il 24 giugno 2016 a Lecce nell'ambito del convegno AIFAG denominato "FEA, biometria, privacy e compliance: il nuovo scenario europeo**".**
In quel contesto furono presentati i risultati dei test di interoperabilità sulla firma grafometrica coordinati dal Prof. Giuseppe Pirlo dell'Università di Bari.
Nel seguito riprendiamo il tema fornendo al lettore gli aggiornamenti sullo stato dell'arte in materia di sicurezza, interoperabilità e periziabilità della firma grafometrica.
Per riprendere il tema ricordiamo come si verifica una firma grafometrica.

Il sottoscrittore firma il documento (nella quasi totalità dei casi pratici un documento in formato PDF) utilizzando uno stilo attivo o passivo (attivo: alimentato, passivo: non alimentato) su un dispositivo in grado di raccogliere il tratto della sottoscrizione e, in maniera protetta, di connetterlo in modo indissolubile a quanto si vuole sottoscrivere.
Le strutture dati della firma grafometrica prodotte dalle varie soluzioni, in assenza di un protocollo standard, sono diverse per ogni fornitore. Di conseguenza queste strutture sono leggibili solo dallo strumento di analisi grafologica dello stesso fornitore. Per semplificare il lavoro degli esperti forensi è risultato molto utile disporre di strutture dati omogenee prodotte su un tracciato standard per i dati grafometrici, che in tal modo possono essere analizzati da un qualsiasi strumento di analisi in grado di elaborare questo tracciato previa conversione.
Naturalmente devono essere applicate le regole stabilite nel Provvedimento prescrittivo del Garante per la protezione dei dati personali (n. 513/2014) che impone di rendere disponibili i dati biometrici solo su richiesta dell'Autorità Giudiziaria quando si è in presenza di un contenzioso.
Nel cennato Provvedimento sono fornite le Regole di protezione del dato biometrico e le indicazioni organizzative per un suo trattamento rispettoso della privacy.
Una volta che il dato è estratto dal suo ambiente protetto, questo deve essere possibile l'elaborazione in modo "interoperabile" da parte dello strumento in uso al perito grafologo.

4.4.1 Le strutture dati ISO/IEC 19794-7 (2014)

È indispensabile generare i dati in un formato standard; a questo scopo è indispensabile produrre i dati biometrici in formato ISO/IEC 19794-7 (2014). Questo è lo standard di riferimento sul tema.
Nel citato standard vengono stabilite le strutture dati e la rappresentazione dei parametri biometrici che caratterizzano la sottoscrizione grafometrica.
Per esempio, le coordinate cartesiane X e Y del tratto grafico, il tempo di acquisizione della coordinata e la differenza di tempo calcolata sulla base della frequenza di campionamento del dispositivo di acquisizione dati. Tutti questi dati sono rappresentabili in un modo standard secondo un tracciato record e la rappresentazione dei dati definita in ISO/IEC 19785-1.
Altri dati sono utili per l'analisi in un giudizio anche se non contemplati nello standard ISO/IEC 19794-7:2014. Tra questi l'informazione sui dispositivi utilizzati per la sottoscrizione e l'acquisizione del dato, da memorizzare utilizzando i due campi liberi presenti nel tracciato e

inserendo le info su VendorID e ProductID (se resi disponibili dall'hardware), che identificano in maniera univoca nel mondo il dispositivo elettronico. Questo potrebbe essere utile, ad esempio, per determinare la calibrazione della pressione per un dispositivo che ne consente l'acquisizione, e per scalare le dimensioni.

4.4.2 Non solo i dati delle firme: i dati di contesto

Dal succitato GDL 001-2014 è emerso che oltre ai dati del gesto di firma letti e prodotti dalle tavolette e penne elettroniche, vi è la possibilità di salvare anche i cosiddetti dati di contesto. Questi, in caso di contenzioso, potrebbero costituire una fonte di ulteriori dati e informazioni in quanto possono rafforzare la tesi di una o dell'altra parte. Oltre ai succitati VendorID e ProductID dei device utilizzati per la raccolta della firma, vi potrebbero trovare spazio anche i dati del computer su cui la firma è stata elaborata, l'utente del sistema operativo del computer, e ove disponibili o utili al contesto, anche le coordinate GPS del luogo di raccolta della firma, oltre a informazioni del gestionale o ERP cui la soluzione di firma è collegata. Il tutto nella libera valutazione dei soggetti preposti alla FEA come individuati nel DPCM 22 febbraio 2013.

In merito alla raccolta, memorizzazione e rappresentazione di questi dati, ad oggi non sono ancora stati fatti studi concreti e completi, ma certamente si potrebbero utilizzare i dati ISO completati con altri dati facoltativi definiti dal proponente la soluzione di FEA nella documentazione di supporto elaborata ai sensi dell'articolo 57, comma 1, lettere e) ed f) del DPCM 22 febbraio 2013.

4.4.3 Verifica e conservazione digitale a norma

Non sempre è evidente alle aziende e professionisti che trasformano i propri processi in digitale, il fatto che i documenti elettronici ottenuti con un processo di firma elettronica, necessitano di un adeguato sistema di conservazione degli stessi. A maggior ragione questo è vero, per la raccolta delle firme FEA di tipo grafometrico che sono per loro natura dei processi e quindi un sistema di conservazione digitale a norma dei documenti, e non una generica cartella memorizzata risulta indispensabile anche per supportare adeguatamente procedure di verifica della firma.

4.4.4 Lo stato dell'arte

Il documento del GDL AIFAG 001-2014 abbinato a quello sull'interoperabilità del GDL AIFAG 001-2016/2017 e lo standard ISO, costituiscono senza dubbio una buona base per poter definire un profilo o delle regole di standardizzazione della costruzione del pacchetto di firma grafometrica da apporre sui documenti e delle procedure necessarie per la corretta implementazione dei processi nella sua interezza.
Altri eventi si sono verificati negli ultimi mesi, che migliorano lo scenario che si sta analizzando in questa sede. La sicurezza dei sistemi grafometrici è rimasta stabile con alcune punte di eccellenza. La certificazione dei sistemi ai sensi dei Common Criteria (standard di riferimento per la sicurezza di questo tipo di hardware e software) non è mai decollata per la mancanza di domanda sul tema. Le aziende investono se ci sono obblighi di legge o specifica domanda del mercato e non c'è né l'una, né l'altra cosa.

Molto importante è la pubblicazione da parte degli esperti di AGI (Associazione Grafologica Italiana) del documento "Le buone prassi per l'analisi forense di firme grafometriche" dove si danno fondamentali indicazioni ai periti grafologi per la conduzione professionale della perizia grafologica in ambiente grafometrico. Da tale studio emerge in particolare una forte e reale esigenza di protezione del dato della firma anche durante le operazioni della perizia da parte del grafologo ed anche una necessità di mappare i dati del gesto, rappresentati in formato elettronico, su misurazioni di parametri nati dall'analisi di firme apposte su supporto analogico (carta e penna).
Sul piano dell'interoperabilità, il documento potrebbe essere ampliato ed esteso, probabilmente al di fuori delle competenze di AGI, comprendendo anche le operazioni a monte del processo di verifica del grafologo, ovvero l'estrazione delle firme dal documento e la loro verifica in termini di collegamento allo stesso, nonché l'estrazione ed analisi dei dati di contesto. Alla data queste sono affidate al terzo fidato ed al tool di verifica di ciascun vendor.
Proseguendo quanto detto in precedenza, lo stato dell'arte del mercato su questo tema potrebbe essere adeguato, se a livello normativo ci fosse l'obbligo di rappresentazione standard (anche tramite l'utilizzo di una conversione standard) delle sottoscrizioni "in chiaro".
Per raggiungere questo obiettivo i tempi sono maturi.
AIFAG ha aggregato le varie professionalità, indispensabili per raggiungere l'obiettivo. In testa le aziende produttrici, poi i grafologi, esperti del Notariato e anche le istituzioni con il coinvolgimento di AgID (l'Agenzia per l'Italia Digitale).
L'ultimo sforzo può concretizzarsi con un gruppo di lavoro coordinato da AgID per la scrittura delle Linee guida previste nell'articolo 61, comma 6 delle Regole tecniche sulle sottoscrizioni informatiche, DPCM 22 febbraio 2013.

6. (…), al fine di favorire la realizzazione di soluzioni di firma elettronica avanzata, l'Agenzia elabora Linee guida sulla base delle quali realizzare soluzioni di firma elettronica avanzata conformi alle presenti regole tecniche.

In tali Linee guida si possono indicare metodi "legali" per decifrare i dati biometrici della firma, per la verifica della stessa a prescindere dallo strumento impiegato per crearla ed a quello grafotecnico che utilizzerà il perito (oggi l'interoperabilità è puramente teorica) con una visione comune di istituzioni, aziende ed esperti.
Queste linee guida potrebbero anche indicare buone prassi nella rappresentazione della firma "a vista". In numerosi casi (Es. l'acquisto di una SIM card) la firma riportata sul documento viene deformata e rimpicciolita su iniziativa di chi gestisce l'applicativo, rendendo complessa la perizia attivata per scopi giudiziari (se si dispone dei dati biometrici è possibile lo *zoom*).
Sarebbe utile l'emanazione di regole comuni per i formati dei dati grafometrici al fine di consentirne un'analisi forense con collegata esclusivamente allo strumento di verifica del fornitore (che elabora esclusivamente i dati elaborati dal suo prodotto).
Questa attività dovrebbe essere supportata dal mercato attraverso lo sviluppo di una proposta ad AgID di Linee Guida sulla FEA, peraltro previste nell'articolo 61, comma 6 del DPCM 22 febbraio 2013.
Una volta stabilite le regole per l'interoperabilità i limiti stabiliti nell'articolo 60 del DPCM 22 febbraio 2013 possono essere eliminati venendo meno il rapporto diretto tra meccanismi tecnologici di generazione della firma e strumento di verifica non più legato a questi ultimi.

5. Il sigillo elettronico qualificato

I sigilli elettronici sono uno dei servizi fiduciari trattati da eIDAS (regolamento UE 2014/910).

La digitalizzazione dei processi con il passaggio da una gestione analogica ad una gestione digitale ha aperto nuove opportunità di business.

Tuttavia, l'economia digitale non è senza preoccupazioni, in particolare per quelle situazioni in cui occorre sapere con chi hai a che fare (identificazione), chi è autorizzato ad accedere ed a quali informazioni (diritti), e come saranno individuate le persone responsabili per i loro impegni online (responsabilità digitale).

Ad oggi, le firme digitali su modello PKI sono ampiamente riconosciute come la migliore pratica per garantire responsabilità digitale per le transazioni. La firma digitale, ed in particolare la tecnologia che ne è alla base, ha quindi un ruolo chiave quale strumento di abilitazione nell'e-business.

Tale tecnologia può essere utilizzata per avere dei vantaggi che si coniugano agli aspetti normativi che ad essa fanno riferimento, ovvero alle sue differenti declinazioni: firme elettroniche qualificate/digitali; sigilli elettronici qualificati.

Nei successivi paragrafi si cercherà di esplicitare il significato del sigillo elettronico, con particolare riferimento a quello qualificato, mettendolo in relazione sia alla firma digitale che alla firma autografa al fine di risalire alla razionalità della sua introduzione nella legislazione comunitaria prima ancora che in quella italiana, ovvero all'utilità del suo impiego.

5.1 Fondamenti tecnici e tecnologici

Abbiamo tutti una elevata dimestichezza con le firme autografe su carta.
A parte questioni legali e contrattuali, le principali caratteristiche di una firma autografa sono:

- essere associata ad un individuo particolare;
- indicare generalmente un impegno relativo a un particolare documento, con il significato esatto che dipende dal contesto.

Sebbene lontane dalla perfezione, le firme cartacee sono state e sono ancora la base di molte transazioni commerciali e legali.
Questo non è dovuto alle caratteristiche intrinseche delle firme autografe, ma piuttosto ai processi di accompagnamento: contratti supplementari e contesto circostante all'atto della firma (testimonianze, cerimonie pubbliche, presenza di un pubblico ufficiale) che possono essere elementi utili per risolvere eventuali controversie, qualora dovessero emergere.
Le firme cartacee sono di per sé relativamente significative: ad esempio, quando in certi casi in cui una "X" apposta alla presenza di un testimone era riconosciuta come valida. Se estratta attraverso la coercizione, l'inganno o la falsificazione, quasi tutte le società considerano una firma autografa apposta su un documento, legalmente non vincolante. L'uso e l'interpretazione di una firma su carta sono tipicamente definiti dalla cultura e dal contesto.

Nell'immaginazione popolare una firma autografa può essere facilmente ricondotta ad un individuo. Nella pratica, questo risulta essere difficile: la maggior parte degli impiegati non è in grado di ricondurre la firma autografa ad un collega, o al responsabile che ha firmato un documento o addirittura un assegno. **Ciò nonostante, tutto questo non è un problema perché nella maggior parte dei casi le firme cartacee sono effettivamente una formalità; la loro successiva verifica è rara.**

La ragione per cui le firme cartacee sembrano funzionare così bene è che nel tempo le società hanno imparato o a non utilizzarle, oppure a supportarle con ulteriori mezzi (ad esempio testimoni, notai, carta intestata aziendale), in situazioni dove è stato difficile risolvere controversie.

Il risultato finale è che le firme sono solo raramente chiamate in causa: c'è fiducia che i casi "rari" di controversie possano essere risolti attraverso procedure speciali che fanno affidamento sul contesto (procure, notai, testimoni), sulla memoria collettiva e su qualsiasi altro elemento utile a risolvere la controversia, sino ad arrivare al limite alla perizia calligrafica.

Firma digitale è invece il termine usato per la sottoscrizione di un documento elettronico, per un processo che dovrebbe essere analogo a quello della firma su carta, ma che fa uso di a tecnologia PKI.

Le analogie con la carta per le firme digitali sono utili, anche se non precise: chiaramente le firme cartacee non possono essere applicate ai documenti che rimangono in forma elettronica. Tuttavia, ulteriori elementi di sicurezza si rendono necessari perché la probabilità di controversie aumenta drammaticamente e non possono essere utilizzate le medesime cautele della firma cartacea: la firma digitale, tipicamente, non può essere apposta in presenza di testimoni (transazione online; riservatezza nell'inserire il PIN di sblocco del certificato privato); inoltre, occorre tutelarsi dalla presenza di potenziali modifiche ai documenti elettronici, non rilevabili.

Le firme digitali coprono queste preoccupazioni, offrendo molta più sicurezza intrinseca rispetto alle firme su carta. Rispetto a tutte le altre forme di firma, le firme digitali consentono con gran facilità la verifica dell'integrità di un documento. Questo non vuol dire che le firme digitali non possano essere usate impropriamente: se mal implementate o non supportato da appropriate procedure e processi, non sono più affidabili delle firme cartacee.

In estrema sintesi, grazie alla PKI, le firme digitali:

- stanno ai documenti elettronici quanto le firme autografe stanno ai documenti cartacei;
- forniscono prova affidabile dell'identità del firmatario (identificazione);
- non possono essere "copiate" da altri documenti;
- assicurano che un documento firmato non può essere modificato in seguito;
- hanno già un valore legale uguale a quello delle firme autografe.

Inoltre, l'ora esatta della firma digitale può essere registrata in modo più affidabile rispetto ad una firma cartacea attraverso l'utilizzo di una marca temporale.

Per il processo di firma digitale ci sono una serie di elementi specificatamente importanti, che riguardano ad esempio le interfacce dei programmi software, che devono essere tali da garantire che gli utenti capiscano il significato delle loro azioni. Tali elementi non sono quindi utili solo per garantire l'integrità dei dati ma anche per catturare le intenzioni effettive degli utenti.

Un processo di firma digitale ben strutturate dovrebbe quindi:

a) catturare l'intero contesto della transazione elettronica o del documento che viene sottoscritto;
b) assicurare che i dati visualizzati dall'utente riflettano con precisione i dati firmati digitalmente (WYSIWYS – What you see is what you sign);
c) richiedere all'utente di palesare la comprensione dell'impegno che si accinge a compiere, ovvero il desiderio di essere legato a questo impegno;
d) autenticare l'utente in modo che la chiave privata dell'utente divenga disponibile per il dispositivo di firma;
e) effettuare il calcolo della firma basata sulla chiave privata del firmatario e l'identità dei dati del firmato;
f) aggiungere, opzionalmente, una marca temporale;
g) inoltrare la transazione firmata per l'elaborazione, l'archiviazione e la successiva verifica.

Specifici dispositivi hardware garantiscono la gestione dell'apposizione della firma, in particolare la possibilità di sblocco della chiave solo da parte del titolare della firma.

Per la verifica della firma lato ricevente, occorre capire se la registrazione delle prove relative ad una transazione sono sufficienti per stabilire, in un secondo momento (anche dopo un periodo di tempo di molti anni), se la firma è valida.

La verifica richiede la generazione e il mantenimento di prove appropriate (ad es. record di transazioni che servono come ricevute elettroniche) e fornisce un alto grado di fiducia che le prove siano accurate e che qualsiasi successiva manipolazione o falsificazione possa essere rilevata.

L'uso di prodotti e servizi che possano fornire firme digitali di alta fiducia (firme qualificate), insieme con una serie di politiche di sicurezza applicata in modo appropriato, forniscono prove adeguate.

Nell'excursus appena esposto in questo capitolo ci sono due elementi che sono rilevanti alla nostra trattazione relativa al sigillo elettronico qualificato:

- molto spesso le firme cartacee sono apposte per formalità, a volte in dipendenza del ruolo che una persona occupa;
- anche se la tecnologia è utile a fare in modo che le firme digitali possano essere più robuste di una firma autografa, questo è vero solo se si adotta un processo adeguato.

La domanda è: mediante la tecnologia, non sarebbe possibile attuare dei processi che rendano efficiente l'espletamento delle formalità?

Il sigillo elettronico è costituito sulla medesima tecnologia della firma digitale: il termine è utilizzato nel regolamento UE n. 910/2014 (regolamento EIDAS) per le transazioni elettroniche all'interno del mercato interno europeo; in particolare, un sigillo elettronico è un dato collegato a un documento elettronico o ad altri dati, che garantisce l'origine e l'integrità dei dati.
Quanto esposto nel presente paragrafo ci serve come chiave di lettura delle norme, al fine di comprendere l'effettiva utilità del sigillo evitando di incorrere in visioni semplicistiche quali: il sigillo come la "firma digitale di una persona giuridica".

Sarebbe forse più corretto vedere il sigillo come la “firma digitale che rispetta un processo complessivo differente”. In particolare, ci soffermeremo sul concetto di controllo esclusivo del processo da parte del soggetto firmatario.

5.2 Basi legali

Dal regolamento eIDAS si possono estrarre le seguenti definizioni:

- **«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;
- **«sigillo elettronico avanzato»**, un sigillo elettronico che soddisfi i requisiti sanciti all’articolo 36;
- **«sigillo elettronico qualificato»**, un sigillo elettronico avanzato creato da un dispositivo per la creazione di un sigillo elettronico qualificato e basato su un certificato qualificato per sigilli elettronici.

I sigilli elettronici sono prodotti con le medesime tecniche crittografiche delle firme elettroniche: il risultato è in entrambi i casi un documento protetto.
Così come per la firma elettronica, quando un documento è sigillato, è possibile verificare l'origine del documento, oltre a rilevare se sono state apportate modifiche al documento dopo l'aggiunta del sigillo.
Ma allora qual è la differenza tra una firma elettronica e un sigillo elettronico? Come già accennato, una risposta semplicistica è che una persona aggiunge una firma, mentre un sigillo viene aggiunto da un'organizzazione. Torneremo il seguito su questo concetto per mostrare che è inesatto.
Riprendendo l’aspetto di processo su cui ci siamo focalizzati nel paragrafo precedente, volendo già entrare più in dettaglio e per dare una risposta più complessa, una firma è apposta da una persona che controlla la chiave privata del certificato, ovvero deve compiere un’azione di autenticazione dimostrando che è chi afferma di essere.
Un sigillo elettronico è invece aggiunto per conto di una persona giuridica, ad esempio un'organizzazione, ovvero non è richiesta alcuna azione diretta di controllo nemmeno da parte della persona responsabile dell’organizzazione.
Questo rende i sigilli elettronici facili da includere nei processi aziendali esistenti, nella ricerca di quell’efficienza dei processi digitali che non si devono limitare a riprodurre quanto si faceva nel mondo analogico. Ad esempio, se una organizzazione produce documenti che vengono inviati ad altre parti e desidera garantire l'integrità di questi documenti, i sigilli elettronici possono essere una buona soluzione.
La sigillatura dei documenti può essere integrata nel processo aziendale, garantendo che tutti i documenti prodotti siano automaticamente sigillati, senza alcuna interazione umana.
Analogamente, è altrettanto semplice includere la verifica dei documenti ricevuti nel processo aziendale. Questo potrebbe quindi automaticamente rifiutare i documenti in cui il sigillo non è valido, o avviare una verifica manuale se ci fossero dei dubbi sulla firma.
Andiamo ora ad approfondire gli aspetti normativi, partendo dal regolamento eIDAS e confrontando gli articoli 26 (requisiti firma elettronica avanzata) e 36 (requisiti sigillo elettronico avanzato).
La sola differenza sta nel comma c:

- [...] art. 26 comma 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 [...]
- [...] art. 36 comma c) - è creato mediante dati per la creazione di un sigillo elettronico che il creatore del sigillo elettronico può, con un elevato livello di sicurezza, usare sotto il proprio controllo per creare sigilli elettronici; e [...]

Di fatto, il sigillo può considerarsi funzionalmente riconducibile alla firma nel momento in cui il fornitore di certificati deve poter ricondurlo ad una persona fisica perseguibile legalmente - interpretazione dei successivi considerando del regolamento eIDAS:

- (59) È opportuno che i sigilli elettronici fungano da prova dell'emissione di un documento elettronico da parte di una determinata persona giuridica, dando la certezza dell'origine e dell'integrità del documento stesso.
- (60) I prestatori di servizi fiduciari che rilasciano certificati qualificati di sigilli elettronici dovrebbero attuare le misure necessarie per poter stabilire l'identità della persona giuridica rappresentante la persona fisica cui è fornito il certificato qualificato di sigillo elettronico, quando tale identificazione è necessaria a livello nazionale nel contesto di procedimenti giudiziari o amministrativi.

Ulteriori differenze/analogie tra firma elettronica avanzata e sigillo elettronico avanzato sono negli allegati al Regolamento eIDAS:

Allegato I - REQUISITI PER I CERTIFICATI QUALIFICATI DI FIRMA ELETTRONICA	**Allegato III - REQUISITI PER I CERTIFICATI QUALIFICATI DEI SIGILLI ELETTRONICI**
I certificati qualificati di firma elettronica contengono:	I certificati qualificati dei sigilli elettronici 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;	a) un'indicazione, almeno in una forma adatta al trattamento automatizzato, del fatto che il certificato è stato rilasciato quale certificato qualificato di **sigillo** elettronico;
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;	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 appaiono 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;	c) almeno il **nome del creatore del sigillo** e, se del caso, il numero di registrazione quali appaiono nei documenti ufficiali;
d) i dati di convalida della **firma elettronica** che corrispondono ai dati per la creazione di una firma elettronica;	d) i dati di convalida del **sigillo elettronico** che corrispondono ai dati per la creazione di un sigillo elettronico;
e) l'indicazione dell'inizio e della fine del	e) l'indicazione dell'inizio e della fine del

periodo di validità del certificato;	periodo di validità del certificato;
f) il codice di identità del certificato che deve essere unico per il prestatore di servizi fiduciari qualificato;	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;	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;	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;	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.	j) qualora i dati per la creazione di un sigillo elettronico connessi ai dati di convalida del sigillo elettronico siano ubicati in un dispositivo per la creazione di un sigillo elettronico qualificato, un'indicazione appropriata di questo fatto, almeno in una forma adatta al trattamento automatizzato.

Queste differenze sono recepite dalla EN 319 411-1 che specifica come nella struttura PDS (PKI Disclosure Statement) del certificato debbano essere previsti e specificati dei limiti di affidamento dello stesso.

In particolare, nella EN 319 411-2 si definisce la possibilità di profilare il certificato per il solo uso di persone giuridiche (QCP-l Qualified Certificate issued to a legal person).

Altre questioni tecniche sostanziali non se ne intravedono; tutti gli aspetti tecnici ed organizzativi nella specifica EN 319 411-2 procedono in modo duale:

- Initial Identity validation:

  - per la firma: The identity of the natural person and, if applicable, any specific attributes of the person, shall be verified:

    a) by the physical presence of the natural person; or

    b) using methods which provide equivalent assurance in terms of reliability to the physical presence and for which the TSP can prove the equivalence.

  - per il sigillo: The identity of the legal person and, if applicable, any specific attributes of the person, shall be verified:

a) by the physical presence of an authorized representative of the legal person;

or

b) using methods which provide equivalent assurance in terms of reliability to the physical presence of an authorized representative of the legal person which the TSP can prove the equivalence.

- Certificate profile:
  - per la firma deve includere: the policy identifier defined in clause 5.3 item a); and/or
    - an OID, allocated by the TSP (or any relevant stakeholder) to the certificate policy applied to issue the certificate.
  - per il sigillo deve includere: the policy identifier defined in clause 5.3 item b); and/or
    - an OID allocated by the TSP (or any relevant stakeholder) to the certificate policy applied to issue the certificate.
- ecc. con altre clausole che vanno di pari passo.

Molto probabilmente il medesimo approccio sarà attuato nel documento ETSI non ancora pubblico: TS 119 172 Signature policies - Part 4: Signature validation policy for European qualified electronic signatures/seals using trusted lists.

Per quanto riguarda il CAD – Codice dell'Amministrazione Digitale, decreto legislativo 7 marzo 2005, n.82, c'è un'interessante sintesi di Giovanni Manca

(http://cantieripadigitale.it/it/2018/06/22/documenti-sigillo-elettronico-caratteristiche-possibili-utilizzi/), da cui si evince che:

> *[…] Nello sforzo di coordinamento il Legislatore nazionale, a parte il richiamo alle definizioni del Regolamento eIDAS, non ha ritenuto di stabilire regole per l'efficacia e il valore probatorio del sigillo elettronico. Questa "dimenticanza" può essere spiegata dal fatto che il Legislatore ritiene sufficiente quanto stabilito a livello europeo, pur generando con questa decisione il problema che il sigillo elettronico resta svincolato da precise regole nazionali rispetto alle sottoscrizioni, che invece sono ampiamente trattate con riferimenti a vari articoli del Codice Civile. Nel seguito, oltre a ricordare cos'è il sigillo elettronico indicano alcune funzioni che lo strumento può svolgere. È anche utile ricordare che il sigillo elettronico è stato introdotto per la prima volta nel Regolamento eIDAS. Quindi non ha la storia decennale della firma elettronica, alla quale comunque si sovrappone tecnicamente in maniera pressoché totale. […]*

Sempre nel medesimo articolo sono riportate anche considerazioni a seguito di un'affermazione dell'avvocato Matilde Ratti [4] che vanno nella direzione di porre il nocciolo della questione sulla

gestione del controllo esclusivo del certificato, ovvero sulla riconducibilità alla persona fisica che rappresenta una persona giuridica.
Assumendo quindi che in Italia per l'utilizzo del sigillo si possa far diretto riferimento al regolamento eIDAS, l'elemento su cui ci possono essere dei dubbi è legato alla trasferibilità di responsabilità: nel momento in cui una persona alla quale la responsabilità del sigillo era riconducibile all'interno dell'organizzazione cessa di essere membro dell'organizzazione stessa, ovvero nel momento in cui non ha più competenza su un processo che adotta il sigillo, devono essere definiti i meccanismi mediante i quali la responsabilità di un processo che sfrutta il sigillo è riconducibile ad altro componente.
Sicuramente modelli organizzativi quali il D. Lgs. 231/2001 o certificazioni di qualità quali ISO 9001 o ISO 27001 possono venire in aiuto.
Tuttavia, mentre la firma digitale è riconducibile in modo diretto ad una persona, nell'ambito di un'organizzazione soprattutto se complessa sarebbe opportuno individuare le opportune deleghe di responsabilità correlate con l'uso di sigilli elettronici (poteri di firma).

5.3 Gli standard europei di riferimento

La normativa tecnica di riferimento richiamata nel precedente paragrafo è disponibile sulla pagina web del comitato tecnico (TC) ESI (Electronic Signatures and Infrastructures Activities) dell'ETSI (European Telecommunications Standards Institute - Istituto Europeo per gli Standard nelle Telecomunicazioni):

https://portal.etsi.org//TBSiteMap/ESI/ESIActivities.aspx

6. Scenari di utilizzo per il sigillo elettronico

L'uso del sigillo elettronico per garantire la prova delle transazioni può facilitare l'implementazione di servizi elettronici per gli individui, riducendo la necessità per loro di utilizzare la firma elettronica.
Così come per i certificati di firma digitale, il certificato di sigillo contiene informazioni che definiscono cosa implica esattamente l'autenticità del documento.
L'autenticità di un documento elettronico può significare che il documento sigillato è stato creato o elaborato in conformità con le regole regolate dal certificato o dalla politica di certificazione.
Il regolamento eIDAS specifica che solo una persona giuridica può creare un sigillo. La creazione di un sigillo elettronico garantisce l'autenticità del documento in conformità con i termini di utilizzo del sigillo elettronico stesso, che sono definiti nel certificato o nella politica di certificazione.
Sulla base di quanto esposto nel capitolo precedente, il sigillo ben si presta ad essere utilizzato in quelle situazioni per cui deve essere apposta una firma di prassi, per formalità.
In questo capitolo sono ripotati una serie di ipotetici scenari d'uso.

6.1 Considerazioni sulla creazione dei sigilli

Un sigillo elettronico avanzato viene creato utilizzando i dati, che sono sotto il controllo del creatore di un sigillo. Per inciso, il regolamento eIDAS non specifica come dovrebbe essere implementato questo controllo. In questo settore il regolamento eIDAS lascia una certa libertà e consente al creatore di un sigillo di stabilire le proprie misure di controllo sui dati utilizzati per posizionare il sigillo.
Garantire l'autenticità e l'integrità dei documenti può essere molto importante per facilitare l'attuazione di una serie di servizi elettronici, garantendo le misure di sicurezza necessarie per affrontare il rischio in un particolare processo aziendale.
Il garante dell'integrità e dell'autenticità di un documento sigillato è il creatore del sigillo. Anche l'ambiente e le condizioni in cui viene creato il sigillo rimangono sotto il suo controllo.
Questo schema consente la creazione di soluzioni tecniche, in cui il meccanismo di tenuta può diventare una parte di un dispositivo fornito o autorizzato da creatore di un sigillo. Questi dispositivi creano un sigillo elettronico sui dati elettronici elaborati da loro. Il sigillo può contenere informazioni sullo schema di elaborazione e sulle condizioni di sicurezza. Individui o persone giuridiche per specifici compiti dedicati possono quindi utilizzare tali dispositivi. Le prove preparate da un tale dispositivo possono proteggere un processo aziendale o altri servizi fiduciari.

6.2 Conservazione digitale

La conservazione digitale utilizza in vari scenari la sottoscrizione. Questo perché la normativa di riferimento sia secondaria che operativa stabilisce l'utilizzo della firma elettronica qualificata. Il caso più diffuso è quello del pacchetto di archiviazione che deve essere sottoscritto dal responsabile della conservazione. Naturalmente è anche prevista l'eventuale sottoscrizione del rapporto di versamento e del pacchetto di distribuzione.
Nella natura giuridica delle cose e in un'ottica di depersonalizzazione del responsabile della conservazione è senz'altro ragionevole ritenere che questa sottoscrizione possa, senza problemi, diventare l'apposizione di un sigillo elettronico.

In molti scenari questa operazione favorisce anche una “serenità psicologica” nella persona responsabile dell’apposizione del sigillo che (in verità senza alcuna specifica base giuridica) opera con maggiore buona volontà rispetto alle operazioni di sottoscrizione.
La separazione, almeno psicologica, tra persona fisica che appone una sottoscrizione digitale e la persona giuridica che appone il sigillo qualificato può determinare molte situazioni che suggeriscono l’uso del sigillo.
Naturalmente se parliamo di conservazione digitale, bisogna attenersi alla normativa vigente che stabilisce l’uso della firma digitale o della firma elettronica qualificata. Solo la modifica normativa può consentire l’utilizzo del sigillo elettronico.
Infatti, la vigente normativa relativa al processo di conservazione (art. 9 DPCM 3 dicembre 2013 Regole tecniche in materia di sistema di conservazione) prevede esplicitamente “la sottoscrizione con firma digitale o firma elettronica qualificata” in ogni caso previsto: (rapporto di versamento (“eventuale” punto e) pacchetto di archiviazione (punto f) e pacchetto di distribuzione (“ove prevista” punto g).
Nei primi due casi la firma deve essere del responsabile della conservazione, mentre nell’ultimo caso non è specificato.
Nella realtà il responsabile della conservazione delega tale firma ad altri soggetti.

Appare evidente che nel processo di conservazione il sigillo potrebbe validamente sostituire, in ogni caso previsto, le firme e consentire una maggiore efficienza del processo di conservazione, in quanto la finalità è soprattutto di attestare la provenienza da un sistema di conservazione e l’integrità dei pacchetti o dei rapporti, piuttosto che una dichiarazione di conoscenza o di espressione di una volontà.
Il sigillo dovrebbe essere quello della persona giuridica che detiene il sistema di conservazione e svolge le attività di conservatore.
Il Manuale di conservazione dovrebbe riportare le regole con cui i sigilli vengono apposti (*internal control mechanism),* prevedendo anche azioni automatiche di sistema.

6.3 Fatturazione elettronica

Nella fatturazione elettronica il sigillo ha trovato la sua prima applicazione “legale” nella pubblica amministrazione. Infatti, le ricevute rilasciate dall’Agenzia delle entrate a fronte dell’invio di fatture elettroniche.
Come direttamente indicato dall’Agenzia delle entrate, l'uso del sigillo apposto dal servizio dell'Agenzia è un'alternativa per chi non è dotato di firma digitale. Serve a garantire l'immodificabilità delle fatture elettroniche destinate a privati:

- se trasmesse tramite Sistema di Interscambio (dal 1° gennaio 2017),
- inviate al servizio di conservazione messo a disposizione dall'Agenzia delle Entrate.

L’Agenzia delle entrate indica che il sigillo è uno strumento che, tra l'altro, permette di rilevare se un documento informatico ha subito modifiche e che é definito dagli artt. 3 e 36 del Regolamento 2014/910/UE "eIDAS" (electronic IDentification Authentication and Signature).
La stessa Agenzia ricorda che, a differenza della firma elettronica, può essere apposto da una persona giuridica.
Di seguito il dump ASN.1 del certificato di sigillo elettronico dell’Agenzia delle entrate.

```
  0 1114: SEQUENCE {
  4  834:   SEQUENCE {
  8    3:     [0] {
 10    1:       INTEGER 2
       :     }
 13    8:     INTEGER 56 57 AC F4 57 DC B2 47
 23   13:     SEQUENCE {
 25    9:       OBJECT IDENTIFIER
       :         sha256WithRSAEncryption (1 2 840 113549 1 1 11)
 36    0:       NULL
       :     }
 38  109:     SEQUENCE {
 40   11:       SET {
 42    9:         SEQUENCE {
 44    3:           OBJECT IDENTIFIER countryName (2 5 4 6)
 49    2:           PrintableString 'IT'
       :         }
       :       }
 53   30:       SET {
 55   28:         SEQUENCE {
 57    3:           OBJECT IDENTIFIER organizationName (2 5 4 10)
 62   21:           PrintableString 'Agenzia delle Entrate'
       :         }
       :       }
 85   27:       SET {
 87   25:         SEQUENCE {
 89    3:           OBJECT IDENTIFIER organizationalUnitName (2 5 4 11)
 94   18:           PrintableString 'Servizi Telematici'
       :         }
       :       }
114   33:       SET {
116   31:         SEQUENCE {
118    3:           OBJECT IDENTIFIER commonName (2 5 4 3)
123   24:           PrintableString 'CA Agenzia delle Entrate'
       :         }
       :       }
       :     }
149   30:     SEQUENCE {
151   13:       UTCTime 16/11/2016 16:17:05 GMT
166   13:       UTCTime 17/11/2019 16:17:05 GMT
       :     }
181  105:     SEQUENCE {
183   11:       SET {
185    9:         SEQUENCE {
187    3:           OBJECT IDENTIFIER countryName (2 5 4 6)
192    2:           PrintableString 'IT'
       :         }
       :       }
```

```
196  30:     SET {
198  28:       SEQUENCE {
200   3:         OBJECT IDENTIFIER organizationName (2 5 4 10)
205  21:         UTF8String 'Agenzia delle Entrate'
     :       }
     :     }
228  26:     SET {
230  24:       SEQUENCE {
232   3:         OBJECT IDENTIFIER '2 5 4 97'
237  17:         UTF8String 'VATIT-06363391001'
     :       }
     :     }
256  30:     SET {
258  28:       SEQUENCE {
260   3:         OBJECT IDENTIFIER commonName (2 5 4 3)
265  21:         UTF8String 'Agenzia delle Entrate'
     :       }
     :     }
     :   }
288 290:   SEQUENCE {
292  13:     SEQUENCE {
294   9:       OBJECT IDENTIFIER rsaEncryption (1 2 840 113549 1 1 1)
305   0:       NULL
     :     }
307 271:     BIT STRING, encapsulates {
312 266:       SEQUENCE {
316 257:         INTEGER
     :           00 AB 7C C6 3F 1F 67 88 DB 18 E4 D8 82 DB DA EF
     :           5B 08 81 20 F4 D7 B2 9F 47 8C D6 63 44 1C 9C A2
     :           6D 13 C4 7F 4B 91 81 8E A5 5B 3F A9 92 24 0B 6E
     :           F6 6F C1 D5 93 EE 79 F9 D2 55 A0 69 AB 8A BB CE
     :           22 B2 09 41 B8 46 B8 80 A4 98 12 0B 07 77 EE 16
     :           61 41 BE F1 48 5D 38 0D A8 7F 07 AA 58 70 3E 5D
     :           DD C5 3B AB 81 BF B5 83 83 F9 E0 86 88 6F 5B AD
     :           62 3A E9 33 3D D9 6E F3 E0 C4 42 C3 29 87 D3 A9
     :           8D 08 3C ED C9 CC 3B 12 16 A8 35 FA 90 8F 19 5C
     :           57 98 CB 9F 18 F9 E9 5D 28 9A 59 5C B8 93 96 78
     :           7C DF 9B BD E2 29 DF 39 51 E6 21 A3 D5 6E 4F CC
     :           2A EC 82 C5 4C 2B 39 72 0A 71 FF ED 20 C0 04 69
     :           48 7A 9C A0 7D D7 E3 82 ED F4 C3 AA 06 09 2B BC
     :           73 B8 FC F5 5E FF 67 50 19 9C E6 C3 0B ED FC AC
     :           DB D3 A9 47 05 C1 B5 9A 8C 0A 32 E9 7C E2 1A FA
     :           7D 27 3B 3F 7F D8 92 C6 77 6C CC AA 4B 49 B3 8C
     :           4B
577   3:         INTEGER 65537
     :       }
     :     }
     :   }
```

```
582 256:    [3] {
586 253:      SEQUENCE {
589  31:       SEQUENCE {
591   3:        OBJECT IDENTIFIER authorityKeyIdentifier (2 5 29 35)
596  24:        OCTET STRING, encapsulates {
598  22:         SEQUENCE {
600  20:           [0]
     :             EA 44 3F 1F 19 E3 37 3E AB AA 94 82 A5 9F EB FC
     :             16 BA 7F B5
     :           }
     :         }
     :       }
622 170:      SEQUENCE {
625   3:       OBJECT IDENTIFIER cRLDistributionPoints (2 5 29 31)
630 162:       OCTET STRING, encapsulates {
633 159:        SEQUENCE {
636 156:         SEQUENCE {
639 153:           [0] {
642 150:             [0] {
645 147:               [6]
     :                 'ldap://cads.entrate.finanze.it/CN=CA%20Agenzia%2'
     :                 '0delle%20Entrate,OU=Servizi%20Telematici,O=Agenz'
     :                 'ia%20delle%20Entrate,C=it?certificateRevocationL'
     :                 'ist'
     :               }
     :             }
     :           }
     :         }
     :       }
795  29:      SEQUENCE {
797   3:       OBJECT IDENTIFIER subjectKeyIdentifier (2 5 29 14)
802  22:       OCTET STRING, encapsulates {
804  20:        OCTET STRING
     :           A5 D3 05 3A 49 7E 2A 20 61 CF 21 95 F3 96 E1 FA
     :           6B 11 22 45
     :         }
     :       }
826  14:      SEQUENCE {
828   3:       OBJECT IDENTIFIER keyUsage (2 5 29 15)
833   1:       BOOLEAN TRUE
836   4:       OCTET STRING, encapsulates {
838   2:        BIT STRING 6 unused bits
     :           '10'B (bit 1)
     :         }
     :       }
     :     }
     :   }
```

```
    :   }
842  13:  SEQUENCE {
844   9:    OBJECT IDENTIFIER sha256WithRSAEncryption (1 2 840 113549 1 1 11)
855   0:    NULL
    :   }
857 257:  BIT STRING
    :    A4 34 80 27 4E 12 62 F3 F2 49 21 BF 7D CF AF 3C
    :    F6 E7 ED E8 D8 E4 EB 20 FE 09 7B 2C E5 76 FF 51
    :    E5 6A CA A5 08 D7 1C 8E 15 AA 73 E4 D1 19 FD 1C
    :    7B 27 17 37 E8 05 F2 8E 85 12 07 F7 37 09 B8 2B
    :    9D 2D 30 5E 70 D4 5C 4D AD 2C 22 5F 8A 6F F8 56
    :    59 F0 68 33 76 96 33 F8 1E 60 57 84 41 1E 07 C1
    :    04 1F 47 BC 8F 8D D7 63 44 0C 88 2B 6F 3E EC 6A
    :    BA BD 50 33 7B A9 FD 09 0B 30 0C 14 09 9E 22 BF
    :    1A D2 06 D9 88 A4 54 91 70 5E D7 6D 25 92 D5 98
    :    AF C9 13 FC C9 26 CF 50 08 DE 7A 18 88 59 59 64
    :    D7 69 DE 1D 96 40 6C 46 DC 35 E7 B7 61 E7 56 77
    :    18 6E 21 43 4F 09 FA 34 AD A1 4F DB AB C2 57 B1
    :    D8 BD 7F 33 3A E4 EE 6B D2 AD 75 B8 AC 84 CA F9
    :    57 3A 95 37 88 60 9A 02 2F 05 5C 09 FF 02 08 C8
    :    1E 8F 69 83 1F 11 E7 4E 80 D6 F6 13 12 20 8B BE
    :    8A F4 67 50 25 08 80 F7 7B 0C 0F 9E B0 71 53 DD
    :  }
```

6.4 Protocollo e repertori informatici

Nella normativa di riferimento e nelle regole tecniche del protocollo informatico non è previsto, né indicato o consigliato, l'uso di una sottoscrizione elettronica per le operazioni di registrazione.
Certo è che in questo contesto lo scopo principale del sigillo (garantire la certezza dell'origine e l'integrità dei dati) e, come già riportato, la possibilità di svincolarne la generazione dall'operatore umano, mediante un procedimento automatico, appaiono estremante calzanti in un conteso dove la trasmissione e la ricezione di un'alta numerosità di documenti informatici è un elemento fondamentale.
Per poter individuare le applicazioni possibili ed appropriate è utile chiarire alcuni aspetti.

La registrazione informatica di protocollo è un'attività che avviene su documenti formati; certifica esclusivamente l'uscita o l'ingresso degli stessi mediante l'associazione di un numero sequenziale ed una data opponibili a terzi. (Ricordiamo che il registro di protocollo è un atto pubblico di fede previlegiata [1] e che la registrazione di protocollo è una validazione temporale [2]).

Nel DPR 445/2000 l'articolo 55 "Segnatura di protocollo" al comma 1 stabilisce che:

"La segnatura di protocollo è l'apposizione o l'associazione all'originale del documento, in forma permanente non modificabile, delle informazioni riguardanti il documento stesso. Essa consente di individuare ciascun documento in modo inequivocabile".
Ovviamente non è nello scopo di questo documento dare indicazioni sulle modalità con cui gestire un servizio primario come quello del protocollo informatico o della gestione dei documenti informatici in generale, ma è inutile nascondere che l'apposizione della segnatura di protocollo all'originale del documento è la prassi consolidata in ambito analogico ed è quella che per consuetudine si cerca di perseguire, non con poche difficoltà, anche sulla documentazione digitale.
La motivazione per la quale purtroppo si insiste con l'apposizione della segnatura di protocollo è che il documento non è inserito in un processo reingegnerizzato in ottica di dematerializzazione ed alla fine viene, spesso inutilmente, stampato.
Si deve sottolineare che con una completa digitalizzazione della documentazione e dei processi, una corretta e piena applicazione delle indicazioni sull'interoperabilità tra sistemi [3] e nel rispetto delle regole tecniche per cui i documenti vanno "identificati e trattati nel sistema di gestione informatica dei documenti" [4], la problematica di "apposizione" della segnatura di protocollo verrebbe meno, a fronte dell'evidente efficienza dell'"associazione".
In ogni caso questa prassi non è corretta perché l'applicazione di procedure pensate per la carta al digitale è scorretta.
Concentrandoci sulle possibile analogie tra segnatura di protocollo e sigillo elettronico è sicuramente possibile configurare i sistemi in modo che appongano con procedura automatica un sigillo informatico oltre alla segnatura a tutta la documentazione protocollata, ampliando le garanzie di origine ed integrità dei documenti (a titolo di esempio pensiamo ad un cittadino che riceve sulla sua posta elettronica ordinaria la scansione di un documento magari con l'indicazione di firma sostituita a mezzo stampa…).
Peraltro, le operazioni di protocollo devono essere considerate separate da quelle di gestione documentale e in questo senso l'apposizione del sigillo come elemento qualificante per la provenienza e l'integrità del documento sigillato deve trovare il corretto equilibrio tra i vari scenari.

Infatti, i documenti informatici arrivano al protocollo tramite il sistema della PEC (che in qualche modo possiamo anche associare al principio giuridico del "domicilio digitale") quindi la loro provenienza è nota.
Il documento nel sistema di gestione documentale segue il procedimento definito nel manuale di gestione e il sigillo non sembra essere indispensabile come elemento che fornisce valore aggiunto a tali operazioni. Anche il protocollo in uscita utilizza la casella di PEC dell'Area Organizzativa Omogenea, quindi anche in questo caso il sigillo non fornisce particolari vantaggi.
La natura tecnologica del sigillo elettronico, che come abbiamo visto è pressoché identica a quella della firma non porta vantaggi nemmeno nella gestione dell'integrità del documento, quando le operazioni successive alla sottoscrizione digitale rischiano di alterarne l'integrità.
Da queste premesse si deduce che il protocollo informatico, sul piano tecnologico dovrebbe evitare di modificare il documento oggetto dell'operazione con la conseguenza di non preservarne l'integrità. In ogni caso l'apposizione di un sigillo sul documento protocollato non sembra portare alcun effettivo vantaggio.
Nella gestione documentale il sigillo può essere utilizzato quando non c'è l'obbligo di sottoscrizione da parte della persona fisica e si vuole garantire la provenienza (in senso di responsabilità legale e non di origine di trasmissione del documento) e l'integrità. Cioè è opportuno rimanere nella specificità dello strumento senza sconfinare in altri scenari tecnici e normativi.
Allo stato dell'arte, quindi, è utile discutere del possibile utilizzo del sigillo elettronico negli scenari di protocollo informatico e gestione documentale, ma al momento non si percepiscono reali vantaggi mentre il rischio di confusione tra strumenti "legali" differenti può essere elevato.

[1] Consiglio di Stato, Sez. IV - 5 ottobre 2010, n. 7309
[2] DPCM 22 febbraio 2013 Art. 41. Riferimenti temporali opponibili ai terzi - Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche
[3] La circolare Agid 23 gennaio 2013 n.60 "segnatura protocollo informatico", che descrive le modalità di produzione del file segnatura.xml, soddisfa il requisito normativo del già citato comma 1 del DPR 445/2000 l'articolo 55 circa "[…] l'associazione all'originale del documento, in forma permanente non modificabile […]"
[4] rif DPCM 13 novembre 2014 Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici Art. 9 comma 3

6.5 Sanità elettronica

La sanità elettronica ha utilizzato le sottoscrizioni elettroniche partendo già dai primi progetti in Lombardia e in altre Regioni. Gli utilizzi da parte degli operatori sanitari sono stati sempre molto ampi e diffusi nonostante un costante mugugno nei confronti di queste tecnologie. Il personale sosteneva che l'informatica e la complessità nel procedimento clinico introduceva ritardi rispetto all'attività sanitaria.
La disponibilità del sigillo può presentare numerose opportunità al sistema sanitario digitalizzato, proprio perché la sua natura impersonale ma con la validità legale per attestare la provenienza e l'integrità del dato supera la necessità associare il firmatario alla persona fisica.
Il procedimento amministrativo clinico può essere ricondotto all'organizzazione, al reparto o comunque alla funzione giuridica operativa che valida il dato.
La firma apposta con procedura automatica può senza problemi essere sostituita dall'apposizione di sigilli elettronici qualificati anch'essi apposti con procedura automatica analoga a quella della sottoscrizione.

Questo per la refertazione degli esami di laboratorio, per la nota di diario clinico e per una serie di altra documentazione clinica che possiamo definire di routine.

6.6 Utilizzi in scenari specifici

La circostanza che la sottoscrizione elettronica è fisiologicamente connessa alla sottoscrizione autografa non deve far perdere di vista il fatto che il sigillo elettronico è stabilito nel regolamento eIDAS per "autenticare" documenti informatici, software, server o qualsiasi bene digitale riferibile ad una persona giuridica.
La conferma che questa ipotesi sia valida si ha con la lettura del Considerando 65 del regolamento: "*Oltre ad autenticare il documento rilasciato dalla persona giuridica, i sigilli elettronici possono anche servire ad autenticare qualsiasi bene digitale della persona giuridica stessa, quali codici di software o server".*
A titolo di esempio possiamo ipotizzare che il codice sorgente di un pacchetto software possa essere sigillato elettronicamente al fine di consolidare il contenuto del codice "sigillato" e la sua riferibilità alla persona giuridica che "possiede" il software.
Questo approccio è utile in quegli scenari dove il cliente, a sua tutela, chiede al produttore del software di depositare i sorgenti presso un Notaio. Al pacchetto software (il codice sorgente e la documentazione) può essere apposto un sigillo elettronico qualificato per avere la presunzione legale di integrità e correttezza dell'origine dei dati ai quali il sigillo elettronico qualificato è associato.
Ancora più efficace è lo scenario delle ricevute di accettazione o di consegna nella Posta Elettronica Certificata dove la firma elettronica delle stesse è effettuata da un server.
L'efficacia probatoria di queste ricevute può essere elevata a livello europeo se la firma elettronica è sostituita da un sigillo elettronico avanzato qualificato.
Questo si può evincere anche dall'articolo 44 del regolamento (Requisiti per i servizi elettronici di recapito certificato qualificato). Infatti, nella lettera d) del paragrafo 1 si stabilisce che "*l'invio e la ricezione dei dati sono garantiti da una firma elettronica avanzata o da un sigillo elettronico avanzato di un prestatore di servizi fiduciari qualificato in modo da escludere la possibilità di modifiche non rilevabili dei dati".*
Stante l'ordinamento nazionale, in attesa delle decisioni governative sul futuro della PEC anche in termini di possibile convergenza con i citati servizi elettronici di recapito certificato qualificato, appare opportuno utilizzare i principi del sigillo elettronico per le ricevute del sistema PEC.
Questo utilizzo comporta la modifica delle regole di riferimento utilizzando lo strumento delle Linee Guida emanate da AgID in conformità all'articolo 71 dell'ultima versione del CAD.
Altri utilizzi del sigillo elettronico sono in scenari completamente originali. Il diritto d'autore sulla rete Internet per musica e fotografia; per proprietà intellettuali o per progetti opera dell'ingegno.
Alcuni utilizzi sono possibili già con la semplice applicazione del regolamento eIDAS.
In molti altri scenari è indispensabile, per la certezza del diritto, che il Legislatore nazionale coordini le normative specifiche con il concetto di sigillo elettronico e delle sue tre fattispecie.
Alla data di pubblicazione del presente documento nel CAD non è presente alcun riferimento al sigillo elettronico e alla sua efficacia probatoria in alternativa alla firma come conseguenza di una maggiore coerenza giuridica con questo strumento comunitario.
Possiamo poi aggiungere che le università producono certificati per studenti, che in genere possono essere scaricati in formato PDF. Ciò rende molto facile per uno studente modificare il diploma e alterare qualsiasi cosa, dai voti alle materie. Sigillando elettronicamente i diplomi, è

semplice verificare che questi siano autentici, che provengano dall'università corretta e che non siano manomessi.
I sigilli elettronici potrebbero anche essere utilizzati per garantire l'integrità delle dichiarazioni bancarie, la conferma dell'occupazione, i documenti di identità, gli atti, i documenti politici, i certificati di formazione, le dichiarazioni fiscali e molti altri.
Un esempio del summenzionato utilizzo di un sigillo elettronico è una macchina fotografica in cui ogni immagine catturata è sigillata con informazioni sull'ora e sul luogo, scaricate dal GPS. Questo timbro garantisce l'autenticità dell'origine delle immagini da uno specifico modello di fotocamera e specifica anche dove e quando è stata scattata la foto. L'entità che presenta questo sigillo è il produttore (o il garante) della fotocamera. Il produttore della fotocamera in questo modo assicura che solo le foto scattate con questa specifica fotocamera, accompagnate dai dati del GPS, abbiano questo sigillo.
Un altro esempio che illustra l'uso del sigillo è uno scanner di carta in cui viene utilizzato il sigillo per garantire l'autenticità e l'integrità dei documenti scansionati. Il produttore dello scanner garantisce che il sigillo venga creato solo su un documento scansionato dalla propria macchina. Tuttavia, nessun documento che non è stato scansionato sullo specifico dispositivo può ricevere un sigillo simile.
L'uso di un sigillo elettronico da parte del produttore del dispositivo consente la consegna di apparecchiature che svolgono varie funzioni e schemi di elaborazione dei dati. Fornisce inoltre la prova che il produttore o il garante del dispositivo garantisce l'autenticità e l'integrità. Questi possono essere dispositivi che elaborano solo il contenuto di documenti elettronici (ad esempio sigillando i messaggi ricevuti o inviati), nonché i dispositivi che forniscono contenuti aggiuntivi, ad esempio un'immagine, movimento, suono, tempo e luogo (ad esempio fotocamere, registratori, videocamere, velocità telecamere e lettori biometrici).
I documenti sigillati possono essere ulteriormente elaborati nel cloud dati o utilizzati come prova per altri servizi fiduciari, che a loro volta creano l'opportunità di creare una serie di servizi aziendali.
L'uso del sigillo elettronico rende quindi possibile la semplificazione dell'utilizzo di servizi elettronici da parte di individui senza la necessità di una firma elettronica.

7. Scenari di utilizzo per la FEA e per la FES (Firma Elettronica Semplice)

La firma elettronica è definita nel regolamento europeo eIDAS (articolo 3, numero 10) e nel nostro ordinamento (CAD) le viene assegnato un valore probatorio liberamente valutabile in giudizio, in relazione alle caratteristiche di sicurezza, integrità e immodificabilità.
Oramai capita a tutti, sul lavoro, ma anche e soprattutto nella vita privata, di ricevere richieste di invio di documenti da sottoscrivere in modo elettronico, o di utilizzare strumenti atti a realizzare firme elettroniche, in possesso di aziende presso cui vi recate a svolgere delle operazioni. Per non parlare di scenari mobili in cui operatori/funzionari incaricati vengono presso le vostre sedi o abitazioni con strumenti appositi e vi chiedono di impiegarli per approvare, confermare, siglare, ecc...
A titolo di esemplificazione si possono citare i casi seguenti:

- la sottoscrizione delle cosiddette contabili bancarie presso gli sportelli degli istituti finanziari, con tablet e penne elettroniche che ci permettono di simulare quanto avviene con la carta e le penne ad inchiostro tradizionali, ovvero la apposizione di tratti olografi su documenti riportanti informazioni dell'operazione appena svolta;
- la sottoscrizione di contratti d'acquisto di prodotti finanziari proposti da intermediatori anche presso le proprie abitazioni o luoghi di lavoro, tramite tablet grafometrici o scambio di email con il documento precontrattuale o contrattuale da confermare tramite l'apposizione di codici cosiddetti One Time Password che pervengono via SMS oppure su apposite applicazioni per gli smartphone oppure ancora su device elettronici con display appositamente realizzati allo scopo e consegnati al firmatario;
- la sottoscrizione della ricevuta di consegna dei vettori che consegnano i pacchi a casa, che chiedono di apporre una firma con delle penne elettroniche sui tablet dei computer palmari. Oppure viceversa, la sottoscrizione del Documento di Trasporto in un magazzino per le consegne, apposta tramite tablet grafometrici;
- lo scambio di documenti da remoto via mail per l'acquisto di servizi o prodotti, quali ad esempio una polizza assicurativa, un servizio sotteso ad un abbonamento di un sito online per l'acquisto di viaggi vacanze, ma anche ragionevolmente i documenti di prevendita di una automobile vista in un concessionario a 200 km dall'abitazione;
- i consensi che vengono richiesti su form di un sito di e-commerce per l'acquisto dei beni offerti dal venditore;
- un ordine di materiale confermato via e-mail al venditore;
- la sottoscrizione su tablet grafometrici di documenti privacy e di raccolta di consensi alla realizzazione del Dossier sanitario elettronico o del consenso informato prima di un esame o di un intervento;
- l'invio di fatture elettroniche alla PA ma dal 01/01/2019 anche ai nostri clienti nello scenario B2B.

Questi sono solo alcuni esempi, ma ci possiamo aspettare in un prossimo futuro, il proliferare di queste pratiche spinte dalla digitalizzazione dei processi aziendali e dalla gestione delle informazioni in forma elettronica ovvero tramite documenti informatici.
Ma per tutte queste firme, l'utente firmatario che tipo di firma elettronica ha apposto?

Ovvero: l'azienda che ne propone il processo e gli strumenti, di che tipo di firma elettronica si è dotata?
È corretto che non vi siano indicazioni esplicite del tipo di firma proposto al firmatario: Firma Elettronica Semplice (FES) o Firma Elettronica Avanzata (FEA)?
A queste domande alcune volte non è chiaro cosa rispondere. Ma la cosa sorprendente, è che se si pongono le stesse domande a firmatari o proponenti documenti da firmare, in uno scenario tradizionale con carta e penna, non è chiaro qual è il tipo di firma che viene raccolta ed il suo valore probatorio. La prassi consolidata e l'univocità degli strumenti, fa intendere che la firma sia sempre la stessa e con lo stesso valore. Ma al contrario, anche con la carta e la penna, le firme raccolte spesso non hanno caratteristiche utili per una perizia grafologica richiesta in caso di disconoscimento: sono fatte in condizioni logistiche non comode, non sono leggibili, vengono raccolte da persone di cui non viene accertata l'identità, ecc...
Pensiamo ad esempio alle firme raccolte sui DDT o sul blocchetto delle consegne di un corriere. Spesso queste non sono delle vere e proprie firme ma sono al più delle sigle, ovvero dei tratti grafici, magari solo le iniziali del vettore o del destinatario. L'azienda con questo tipo di documentazione, intende attestare l'avvenuto ritiro piuttosto che una approvazione esplicita delle informazioni e della merce indicata sui documenti. Con lo stesso scenario, la situazione potrebbe cambiare se la merce che viene ritirata ha valore rilevante oppure se la può ritirare solo una persona con determinate caratteristiche: per esempio una persona che possiede un patentino che lo abilita all'uso di medicinali o fitofarmaci in campo veterinario o agrario. In questi ultimi casi, l'attenzione a raccogliere una firma leggibile, apposta da una persona la cui identità sia stata prima verificata è auspicabile, se non addirittura necessaria per poter produrre documentazione con l'adeguato valore probatorio.
La normativa nazionale che definisce le firme elettroniche, ovvero il Codice dell'amministrazione Digitale, e le regole tecniche contenute nel DPCM 22 febbraio 2013 che ne fornisce le linee guida per la loro realizzazione, definiscono vari tipi di Firma Elettronica con validità giuridiche differenti e regole di creazione ulteriormente differenti.
A tutto ciò, anche il regolamento europeo eIDAS in vigore negli Stati membri dal primo luglio 2016, ne stabilisce la definizione e, come spiegato nell'articolo disponibile al seguente collegamento:
https://www.agendadigitale.eu/documenti/firma-elettronica-cose-e-le-differenze-tra-firma-digitale-semplice-qualificata-certificata/ ,
con un significato diverso nell'ambito delle normative nazionali.
Infatti, se da un lato se ne trovano definizioni analoghe per nomenclatura quali ad esempio Firma Elettronica Avanzata, Firma Elettronica Qualificata, la loro applicazione tecnico giuridica nel contesto nazionale dei singoli stati membri può essere differente creando non pochi problemi di interoperabilità dei documenti scambiati tra cittadini di stati differenti.
Firma Elettronica cosiddetta Semplice (FES) è definita come dati connessi ad altri dati utilizzati per firmare. Mentre la Firma Elettronica Avanzata è una firma elettronica che soddisfa le regole tecniche contenute nel paragrafo quinto del DPCM 22 febbraio 2013, atte a creare una connessione tra i dati da firmare e quelli della firma che garantiscano la possibilità di identificare univocamente il firmatario.
Partendo dalla definizione delle due tipologie di firme elettroniche, ci soffermeremo sulle loro differenze sostanziali e proveremo a suggerire una chiave di lettura e di interpretazione per le organizzazioni che desiderano realizzare questi processi.
Torniamo alle domande: che tipo di firma ha usato il firmatario e che tipo di firma ha proposto il proponente. E quindi, quali documenti informatici verranno prodotti da quei processi?

7.1 Firme Elettroniche Semplici

Prendiamo innanzitutto in considerazione la Firma Elettronica cosiddetta Semplice (FES), ovvero quella in cui ci si è soffermati "solo" a soddisfare i requisiti della definizione di principio: dati connessi ad altri dati utilizzati per firmare.
Questo tipo di firma è applicata da molti dei processi che vengono impiegati giornalmente e che sono citati all'inizio del paragrafo. Si veda ad esempio l'invio di una e-mail: il contenuto del testo, che perviene al destinatario assieme all'indirizzo e-mail del mittente, si ritiene "firmato" dal mittente e quindi costituisce documento informatico.
Il consenso fornito su di una *form* di un sito durante l'acquisto di un viaggio in modalità e-commerce, verrà registrato dal portale assieme ai dati di autenticazione forniti per poter accedere al modulo e che sono stati rilasciati a seguito di una procedura di identificazione ed accettazione delle condizioni di utilizzo del servizio. La registrazione del consenso, correlato alle informazioni oggetto dell'approvazione costituiscono un documento informatico sottoscritto con firma elettronica semplice.
Anche l'uso di una penna elettronica sullo schermo di un tablet o di uno smartphone, possono rappresentare una FES, in quanto non tutti i dispositivi di questo tipo sono in grado di rilevare le cosiddette informazioni biometriche o non vengono impiegati per farlo, ma viene catturata solo l'immagine del tratto olografo ed apposto sul documento. Ma non solo: non vi è traccia della procedura di identificazione nel processo attuato prima della raccolta della firma.
Il documento informatico che ne deriva, vede la sua validità come forma scritta ed il suo valore probatorio, liberamente valutabili in giudizio in riferimento alle sue caratteristiche di sicurezza, integrità e immodificabilità. Purtroppo, nelle varie revisioni del CAD, la firma cosiddetta FES ha mutato valore: si è passati da un non valore di forma scritta, ad un valore di forma scritta per poi tornare nell'ultima revisione di gennaio 2018 ad un non valore di forma scritta.
Ad una prima lettura di queste frasi, magari da parte di non addetti ai lavori come ad esempio gli imprenditori che si accingono ad implementare questo tipo di firme, spesso si sente dire: "Queste firme valgono poco o niente".
Questo assolutamente non corrisponde a verità. D'altro canto, per tornare al parallelo con la carta, anche una copia di un documento contenente indicazioni manoscritte, può essere portato in giudizio con esito favorevole.
Come citato nel paragrafo precedente, un ruolo determinante in ambito digitale, in merito alla validità del documento e della sottoscrizione, lo ha il processo di generazione della firma e del documento e la sua conservazione. Questi devono essere in grado di garantire:

1. la sicurezza durante la fase di realizzazione e formazione, che impedisce la possibilità di alterazione dei dati firmati e costituenti la firma, collegandoli in modo unico ed inscindibile tra di loro, garantendo l'assenza di elementi in grado di alterare i dati in modo malevolo, come ad esempio mediante *script*;
2. l'integrità dei dati, ovvero la possibilità di verificare che i dati oggetto della firma e la firma stessa siano esattamente quelli dell'istante di firma;
3. l'immodificabilità dei dati, ovvero la possibilità di rilevare eventuali modifiche ai dati pervenute dopo l'apposizione della firma.

7.2 Firma Elettronica Avanzata (FEA)

Prendiamo in considerazione la Firma Elettronica Avanzata (FEA), ovvero un particolare tipo di firma elettronica che soddisfa alle regole tecniche definite nel DPCM 22 febbraio 2013.
La raccolta di questo tipo di firme è un processo aziendale che richiede adempimenti e lo svolgimento di azioni da parte di personale incaricato dall'azienda atte a dare le maggiori garanzie di bontà e forza probatoria che le firme FEA forniscono.
Le firme FEA permettono di ottenere documenti informatici che soddisfano la forma scritta e sono e permettono di ottenere in particolare due caratteristiche molto importanti rispetto alle FES:

- nel processo di raccolta è prevista l'identificazione del firmatario, una prima volta in fase di accettazione delle condizioni di utilizzo dello strumento, e ad ogni apposizione di una firma successiva;
- i dati del firmatario permettono di ricondurli univocamente ad esso.

Queste due caratteristiche determinano per un'azienda un fattore discriminante molto importante nella scelta di adottare una FEA anziché una FES. Infatti, se i documenti su cui si desidera impiegare questo tipo di processi presuppone un rischio, elevato di contenziosi e di dover ricorrere a dimostrazioni della paternità dei dati della firma, la FEA è una scelta consigliata se non obbligata.

7.3 Come valutare la scelta?

La valutazione di impiegare un tipo di firma FES o una più forte ad esempio una FEA, passa da una valutazione basata fondamentalmente su tre livelli:

- l'usabilità del processo e degli strumenti. Sembra una frase banale, ma spesso i requisiti dei processi sottesi all'apposizione di un particolare tipo di firma, non sono applicabili al processo documentale organizzativo. Ad esempio, se nessuno dei terzi firmatari è in possesso di smartcard o token USB con certificati di firma qualificata, è impensabile voler impostare il processo sulle Firme Digitali;
- il livello giuridico che il documento deve avere, in termini sostanzialmente di necessità di garantire la forma scritta, oppure la prescrizione di un regolamento specifico in cui il documento viene prodotto. Ad esempio, IVASS, l'Istituto di Vigilanza per le compagnie di assicurazione, prevede l'impiego di Firme Elettroniche almeno Avanzate per la sottoscrizione dei contratti e polizze;
- l'altro livello di valutazione è il valore probatorio, e questo è nuovamente collegato anche alla sicurezza e metodologia impiegate per la formazione del documento ed ai dati della firma personalissimi del firmatario, raccolti durante l'operazione. Più questi sono completi e permettono di ricondurre in modo univoco al firmatario, più sarà possibile dimostrare la paternità della firma e quindi della documentazione.

D'altro canto, queste caratteristiche a ben vedere sono presenti anche nella forma cartacea "tradizionale". Come potremmo verificare che un documento sia stato sottoscritto da una determinata persona, se ne abbiamo solo una fotocopia, il tratto non è leggibile e non vi sono tracce certe sulla non modificabilità dei dati nel tempo? Oppure come è possibile avere certezza che il firmatario sia stato identificato prima di procedere e che quindi sia stato proprio lui a vergare la carta?
Per esempio, impiegando un procedimento analogo a quello per la raccolta di firme FEA, ma rilassandone alcuni vincoli imposti dalle regole tecniche del DPCM 22 febbraio 2013, si possono ottenere dei documenti con delle firme altamente sicure, che sono in grado di garantire che sono

state raccolte per quel documento e solo per lui, che contengono dati di contesto non modificabili, indicanti informazioni utili a poter dimostrare il processo utilizzato per apporle e la sua bontà.

Come si nota, sia su carta che in digitale, il nocciolo della affidabilità e della garanzia di paternità risiedono nella modalità di formazione e conservazione del documento stesso nella sua completezza e delle "prove" necessarie a dimostrare anche molto tempo dopo, che i dati non siano stati modificati in modo malevolo.

7.4 Sanità elettronica

Un ambito di impiego degli strumenti digitali molto interessante è quello della sanità. I processi organizzativi della sanità prevedono molto spesso nei percorsi di cura, la compilazione da parte dei pazienti di documenti da sottoscrivere su cui vengono raccolti dati dello stato di salute e sempre più spesso consensi.

Per la natura dei dati raccolti e degli scopi del documento, ovvero tutelare paziente, struttura sanitaria, medici ed operatori in merito ad interventi farmacologici ed operatori, manuali o chirurgici, il loro trattamento deve garantire la sicurezza e riservatezza del dato trattato.

Il fatto di digitalizzare tali documenti può dare maggior efficienza e garanzie di tutela, in quanto i documenti informatici possono viaggiare in modo più veloce della carta, anche tra diversi reparti di una struttura sanitaria, e maggiormente protetti in quanto visibili solo tramite opportuni software che li trattano, a cui gli utenti che vi accedono sono solo quelli provvisti di credenziali di autenticazione e con determinate autorità e permessi sulle operazioni possibili su di essi.

Alcuni dei documenti coinvolti in questi processi sono:

1. Raccolta dei consensi privacy
2. Consenso alla costruzione del Dossier Sanitario Elettronico (DSE) o del Fascicolo Sanitario Elettronico (FSE)
3. Delega per il ritiro dei referti
4. Questionari anamnestici
5. Informative specifiche per esame diagnostico
6. Consenso informato per esami, terapie o interventi

La produzione dei documenti e la gestione dei dati, avviene già ora nella quasi totalità dei casi, impiegando programmi gestionali specifici di settore, i quali permettono di costruire i documenti che vengono stampati per la raccolta dei consensi e delle sottoscrizioni con la penna. La trasformazione di questi flussi in modo completamente digitale, tramite la compilazione e raccolta dei dati e delle Firme Elettroniche da parte dei pazienti e medici ed operatori coinvolti nello svolgimento della pratica sanitaria, permette di ottenere un nuovo processo che non necessita più di stampare i documenti e di raccoglierli dopo la loro compilazione.

Ma quali tipi di Firme Elettroniche sono idonee o addirittura obbligatorie per questi documenti?

Le firme elettroniche digitali sono già molto impiegate in questi flussi, sia quelle con smartcard da parte dei medici, sia quelle remote ed automatiche effettuate tramite dispositivi HSM. Anche il neonato sigillo elettronico come detto nei capitoli precedenti, avrà sicuramente un impiego diffuso. La nuova frontiera è costituita dalla raccolta delle sottoscrizioni dei pazienti. Per questi

ultimi, l'avvento delle firme grafometriche effettuate con i tablet e le penne elettroniche, ha costituito un grande interesse da parte del mondo della sanità. L'impiego di tablet e penne grafometriche permette a qualunque persona di sottoscrivere un documento con un gesto che è analogo a quanto fino ad ora con le penne e la carta. Ovviamente il supporto su cui viene fatto non è un foglio di carta e quindi particolare attenzione andrà posta nella realizzazione ergonomica della postazione e del programma che presenta il documento al paziente.

Uno degli aspetti più importanti da tenere in considerazione nell'ambito sanitario, è la disomogeneità dell'alfabetizzazione informatica dei fruitori del sistema, ovvero i pazienti. Questo è dovuto a vari motivi ma uno dei più importanti che gioca un ruolo fondamentale è l'età; ci vorrà ancora qualche generazione perché una persona considerata anziana sia abituata ad utilizzare il computer e strumenti tecnologici come i tablet ed i telefoni. In questo senso, l'adozione delle firme grafometriche permette anche a questo tipo di pazienti di utilizzarli senza particolari ostacoli.
Un altro degli aspetti da tenere in considerazione vista la facilità di spostamento delle persone degli ultimi anni, è la provenienza del paziente. Come è noto e ricordato più volte in questo documento, le firme elettroniche hanno normazione differente nei vari paesi, anche se il regolamento eIDAS, quantomeno per il mercato Europeo, tende a diminuire questi effetti.
Questi strumenti possono essere coinvolti in processi aziendali di raccolta delle firme elettroniche olografe, sia di tipo semplice (FES) che d tipo avanzato (FEA). L'impiego di firme di tipo Avanzato porta con sé un valore giuridico di forma scritta e per la natura delle firme FEA, anche notevoli vantaggi in termini di forza probatoria. I processi FEA di tipo grafometrico, per il rispetto delle regole tecniche del DPCM 22 febbraio 2013 e per il coinvolgimento dei dati biometrici raccolti ed inseriti nei documenti, al momento risultano più complessi da realizzare e da svolgere rispetto a quelli per le firme semplici. Spesso non è una reale complicazione, ma a volte viene vissuta come tale dagli operatori. Una di queste è sicuramente la fase di *enrollment* di un nuovo firmatario, attività che va svolta la prima volta che un paziente deve sottoscrivere un documento in quella particolare struttura, e che richiede la scansione di un documento di identità e l'accettazione delle regole di implementazione dei processi di FEA.

Molti di questi ostacoli potrebbero essere superati con una revisione e semplificazione delle regole tecniche da parte di AGID ed il ministero della sanità. Per la verità nelle regole tecniche è prevista una semplificazione proprio in ambito sanitario nell'art. 57, che prevede la raccolta del consenso all'accettazione d'uso dello strumento, certificata e certificata con una dichiarazione firmata digitalmente dal personale esercente la professione sanitaria. Essendo però il mondo delle aziende che operano in sanità piuttosto variegato, costituito da aziende pubbliche, aziende puramente private, ed aziende che operano in convenzione o parzialmente in convenzione e che il primo approccio con il paziente non avviene solitamente con un medico, vi sono ancora molte remore da parte dei direttori sanitari ed amministrativi nell'applicare questa semplificazione.

Il fatto che non vi siano regole specifiche e complete per la digitalizzazione in sanità, porta spesso le aziende a scegliere in autonomia processi di tipo FEA o FES, ispirandosi dalle procedure attualmente impiegate con i metodi cartacei tradizionali che non sempre per prassi prevedono criteri forti di identificazione o di compilazione e conservazione del documento stesso.

Ma soprattutto che prevedono un unico tipo di firma autografa con la penna analogica!

La conservazione dei documenti è anche uno dei fattori molto importanti da citare. Attualmente molte strutture sanitarie, per la conservazione del cartaceo si avvalgono di magazzini di società terze che svolgono servizi di *Document Management* su supporti tradizionali. La conservazione dei

documenti prodotti in digitale deve essere svolta necessariamente con processi di conservazione digitale a norma. La gestione digitale del documento, dalla sua produzione fino alla conservazione, per l'esigenza di rispettare i criteri di qualità, sicurezza, integrità e immodificabilità richiesta dal DPCM 13 novembre 2014 sul documento informatico, a nostro avviso, aumenterebbe la garanzia di protezione e leggibilità nel tempo. Questo con l'applicazione delle regole per la conservazione delle firme elettroniche e della loro verificabilità nel tempo. Anche evolvendo verso quanto previsto sul tema dalla *Long Term Data Preservation* nel regolamento eIDAS.

Su tutti questi argomenti è stata emessa anche una Circolare AgID n. 1/2018 del 24/gennaio/2018 sulle "Linee guida per la Dematerializzazione del Consenso Informato in Diagnostica per Immagini" che ha analizzato la realizzazione in un ambito ristretto, come quello appunto della diagnostica per immagini.

7.5 Articolo 60 del DPCM 22 febbraio 2013

Fin dalla sua pubblicazione in Gazzetta Ufficiale, l'articolo 60 del DPCM 22 febbraio 2013 posto nel Titolo V ove vengono descritte le regole tecniche per la costruzione di una firma FEA, destò perplessità e preoccupazioni per l'implementazione di questo tipo di firme.

Questo articolo stabilisce, nel suo unico comma, che "*La firma elettronica avanzata realizzata in conformità con le disposizioni delle presenti regole tecniche, è utilizzabile limitatamente ai rapporti giuridici intercorrenti tra il sottoscrittore e il soggetto di cui all'art. 55, comma 2, lettera a)*" ove il soggetto di cui all'art. 55, comma 2, lettera a) è il soggetto proponente la soluzione di FEA.

Detto in altre parole, la firma elettronica FEA, raccolta con la soluzione dell'azienda Acme SpA dal soggetto firmatario Mario Rossi, ha valore limitatamente ai documenti di Acme SpA che trattano di Mario Rossi.

Data la natura tecnologicamente neutrale dell'implementazione delle firme FEA, prevista anche dal regolamento europeo eIDAS, è facilmente immaginabile e comprensibile il ragionamento che ha portato all'introduzione di questo articolo: impedire possibili contestazioni su documenti e firme raccolte con soluzioni di terzi non completamente conosciute dai proprietari dei documenti, ma soprattutto l'assenza nel DPCM di una procedura che, dato un documento firmato con FEA, ne permetta la verifica della validità della firma a terzi. Dove i terzi sono ad esempio i destinatari del documento. Quest'ultimo aspetto è molto importante ed è strettamente correlato ai temi tecnici discussi in precedenza.
Uno scenario in cui questo aspetto diventa rilevante è ad esempio quello della presentazione di documentazione o istanze verso la PA o comunque verso gli uffici di una azienda. Un documento inviato dal soggetto mittente, firmato con firma digitale, è verificabile dal destinatario, mentre un documento firmato con firma FEA (ma anche FES) no.
Vi sono molti altri scenari in cui vengono fatti sottoscrivere documenti di terzi da soggetti da essi incaricati. Basti pensare alle relazioni di intermediazione di prodotti finanziari ed assicurativi, oppure le attività di rappresentanza e compravendita. Un accordo tra le parti, per permettere di utilizzare la soluzione di FEA del mandatario da parte del mandante permetterebbe di superare i limiti di questo articolo ma richiede una negoziazione tra le parti non sempre di facile natura, soprattutto richiederebbe una valutazione del processo di FEA per una sua eventuale accettazione dal mandante che lo dovrà adottare come processo proprio, proposto da altri.

Per favorire ciò, sarebbe auspicabile una attività di regolamentazione da parte di AgID nell'ambito di quanto vigente nell'articolo 61, comma 6 del DPCM 22 febbraio 2013 (stesura di specifiche Linee Guida) che permetta di delineare profili dei processi e delle soluzioni di FEA, in modo che per le aziende proponenti sia più semplice stabilire le regole di adozione. Per esemplificare: l'impresa di assicurazione A permette di usare la soluzione di FEA dei brokers, purché sia del profilo XX. Anche questo approccio però, seppur semplificativo, non dipanerebbe comunque l'impedimento causato dall'articolo in questione, molto sentito dal mercato e spesso motivo di abbandono della decisione di digitalizzare i processi da parte delle aziende di piccole dimensioni o dai professionisti.
Ad una analisi poco tecnica ma molto pratica dell'articolo 60, non c'è corrispondenza a quanto accade oggi nella prassi di questi processi organizzativi svolti in modo tradizionale cartaceo, se non eventualmente in ambito PA. In quest'ultimo la presentazione di documentazione ed istanze svolge spesso processi che debbono essere verificabili anche con procedure di protocollo. Ma in ambito ad esempio di scenari B2B o B2C cartacei tradizionali, il mandante affida al mandatario anche l'onere di garantire la bontà, qualità ed affidabilità delle dichiarazioni raccolte dai terzi sui documenti, ivi comprese l'identificazione e le firme a penna.
Non solo: spesso le aziende si affidano a processi in cui i documenti che gli vengono sottoposti dai terzi sono copie elettroniche di cartacei, formate con qualsivoglia applicazione o programma, sempre più spesso foto fatte con il cellulare. In questo caso di certo non si può parlare di possibilità di verifica delle firme da parte del destinatario, o ancor peggio della bontà ed affidabilità ed immodificabilità del documento originale cartaceo di cui la copia non può portare traccia.

8. Interoperabilità delle firme e dei sigilli nel regolamento eIDAS

È noto che il procedimento di verifica di una firma qualificata può portare a un diagnostico di "firma non valida" senza che l'estensore della verifica abbia maggiori dettagli su questa spiacevole situazione.
Perché la firma non è valida? Perché il documento sottoscritto non è integro, perché la crittografia non è conforme alla normativa piuttosto che i formati utilizzati per la firma elettronica avanzata non sono conformi alle specifiche o banalmente perché qualche bit non è impostato in modo corretto?
Una novità che possiamo già considerare molto importante e significativa è costituita dalla più recente emissione di specifiche tecniche nell'ambito della realizzazione delle previsioni del regolamento eIDAS.
Infatti, dobbiamo ricordare che in questo regolamento, tra i servizi fiduciari sono compresi anche quelli per la creazione, la verifica e convalida di firme elettroniche, sigilli elettronici o validazioni temporali elettroniche.
All'interno del medesimo regolamento sono stabiliti specificamente i requisiti per la convalida delle firme elettroniche qualificate (articolo 32).
Quest'ultima norma è piuttosto strutturata e prevede che il processo di convalida di una firma elettronica qualificata conferma la validità di una tale firma purché siano soddisfatti una serie di requisiti.
In particolare:

- il certificato associato alla firma fosse, al momento della firma, un certificato qualificato di firma elettronica conforme all'allegato I di eIDAS;
- il certificato qualificato è stato rilasciato da un prestatore di servizi fiduciari qualificato ed è valido al momento della firma;

- i dati di convalida siano corrispondenti con quelli trasmessi alla parte facente affidamento sulla certificazione;
- l'insieme unico di dati che rappresenta il firmatario nel certificato sia correttamente trasmesso alla parte facente affidamento sulla certificazione;
- l'impiego di un eventuale pseudonimo sia chiaramente indicato alla parte facente affidamento sulla certificazione, se uno pseudonimo era utilizzato al momento della firma;
- la firma elettronica sia stata creata da un dispositivo per la creazione di una firma elettronica qualificata;
- l'integrità dei dati firmati non sia stata compromessa;
- i requisiti base di una firma elettronica avanzata fossero soddisfatti al momento della firma:

Il regolamento eIDAS stabilisce nel medesimo articolo che il sistema utilizzato per convalidare la firma elettronica qualificata fornisce alla parte facente affidamento sulla certificazione (la persona fisica o giuridica che fa affidamento su un'identificazione elettronica o su un servizio fiduciario) il risultato corretto del processo di convalida e le consente di rilevare eventuali questioni attinenti alla sicurezza.
Il regolamento eIDAS stabilisce regole anche per il servizio di convalida qualificato delle firme elettroniche qualificate che può essere prestato solo da un soggetto qualificato e, nota particolare, consente alle parti facenti affidamento sulla certificazione di ricevere il risultato del processo di convalida in un modo automatizzato che sia affidabile ed efficiente e rechi la firma elettronica avanzata o il sigillo elettronico avanzato del prestatore del servizio di convalida qualificato.
Al lettore non sarà sfuggito il fatto che la messa in opera di questa normativa fa nascere il grafologo digitale ovvero un soggetto qualificato che convalida "legalmente" le sottoscrizioni e quindi soggetto a vigilanza tramite gli organismi nazionali notificati (in Italia è l'AgID e per i dispositivi di firma l'OCSI presso il Ministero dello Sviluppo Economico).
Questo soggetto firmando o sigillando la convalida della firma (o sigillo) posta a verifica si assume la responsabilità della convalida della sottoscrizione.
Queste circostanze hanno attivato in ETSI il classico procedimento di standardizzazione che ha, alla data prodotto i documenti seguenti:

TR 119 100 v1.1.1 Guidance on the use of standards or signature creation and validation.

TS 119 101 v1.1.1 Policy and security requirements for applications for signature creation and signature validation.
TS 119 102-1 v1.2.1 Procedures for Creation and Validation of AdES Digital Signatures, Part 1: Creation and Validation.

TS 119 102-2 v1.1.1 Procedures for Creation and Validation of AdES Digital Signatures, Part 2: Signature Validation Report.

TS 119 441 v1.1.1 Policy requirements for TSP providing signature validation services.

Un elevato numero di standard è stato pubblicato da ETSI per definire I formati dei certificati e delle firme elettroniche avanzate. Questo particolare aspetto non è oggetto del presente articolo.
Ci occupiamo invece della tematica della verifica e convalida delle firme alla luce di questi standard appena puntualmente indicati.

Affinché questi standard siano pienamente applicabili in conformità al regolamento eIDAS si dovrà attendere la pubblicazione della specifica decisione di esecuzione della Commissione europea.
Naturalmente gli Stati membri possono procedere autonomamente applicando gli standard senza che questo sia impedito da alcuna normativa.
Le policy contenuta nella specifica 119 441 sono la base per il procedimento di qualifica dello specifico prestatore di servizi fiduciari.
Di particolare rilevanza e novità è invece la specifica 119 102-1 che in modo articolato e dettagliato fornisce le metodologie per generare, verificare e convalidare le firme.
La specifica di 79 pagine è molto complessa e conferma sostanzialmente gli aspetti ben noti nella generazione della firma in linea con il nostro CAD. È comunque apprezzabile che tutti gli elementi che coinvolgono la sottoscrizione siano definiti e descritti (Es. il documento da sottoscrivere, la presentazione di questo al sottoscrittore, gli attributi della sottoscrizione, ecc.).
Decisamente innovativa è l'introduzione nella convalida della firma di un modello di riferimento ben specificato.
Nell'ambito del procedimento di verifica si stabiliscono tre stati di verifica:

TOTAL-PASSED: nel caso che i controlli crittografici (compresi i controlli delle impronte dei documenti a qualsiasi titolo calcolate sugli oggetti) abbiano esito positivo insieme alle politiche di convalida della firma.

TOTAL-FAILED: nel caso i controlli precedenti falliscano ovvero il certificato digitale non è valido al momento della sottoscrizione o perché la firma non è conforme ai formati stabiliti negli standard di base per quanto attiene ai componenti di formazione dei formati stessi.

INDETERMINATE: quando non ci si trova in nessuno degli stati precedenti.

Questi nuovi paradigmi consentono un nuovo approccio alla verifica della firma. Certamente dobbiamo continuare a verificare che il documento sottoscritto sia integro, che il firmatario sta utilizzando un certificato valido o che sono soddisfatti alcuni specifici requisiti della firma come, ad esempio, l'appartenenza del firmatario ad un ordine professionale.
Gli stati della convalida devono essere dettagliati in modo standard nel report di convalida e ogni decisione operativa è comunque predefinita e deve essere conforme ad una precisa regola stabilita in questa specifica.
Questa metodologia consente di migliorare il procedimento attuale applicato dai prestatori di servizi fiduciari attualmente qualificati in Italia (ma anche in Europa). Allo stato attuale si applicano le regole di dettaglio AgID (le regole tecnologiche contenute nelle deliberazioni e determine, peraltro da aggiornare in ottica comunitaria) e gli standard sui blocchi base di costruzione dei documenti firmati (CAdES, PAdES e XAdES).
In questo nuovo contesto europeo la verifica di una firma è un'operazione vincolante, su regole precise e comportamenti errati o fraudolenti comportano sanzioni anche economiche come per tutti i servizi fiduciari qualificati.
Oggi le verifiche vengono condotte sulla base di inevitabili interpretazioni dei certificatori (che ricordiamo sono qualificati solo per l'emissione di certificati qualificati e validazioni temporali) con il risultato di avere diagnostici di "firma non valida" senza avere informazioni specifiche sulla natura del problema.
Sarebbe molto positivo se l'AgID, anticipando i tempi, cominciasse a sviluppare le specifiche Linee Guida consentendo un grande salto di qualità e incremento di efficienza al mercato nazionale che

costituisce ampiamente il maggiore utilizzatore europeo e mondiale di firme digitali con circa 21 milioni di certificati qualificati attivi (fonte AgID).
Per completezza concludiamo precisando che i meccanismi previsti per la convalida dei sigilli elettronici qualificati sono analoghi a quelli delle firme.

9. Considerazioni finali

Come abbiamo visto, nonostante i 20 anni passati dalle prime regole tecniche sulle sottoscrizioni stabilite con il DPCM 8 febbraio 1999 la ruota continua a girare e le tecnologie di riferimento continuano a mutare modificando ecosistema e punti di riferimento.
Nel 2019 la sottoscrizione qualificata ha raggiunto una diffusione elevatissima con oltre 21.000.000 di certificati qualificati di sottoscrizione dei quali circa l'85% è installato per applicazioni di firma remota; questa tipologia di sottoscrizione è stata utilizzata sopra il miliardo di volte. Anche le marche temporali rilasciate hanno raggiunto e superato ampiamente un paio di miliardi. Più recente e meno diffuso l'utilizzo del sigillo qualificato.
La FEA realizzata con tecnologia grafometrica ha raggiunto decine di migliaia di postazioni, anche in mobilità, nel mondo assicurativo, bancario e industriale. Meno diffusa lo è nella pubblica amministrazione dove si sta puntando su SPID, CIE 3.0 e CNS.
Nel breve e medio periodo ci possiamo aspettare la crescita dell'utilizzo del sigillo qualificato (quello semplice è utilizzato nella fatturazione elettronica) e lo sviluppo del rapporto tra le identità digitali gestite con SPID e la CIE 3.0 considerando anche il loro status id identità europea notificata.
Al momento di pubblicazione di questo documento stanno per essere pubblicate le Linee guida per la cosiddetta "firma con SPID" a seguito di quanto stabilito nell'articolo 20, comma 1-bis del CAD vigente.
Per l'efficacia giuridica della forma scritta il Legislatore nazionale ha introdotto i registri distribuiti e gli smart contract. Quindi anche la blockchain comincia a occupare spazi nelle questioni dell'identità, dell'integrità e imputabilità delle transazioni e dei documenti e della validazione temporale.
Il dubbio che rimane è se l'innovazione deve essere preceduta dalla *compliance* normativa che poi ne limita l'evoluzione in un periodo dove è inevitabile che la tecnologia evolve a una velocità tale che il Legislatore non può seguire.

10. Bibliografia e Linkografia

[1] Decreto legislativo, 7 marzo 2005, n. 82 e successive modificazioni, Codice dell'amministrazione digitale.

[2] Regolamento UE n. 910/2014 del Parlamento Europeo e del Consiglio del 23 luglio 2014, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE.

[3] ENISA, Security guidelines on the appropriate use of qualified electronic seals. Version 2.0. December 2016.

[4] A cura di Francesco Delfini e Giusella Finocchiaro, Identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno. Commento al Regolamento UE 910/2014. G. Giappichelli Editore, 2017.

https://www.agendadigitale.eu/documenti/firma-digitale-cose-come-funziona-e-come-ottenerla/

https://www.agendadigitale.eu/documenti/spid-e-firma-digitale-che-cambiera-con-le-nuove-norme/

https://www.agendadigitale.eu/documenti/firme-elettroniche-un-decalogo-la-risposta-a-dieci-dubbi-ricorrenti/

https://www.agendadigitale.eu/documenti/firma-elettronica-cose-e-le-differenze-tra-firma-digitale-semplice-qualificata-certificata/

https://www.agendadigitale.eu/documenti/firma-elettronica-avanzata-grafometrica-sicurezza-interoperabilita-e-periziabilita/

http://cantieripadigitale.it/it/2018/08/27/sigillo-elettronico-casi-duso/

http://cantieripadigitale.it/it/2018/06/22/documenti-sigillo-elettronico-caratteristiche-possibili-utilizzi/

http://cantieripadigitale.it/it/2018/05/29/documenti-digitali-perche-identita-firma-questione-aperta/

Appendice

A.1 Esempi di sigillo elettronico qualificato

ARUBAPEC

```
   0 1840: SEQUENCE {
   4 1304:   SEQUENCE {
   8    3:     [0] {
  10    1:       INTEGER 2
        :       }
  13    8:     INTEGER 31 07 21 E2 7B 48 F3 6A
  23   13:     SEQUENCE {
  25    9:       OBJECT IDENTIFIER
        :         sha256WithRSAEncryption (1 2 840 113549 1 1 11)
        :         (PKCS #1)
  36    0:       NULL
        :       }
  38  186:     SEQUENCE {
  41   11:       SET {
  43    9:         SEQUENCE {
  45    3:           OBJECT IDENTIFIER countryName (2 5 4 6)
        :             (X.520 DN component)
  50    2:           PrintableString 'IT'
        :           }
        :         }
  54   25:       SET {
  56   23:         SEQUENCE {
  58    3:           OBJECT IDENTIFIER localityName (2 5 4 7)
        :             (X.520 DN component)
  63   16:           UTF8String 'Ponte San Pietro'
        :           }
        :         }
  81   23:       SET {
  83   21:         SEQUENCE {
  85    3:           OBJECT IDENTIFIER organizationName (2 5 4 10)
        :             (X.520 DN component)
  90   14:           UTF8String 'Actalis S.p.A.'
        :           }
        :         }
 106   26:       SET {
 108   24:         SEQUENCE {
 110    3:           OBJECT IDENTIFIER '2 5 4 97'
 115   17:           UTF8String 'VATIT-03358520967'
        :           }
        :         }
 134   41:       SET {
 136   39:         SEQUENCE {
 138    3:           OBJECT IDENTIFIER organizationalUnitName (2 5 4 11)
        :             (X.520 DN component)
 143   32:           UTF8String 'Qualified Trust Service Provider'
        :           }
        :         }
 177   48:       SET {
```

```
179   46:         SEQUENCE {
181    3:           OBJECT IDENTIFIER commonName (2 5 4 3)
        :             (X.520 DN component)
186   39:           UTF8String 'Actalis EU Qualified Certificates CA G2'
        :           }
        :         }
        :       }
227   30:     SEQUENCE {
229   13:       UTCTime 24/01/2019 09:01:22 GMT
244   13:       UTCTime 23/04/2023 09:01:22 GMT
        :       }
259  114:     SEQUENCE {
261   11:       SET {
263    9:         SEQUENCE {
265    3:           OBJECT IDENTIFIER countryName (2 5 4 6)
        :             (X.520 DN component)
270    2:           PrintableString 'IT'
        :           }
        :         }
274   23:       SET {
276   21:         SEQUENCE {
278    3:           OBJECT IDENTIFIER organizationName (2 5 4 10)
        :             (X.520 DN component)
283   14:           UTF8String 'Actalis S.p.A.'
        :           }
        :         }
299   26:       SET {
301   24:         SEQUENCE {
303    3:           OBJECT IDENTIFIER '2 5 4 97'
308   17:           UTF8String 'VATIT-03358520967'
        :           }
        :         }
327   21:       SET {
329   19:         SEQUENCE {
331    3:           OBJECT IDENTIFIER commonName (2 5 4 3)
        :             (X.520 DN component)
336   12:           UTF8String 'DEMO SIGILLO'
        :           }
        :         }
350   23:       SET {
352   21:         SEQUENCE {
354    3:           OBJECT IDENTIFIER dnQualifier (2 5 4 46)
        :             (X.520 DN component)
359   14:           PrintableString '66404001509450'
        :           }
        :         }
        :       }
375  290:     SEQUENCE {
379   13:       SEQUENCE {
381    9:         OBJECT IDENTIFIER rsaEncryption (1 2 840 113549 1 1 1)
        :           (PKCS #1)
392    0:         NULL
        :         }
394  271:       BIT STRING, encapsulates {
399  266:         SEQUENCE {
403  257:           INTEGER
        :             00 99 A3 CB D5 FC 10 D4    ........
```

```
         :             88 1E C2 3A 5B 0B 6A 37    ...:[.j7
         :             BB A7 76 32 86 7B 02 4E    ..v2.{.N
         :             F9 3C 91 85 9B 4D B9 06    .<...M..
         :             DC B7 BF C3 3E C2 31 A5    ....>.1.
         :             66 24 21 A7 AB 88 97 7B    f$!....{
         :             9D F3 9D F9 03 1A B7 62    .......b
         :             85 03 58 9E 4C C5 E3 DC    ..X.L...
         :             D7 13 13 4A 96 D5 FF 03    ...J....
         :             0D AC A9 64 35 81 D6 2B    ...d5..+
         :             C8 38 9D 34 C3 94 85 00    .8.4....
         :             88 CE C2 72 2D 9E BA BF    ...r-...
         :             7C 4A B4 3B B0 49 F5 34    |J.;.I.4
         :             19 79 DC 42 67 65 AB 1C    .y.Bge..
         :             F8 46 56 56 9E 62 23 48    .FVV.b#H
         :             E1 C4 54 0A B3 20 E0 0D
         :                     [ Another 129 bytes skipped ]
 664    3:           INTEGER 65537
         :           }
         :         }
         :       }
 669  639:     [3] {
 673  635:       SEQUENCE {
 677  133:         SEQUENCE {
 680    8:           OBJECT IDENTIFIER authorityInfoAccess (1 3 6 1 5 5 7
1 1)
         :             (PKIX private extension)
 690  121:           OCTET STRING, encapsulates {
 692  119:             SEQUENCE {
 694   59:               SEQUENCE {
 696    8:                 OBJECT IDENTIFIER caIssuers (1 3 6 1 5 5 7 48
2)
         :                   (PKIX subject/authority info access
descriptor)
 706   47:                 [6]
         :                   'http://cacert.actalis.it/certs/actalis-
eidas-g2'
         :                 }
 755   56:               SEQUENCE {
 757    8:                 OBJECT IDENTIFIER ocsp (1 3 6 1 5 5 7 48 1)
         :                   (PKIX)
 767   44:                 [6]
         :                   'http://ocsp08.actalis.it/va/actalis-eidas-
g2'
         :                 }
         :               }
         :             }
         :           }
 813   29:         SEQUENCE {
 815    3:           OBJECT IDENTIFIER subjectKeyIdentifier (2 5 29 14)
         :             (X.509 extension)
 820   22:           OCTET STRING, encapsulates {
 822   20:             OCTET STRING
         :               50 EE 7F D6 63 FC 67 10    P...c.g.
         :               40 C0 55 E2 6F 1A 2F 15    @.U.o./.
         :               3D CD E4 47                =..G
         :             }
         :           }
```

```
 844   31:         SEQUENCE {
 846    3:           OBJECT IDENTIFIER authorityKeyIdentifier (2 5 29 35)
        :             (X.509 extension)
 851   24:           OCTET STRING, encapsulates {
 853   22:             SEQUENCE {
 855   20:               [0]
        :                 22 3C CB 58 A8 2F AF CE    "<.X./..
        :                 29 E2 2F DA FD 0D 42 35    )./...B5
        :                 D4 74 BA 12                .t..
        :               }
        :             }
        :           }
 877   26:         SEQUENCE {
 879    3:           OBJECT IDENTIFIER issuerAltName (2 5 29 18)
        :             (X.509 extension)
 884   19:           OCTET STRING, encapsulates {
 886   17:             SEQUENCE {
 888   15:               [1] 'info@actalis.it'
        :               }
        :             }
        :           }
 905  218:         SEQUENCE {
 908    8:           OBJECT IDENTIFIER qcStatements (1 3 6 1 5 5 7 1 3)
        :             (PKIX private extension)
 918  205:           OCTET STRING, encapsulates {
 921  202:             SEQUENCE {
 924    8:               SEQUENCE {
 926    6:                 OBJECT IDENTIFIER etsiQcsCompliance (0 4 0
1862 1 1)
        :                   (ETSI TS 101 862 qualified certificates)
        :                 }
 934   11:               SEQUENCE {
 936    6:                 OBJECT IDENTIFIER
        :                   etsiQcsRetentionPeriod (0 4 0 1862 1 3)
        :                   (ETSI TS 101 862 qualified certificates)
 944    1:                 INTEGER 20
        :                 }
 947    8:               SEQUENCE {
 949    6:                 OBJECT IDENTIFIER etsiQcsQcSSCD (0 4 0 1862 1
4)
        :                   (ETSI TS 101 862 qualified certificates)
        :                 }
 957   19:               SEQUENCE {
 959    6:                 OBJECT IDENTIFIER '0 4 0 1862 1 6'
 967    9:                 SEQUENCE {
 969    7:                   OBJECT IDENTIFIER '0 4 0 1862 1 6 2'
        :                   }
        :                 }
 978  145:               SEQUENCE {
 981    6:                 OBJECT IDENTIFIER '0 4 0 1862 1 5'
 989  134:                 SEQUENCE {
 992   65:                   SEQUENCE {
 994   59:                     IA5String
        :                     'https://www.actalis.it/repository/actalis-
qualif'
        :                     '-pds-it.pdf'
1055    2:                     PrintableString 'it'
```

```
         :                     }
1059   65:                   SEQUENCE {
1061   59:                     IA5String
         :                     'https://www.actalis.it/repository/actalis-
qualif'
         :                     '-pds-en.pdf'
1122    2:                     PrintableString 'en'
         :                     }
         :                   }
         :                 }
         :               }
         :             }
         :           }
1126  102:         SEQUENCE {
1128    3:           OBJECT IDENTIFIER certificatePolicies (2 5 29 32)
         :             (X.509 extension)
1133   95:           OCTET STRING, encapsulates {
1135   93:             SEQUENCE {
1137    9:               SEQUENCE {
1139    7:                 OBJECT IDENTIFIER '0 4 0 194112 1 3'
         :                 }
1148   80:               SEQUENCE {
1150    6:                 OBJECT IDENTIFIER '1 3 159 11 1 1'
1158   70:                 SEQUENCE {
1160   68:                   SEQUENCE {
1162    8:                     OBJECT IDENTIFIER cps (1 3 6 1 5 5 7 2 1)
         :                       (PKIX policy qualifier)
1172   56:                     IA5String
         :                     'https://www.actalis.it/repository/actalis-
qualif'
         :                     '-cps.pdf'
         :                     }
         :                   }
         :                 }
         :               }
         :             }
         :           }
1230   64:         SEQUENCE {
1232    3:           OBJECT IDENTIFIER cRLDistributionPoints (2 5 29 31)
         :             (X.509 extension)
1237   57:           OCTET STRING, encapsulates {
1239   55:             SEQUENCE {
1241   53:               SEQUENCE {
1243   51:                 [0] {
1245   49:                   [0] {
1247   47:                     [6]
         :                     'http://crl08.actalis.it/va/actalis-eidas-
g2/crl'
         :                     }
         :                   }
         :                 }
         :               }
         :             }
         :           }
1296   14:         SEQUENCE {
1298    3:           OBJECT IDENTIFIER keyUsage (2 5 29 15)
         :             (X.509 extension)
```

```
1303    1:            BOOLEAN TRUE
1306    4:            OCTET STRING, encapsulates {
1308    2:              BIT STRING 6 unused bits
        :                '10'B (bit 1)
        :              }
        :            }
        :          }
        :        }
        :      }
1312   13:    SEQUENCE {
1314    9:      OBJECT IDENTIFIER sha256WithRSAEncryption (1 2 840 113549
1 1 11)
        :        (PKCS #1)
1325    0:      NULL
        :      }
1327  513:    BIT STRING
        :      8B 82 A9 72 B0 AD 6A 05    ...r..j.
        :      91 03 1A 04 A8 4E A0 01    .....N..
        :      46 96 0D 38 72 02 A4 AB    F..8r...
        :      D5 AD 91 C8 D2 C6 EB C7    ........
        :      A4 F1 F9 AC 1D F5 54 E9    ......T.
        :      FF E7 CA C8 D3 EB 96 90    ........
        :      27 6F DD E2 D2 39 B0 7C    'o...9.|
        :      E0 FF DD 83 C0 1D 27 6B    ......'k
        :      C5 F5 50 87 EA DF 39 D4    ..P...9.
        :      3F 7D 68 5E 88 D8 97 12    ?}h^....
        :      76 BE C6 B5 7F 0F 8D DD    v.......
        :      06 66 35 E3 06 74 90 53    .f5..t.S
        :      B7 8D 74 2A 4E 3A CA A1    ..t*N:..
        :      39 B4 7F 67 DF 16 E2 64    9..g...d
        :      19 7C 79 8D 0E E5 DA 7A    .|y....z
        :      A0 CB AC 21 D5 2B 17 38
        :              [ Another 384 bytes skipped ]
        :    }
```

INFOCERT

```
   0 2064: SEQUENCE {
   4 1528:   SEQUENCE {
   8    3:     [0] {
  10    1:       INTEGER 2
        :       }
  13    2:     INTEGER 29864
  17   13:     SEQUENCE {
  19    9:       OBJECT IDENTIFIER
        :         sha256WithRSAEncryption (1 2 840 113549 1 1 11)
  30    0:       NULL
        :       }
  32  168:     SEQUENCE {
  35   11:       SET {
  37    9:         SEQUENCE {
  39    3:           OBJECT IDENTIFIER countryName (2 5 4 6)
  44    2:           PrintableString 'IT'
        :           }
        :         }
  48   24:       SET {
  50   22:         SEQUENCE {
  52    3:           OBJECT IDENTIFIER organizationName (2 5 4 10)
  57   15:           UTF8String 'InfoCert S.p.A.'
        :           }
        :         }
  74   41:       SET {
  76   39:         SEQUENCE {
  78    3:           OBJECT IDENTIFIER organizationalUnitName (2 5 4 11)
  83   32:           UTF8String 'Qualified Trust Service Provider'
        :           }
        :         }
 117   26:       SET {
 119   24:         SEQUENCE {
 121    3:           OBJECT IDENTIFIER '2 5 4 97'
 126   17:           UTF8String 'VATIT-07945211006'
        :           }
        :         }
 145   56:       SET {
 147   54:         SEQUENCE {
 149    3:           OBJECT IDENTIFIER commonName (2 5 4 3)
 154   47:           UTF8String
        :             'InfoCert Qualified Electronic Signature CA 3 CL'
        :           }
        :         }
        :       }
 203   30:     SEQUENCE {
 205   13:       UTCTime 10/01/2019 08:43:10 GMT
 220   13:       UTCTime 10/01/2022 00:00:00 GMT
        :       }
 235  108:     SEQUENCE {
 237   23:       SET {
 239   21:         SEQUENCE {
 241    3:           OBJECT IDENTIFIER commonName (2 5 4 3)
 246   14:           UTF8String 'InfoCert eSeal'
        :           }
        :         }
```

```
262   11:       SET {
264    9:         SEQUENCE {
266    3:           OBJECT IDENTIFIER countryName (2 5 4 6)
271    2:           PrintableString 'IT'
       :           }
       :         }
275   24:       SET {
277   22:         SEQUENCE {
279    3:           OBJECT IDENTIFIER organizationName (2 5 4 10)
284   15:           UTF8String 'InfoCert S.p.A.'
       :           }
       :         }
301   26:       SET {
303   24:         SEQUENCE {
305    3:           OBJECT IDENTIFIER '2 5 4 97'
310   17:           UTF8String 'VATIT-07945211006'
       :           }
       :         }
329   14:       SET {
331   12:         SEQUENCE {
333    3:           OBJECT IDENTIFIER stateOrProvinceName (2 5 4 8)
338    5:           UTF8String 'Italy'
       :           }
       :         }
       :       }
345  290:     SEQUENCE {
349   13:       SEQUENCE {
351    9:         OBJECT IDENTIFIER rsaEncryption (1 2 840 113549 1 1 1)
362    0:         NULL
       :         }
364  271:       BIT STRING, encapsulates {
369  266:         SEQUENCE {
373  257:           INTEGER
       :             00 EB 8B F9 30 91 3B 03 47 E9 34 DD 89 0A 4E A5
       :             FC BE D8 F6 2F B4 F9 63 6D 70 98 E1 FD A2 72 6D
       :             F6 42 91 D3 82 F4 C0 F3 48 99 09 E1 56 1C 62 0A
       :             7B 24 3E E9 71 F0 11 0D 39 14 89 79 BD 2E FB B9
       :             B3 6C DC DA A8 7E D7 E7 3B 58 E8 7F 7D C7 31 55
       :             16 25 6F CB 03 26 A6 D0 B5 C0 CF 92 77 A8 5C FF
       :             09 37 C0 F0 15 9E E8 E9 00 51 0D 91 B0 BB 8F C7
       :             7B 06 D3 CC 88 CE B2 51 77 72 03 0D CB AA 84 55
       :                     [ Another 129 bytes skipped ]
634    3:           INTEGER 65537
       :           }
       :         }
       :       }
639  893:     [3] {
643  889:       SEQUENCE {
647    9:         SEQUENCE {
649    3:           OBJECT IDENTIFIER basicConstraints (2 5 29 19)
654    2:           OCTET STRING, encapsulates {
656    0:             SEQUENCE {}
       :             }
       :           }
658  260:         SEQUENCE {
662    3:           OBJECT IDENTIFIER cRLDistributionPoints (2 5 29 31)
667  252:           OCTET STRING, encapsulates {
```

```
 670  249:              SEQUENCE {
 673  246:                SEQUENCE {
 676  243:                  [0] {
 679  240:                    [0] {
 682   41:                      [6]
       :                      'http://crlcl.infocert.it/ca3/qc/CRL01.crl'
 725  194:                      [6]
       :
'ldap://ldapcl.infocert.it/cn%3DInfoCert%20Qualif'
       :
'ied%20Electronic%20Signature%20CA%203%20CL%20CRL'
       :
'01,ou%3DQualified%20Trust%20Service%20Provider,o'
       :
'%3DINFOCERT%20SPA,c%3DIT?certificateRevocationLi'
       :                      'st'
       :                      }
       :                    }
       :                  }
       :                }
       :              }
 922  111:          SEQUENCE {
 924    8:            OBJECT IDENTIFIER authorityInfoAccess (1 3 6 1 5 5 7
1 1)
 934   99:            OCTET STRING, encapsulates {
 936   97:              SEQUENCE {
 938   42:                SEQUENCE {
 940    8:                  OBJECT IDENTIFIER ocsp (1 3 6 1 5 5 7 48 1)
 950   30:                  [6] 'http://ocspcl.ca3.infocert.it/'
       :                  }
 982   51:                SEQUENCE {
 984    8:                  OBJECT IDENTIFIER caIssuers (1 3 6 1 5 5 7 48
2)
 994   39:                  [6] 'http://certcl.infocert.it/ca3/qc/CA.crt'
       :                  }
       :                }
       :              }
1035  101:          SEQUENCE {
1037    3:            OBJECT IDENTIFIER certificatePolicies (2 5 29 32)
1042   94:            OCTET STRING, encapsulates {
1044   92:              SEQUENCE {
1046    9:                SEQUENCE {
1048    7:                  OBJECT IDENTIFIER '0 4 0 194112 1 3'
       :                  }
1057   79:                SEQUENCE {
1059    6:                  OBJECT IDENTIFIER '1 3 76 36 1 1 46'
1067   69:                  SEQUENCE {
1069   67:                    SEQUENCE {
1071    8:                      OBJECT IDENTIFIER cps (1 3 6 1 5 5 7 2 1)
1081   55:                      IA5String
       :
'http://www.firma.infocert.it/documentazione/manu'
       :                      'ali.php'
       :                      }
       :                    }
```

```
         :                 }
         :               }
         :             }
         :           }
1138  132:         SEQUENCE {
1141    8:           OBJECT IDENTIFIER qcStatements (1 3 6 1 5 5 7 1 3)
1151  120:           OCTET STRING, encapsulates {
1153  118:             SEQUENCE {
1155    8:               SEQUENCE {
1157    6:                 OBJECT IDENTIFIER etsiQcsCompliance (0 4 0
1862 1 1)
         :                 }
1165    8:               SEQUENCE {
1167    6:                 OBJECT IDENTIFIER etsiQcsQcSSCD (0 4 0 1862 1
4)
         :                 }
1175   11:               SEQUENCE {
1177    6:                 OBJECT IDENTIFIER
         :                   etsiQcsRetentionPeriod (0 4 0 1862 1 3)
1185    1:                 INTEGER 20
         :                 }
1188   19:               SEQUENCE {
1190    6:                 OBJECT IDENTIFIER '0 4 0 1862 1 6'
1198    9:                 SEQUENCE {
1200    7:                   OBJECT IDENTIFIER '0 4 0 1862 1 6 2'
         :                   }
         :                 }
1209   62:               SEQUENCE {
1211    6:                 OBJECT IDENTIFIER '0 4 0 1862 1 5'
1219   52:                 SEQUENCE {
1221   50:                   SEQUENCE {
1223   44:                     IA5String
         :                     'https://www.firma.infocert.it/pdf/PKI-
DS.pdf'
1269    2:                     PrintableString 'EN'
         :                     }
         :                   }
         :                 }
         :               }
         :             }
         :           }
1273   14:         SEQUENCE {
1275    3:           OBJECT IDENTIFIER keyUsage (2 5 29 15)
1280    1:           BOOLEAN TRUE
1283    4:           OCTET STRING, encapsulates {
1285    2:             BIT STRING 6 unused bits
         :               '10'B (bit 1)
         :             }
         :           }
1289  213:         SEQUENCE {
1292    3:           OBJECT IDENTIFIER authorityKeyIdentifier (2 5 29 35)
1297  205:           OCTET STRING, encapsulates {
1300  202:             SEQUENCE {
1303   20:               [0]
         :                 54 33 C0 1D 99 98 90 FD FB 09 94 67 F8 1D CC
09
         :                 52 A1 0F A6
```

```
1325  174:               [1] {
1328  171:                 [4] {
1331  168:                   SEQUENCE {
1334   11:                     SET {
1336    9:                       SEQUENCE {
1338    3:                         OBJECT IDENTIFIER countryName (2 5 4
6)
1343    2:                         PrintableString 'IT'
         :                         }
         :                       }
1347   24:                     SET {
1349   22:                       SEQUENCE {
1351    3:                         OBJECT IDENTIFIER organizationName (2
5 4 10)
1356   15:                         UTF8String 'InfoCert S.p.A.'
         :                         }
         :                       }
1373   41:                     SET {
1375   39:                       SEQUENCE {
1377    3:                         OBJECT IDENTIFIER
         :                           organizationalUnitName (2 5 4 11)
1382   32:                         UTF8String 'Qualified Trust Service
Provider'
         :                         }
         :                       }
1416   26:                     SET {
1418   24:                       SEQUENCE {
1420    3:                         OBJECT IDENTIFIER '2 5 4 97'
1425   17:                         UTF8String 'VATIT-07945211006'
         :                         }
         :                       }
1444   56:                     SET {
1446   54:                       SEQUENCE {
1448    3:                         OBJECT IDENTIFIER commonName (2 5 4 3)
1453   47:                         UTF8String
         :                       'InfoCert Qualified Electronic Signature CA
3 CL'
         :                         }
         :                       }
         :                     }
         :                   }
         :                 }
1502    1:               [2] 01
         :                 }
         :             }
         :           }
1505   29:         SEQUENCE {
1507    3:           OBJECT IDENTIFIER subjectKeyIdentifier (2 5 29 14)
1512   22:           OCTET STRING, encapsulates {
1514   20:             OCTET STRING
         :               41 2B DC 47 20 45 4A ED C4 DE 27 80 75 B0 E6 E2
         :               30 A0 CB 39
         :             }
         :           }
         :         }
         :       }
         :     }
```

```
1536   13:   SEQUENCE {
1538    9:     OBJECT IDENTIFIER sha256WithRSAEncryption (1 2 840 113549
1 1 11)
1549    0:     NULL
        :     }
1551  513:   BIT STRING
        :     46 C4 47 28 A6 5C D4 05 A5 23 0C DF C3 8A 4D AD
        :     A7 6E 58 48 DC E7 AE F2 41 6D B8 3D 2F 94 7D 1C
        :     94 E5 5E 51 49 CD B6 02 CC 15 CC D6 D1 89 46 18
        :     A7 9A 58 A1 41 04 9B 12 9D 73 B3 83 DB F1 E7 74
        :     EB 9E 7D 45 40 77 85 06 B5 07 E6 FA 15 ED FD F5
        :     05 9F 4B FF CB DB 3A 72 0C DF 8E AA 7E CF 4E 9F
        :     47 1F 1A E8 89 AF FC DD 9B 48 89 71 FF 99 27 97
        :     CD F7 D4 A7 DB 66 A3 D1 1F 4C 3B B3 09 5A A2 02
        :             [ Another 384 bytes skipped ]
        :   }
```

NAMIRIAL

```
SEQUENCE (3 elem)
  SEQUENCE (8 elem)
    [0] (1 elem)
      INTEGER 2
    INTEGER (61 bit) 1341379375139122088
    SEQUENCE (2 elem)
      OBJECT IDENTIFIER 1.2.840.113549.1.1.11 sha256WithRSAEncryption
(PKCS #1)
      NULL
    SEQUENCE (5 elem)
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.3 commonName (X.520 DN component)
          UTF8String Namirial EU Qualified CA
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.11 organizationalUnitName (X.520 DN
component)
          UTF8String Trust Service Provider
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.10 organizationName (X.520 DN
component)
          UTF8String Namirial S.p.A.
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.97
          UTF8String VATIT-02046570426
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.6 countryName (X.520 DN component)
          PrintableString IT
    SEQUENCE (2 elem)
      UTCTime 2018-09-26 12:29:37 UTC
      UTCTime 2024-12-25 12:29:37 UTC
    SEQUENCE (5 elem)
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.46 dnQualifier (X.520 DN component)
          PrintableString ID99
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.3 commonName (X.520 DN component)
          UTF8String NAMIRIAL DEMO ORG
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.10 organizationName (X.520 DN
component)
          UTF8String NAMIRIAL DEMO ORG
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.97
          UTF8String VATIT-12345678901
      SET (1 elem)
        SEQUENCE (2 elem)
```

```
          OBJECT IDENTIFIER 2.5.4.6 countryName (X.520 DN component)
          PrintableString IT
    SEQUENCE (2 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 1.2.840.113549.1.1.1 rsaEncryption (PKCS #1)
        NULL
      BIT STRING (1 elem)
        SEQUENCE (2 elem)
          INTEGER (2048 bit)
279077371572673817401967927303698866286855256176737566763546095474617…
          INTEGER 65537
    [3] (1 elem)
      SEQUENCE (7 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 1.3.6.1.5.5.7.1.1 authorityInfoAccess (PKIX
private extension)
          OCTET STRING (1 elem)
            SEQUENCE (2 elem)
              SEQUENCE (2 elem)
                OBJECT IDENTIFIER 1.3.6.1.5.5.7.48.2 caIssuers (PKIX
subject/authority info access descriptor)
                [6] https://docs.namirialtsp.com/documents/NamCA4K.crt
              SEQUENCE (2 elem)
                OBJECT IDENTIFIER 1.3.6.1.5.5.7.48.1 ocsp (PKIX)
                [6] http://ocsp.namirialtsp.com/ocsp/certstatus
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.29.14 subjectKeyIdentifier (X.509
extension)
          OCTET STRING (1 elem)
            OCTET STRING (20 byte)
DCFEFCCAF5CCAD8D179961824A5C07D60FA2FAF7
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.29.35 authorityKeyIdentifier (X.509
extension)
          OCTET STRING (1 elem)
            SEQUENCE (1 elem)
              [0] (20 byte) 63B8CDB84952E5E7097B578CFB7A410E41AA7859
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 1.3.6.1.5.5.7.1.3 qcStatements (PKIX private
extension)
          OCTET STRING (1 elem)
            SEQUENCE (5 elem)
              SEQUENCE (1 elem)
                OBJECT IDENTIFIER 0.4.0.1862.1.1 etsiQcsCompliance (ETSI
TS 101 862 qualified certificates)
              SEQUENCE (2 elem)
                OBJECT IDENTIFIER 0.4.0.1862.1.3 etsiQcsRetentionPeriod
(ETSI TS 101 862 qualified certificates)
                INTEGER 20
              SEQUENCE (1 elem)
                OBJECT IDENTIFIER 0.4.0.1862.1.4 etsiQcsQcSSCD (ETSI TS
101 862 qualified certificates)
              SEQUENCE (2 elem)
                OBJECT IDENTIFIER 0.4.0.1862.1.6
                SEQUENCE (1 elem)
                  OBJECT IDENTIFIER 0.4.0.1862.1.6.2
              SEQUENCE (2 elem)
```

```
                OBJECT IDENTIFIER 0.4.0.1862.1.5
                SEQUENCE (2 elem)
                  SEQUENCE (2 elem)
                    IA5String
https://docs.namirialtsp.com/documents/PDS/PDS_en.pdf
                    PrintableString en
                  SEQUENCE (2 elem)
                    IA5String
https://docs.namirialtsp.com/documents/PDS/PDS_it.pdf
                    PrintableString it
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.29.32 certificatePolicies (X.509
extension)
          OCTET STRING (1 elem)
            SEQUENCE (3 elem)
              SEQUENCE (2 elem)
                OBJECT IDENTIFIER 1.3.6.1.4.1.36203.1.2.3
                SEQUENCE (1 elem)
                  SEQUENCE (2 elem)
                    OBJECT IDENTIFIER 1.3.6.1.5.5.7.2.1 cps (PKIX policy
qualifier)
                    IA5String https://docs.namirialtsp.com/
              SEQUENCE (1 elem)
                OBJECT IDENTIFIER 0.4.0.194112.1.3
              SEQUENCE (1 elem)
                OBJECT IDENTIFIER 0.4.0.2042.1.2
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.29.31 cRLDistributionPoints (X.509
extension)
          OCTET STRING (1 elem)
            SEQUENCE (1 elem)
              SEQUENCE (1 elem)
                [0] (1 elem)
                  [0] (1 elem)
                    [6] http://crl.namirialtsp.com/CA4K.crl
        SEQUENCE (3 elem)
          OBJECT IDENTIFIER 2.5.29.15 keyUsage (X.509 extension)
          BOOLEAN true
          OCTET STRING (1 elem)
            BIT STRING (2 bit) 01
  SEQUENCE (2 elem)
    OBJECT IDENTIFIER 1.2.840.113549.1.1.11 sha256WithRSAEncryption (PKCS
#1)
    NULL
  BIT STRING (4096 bit)
100001101000001000101001100001101101111100010100001010000011111001001…
```

Allegato I

1. Riferimenti al sigillo elettronico nel regolamento eIDAS.

Nel seguito sono riportati tutti i riferimenti al sigillo elettronico nel regolamento europeo 910/2014.

Riferimenti nelle premesse:

(50) Poiché attualmente le autorità competenti negli Stati membri utilizzano formati diversi di firme elettroniche avanzate per firmare elettronicamente i loro documenti, occorre garantire che almeno alcuni formati di firma elettronica possano essere supportati tecnicamente dagli Stati membri allorché ricevono documenti firmati elettronicamente. Analogamente, allorché le autorità competenti negli Stati membri fanno uso di sigilli elettronici, occorre garantire che supportino almeno alcuni formati di ***sigillo elettronico avanzato****.*

(58) 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.*

(59) È opportuno che i ***sigilli elettronici*** *fungano da prova dell'emissione di un documento elettronico da parte di una determinata persona giuridica, dando la certezza dell'origine e dell'integrità del documento stesso.*

(60) I prestatori di servizi fiduciari che rilasciano certificati qualificati di ***sigilli elettronici*** *dovrebbero attuare le misure necessarie per poter stabilire l'identità della persona giuridica rappresentante la persona fisica cui è fornito il certificato qualificato di* ***sigillo elettronico****, quando tale identificazione è necessaria a livello nazionale nel contesto di procedimenti giudiziari o amministrativi.*

(61) È opportuno che il presente regolamento garantisca la conservazione a lungo termine delle informazioni, al fine di assicurare la validità giuridica delle firme elettroniche e dei ***sigilli elettronici*** *nel lungo periodo, garantendo che possano essere convalidati indipendentemente da futuri mutamenti tecnologici.*

(62) Al fine di garantire la sicurezza della validazione temporale elettronica qualificata, il presente regolamento dovrebbe richiedere l'uso di un ***sigillo elettronico avanzato*** *o di una firma elettronica avanzata o di altri metodi equivalenti. È prevedibile che l'innovazione produca nuove tecnologie in grado di assicurare alla validazione temporale un livello di sicurezza equivalente. Ogni qualvolta venga utilizzato un metodo diverso dal* ***sigillo elettronico avanzato*** *o dalla firma elettronica avanzata, dovrebbe spettare al prestatore di servizi fiduciari qualificato dimostrare, nella relazione di valutazione di conformità, che tale metodo garantisce un livello equivalente di sicurezza e soddisfa gli obblighi previsti nel presente regolamento.*

Nell'articolato del regolamento troviamo quanto segue:

Articolo 3 - Definizioni

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;

26) «sigillo elettronico avanzato», un sigillo elettronico che soddisfi i requisiti sanciti all'articolo 36;

27) «sigillo elettronico qualificato», un sigillo elettronico avanzato creato da un dispositivo per la creazione di un sigillo elettronico qualificato e basato su un certificato qualificato per sigilli elettronici;

28) «dati per la creazione di un sigillo elettronico», i dati unici utilizzati dal creatore del sigillo elettronico per creare un sigillo elettronico;

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;

30) «certificato qualificato di sigillo elettronico», un certificato di sigillo elettronico che è rilasciato da un prestatore di servizi fiduciari qualificato ed è conforme ai requisiti di cui all'allegato III;

31) «dispositivo per la creazione di un sigillo elettronico», un software o hardware configurato utilizzato per creare un sigillo elettronico;

32) «dispositivo per la creazione di un sigillo elettronico qualificato», un dispositivo per la creazione di un sigillo elettronico che soddisfa mutatis mutandis i requisiti di cui all'allegato II;

40) «dati di convalida», dati utilizzati per convalidare una firma elettronica o un sigillo elettronico;

41) «convalida», il processo di verifica e conferma della validità di una firma o di un sigillo elettronico.

Riferimenti al sigillo elettronico si trovano

nell'articolo 24, paragrafo 1, lettera c)

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

nell'articolo 33, paragrafo 1, lettera b)

*b) consente alle parti facenti affidamento sulla certificazione di ricevere il risultato del processo di convalida in un modo automatizzato che sia affidabile ed efficiente e rechi la firma elettronica avanzata o **il sigillo elettronico avanzato** del prestatore del servizio di convalida qualificato.*

La sezione 5 di del regolamento eIDAS è completamente dedicata ai sigilli elettronici:

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.

Articolo 36

Requisiti dei sigilli elettronici avanzati

Un sigillo elettronico avanzato soddisfa i seguenti requisiti:

a) è connesso unicamente al creatore del sigillo;

b) è idoneo a identificare il creatore del sigillo;

c) è creato mediante dati per la creazione di un sigillo elettronico che il creatore del sigillo elettronico può, con un elevato livello di sicurezza, usare sotto il proprio controllo per creare sigilli elettronici; e

d) è collegato ai dati cui si riferisce in modo da consentire l'identificazione di ogni successiva modifica di detti dati.

Articolo 37

Sigilli elettronici nei servizi pubblici

1. Se uno Stato membro richiede un sigillo elettronico avanzato per poter utilizzare i servizi online offerti da un organismo del settore pubblico, o per suo conto, tale Stato membro riconosce i sigilli elettronici avanzati, i sigilli elettronici avanzati basati su un certificato qualificato di sigillo elettronico e i sigilli elettronici qualificati che almeno siano nei formati o utilizzino i metodi definiti negli atti di esecuzione di cui al paragrafo 5.

2. Se uno Stato membro richiede un sigillo elettronico avanzato basato su un certificato qualificato per poter utilizzare i servizi online offerti da un organismo del settore pubblico, o per suo conto, tale Stato membro riconosce i sigilli elettronici avanzati basati su un certificato qualificato e i sigilli elettronici qualificati che almeno siano nei formati o utilizzino i metodi definiti negli atti di esecuzione di cui al paragrafo 5.

3. Gli Stati membri non richiedono, per l'utilizzo transfrontaliero in un servizio online offerto da un organismo del settore pubblico, un sigillo elettronico dotato di un livello di garanzia di sicurezza più elevato di quello del sigillo elettronico qualificato.

4. La Commissione può, mediante atti di esecuzione, stabilire i numeri di riferimento delle norme applicabili ai sigilli elettronici avanzati. Si presume che i requisiti per i sigilli elettronici avanzati di cui ai paragrafi 1 e 2 del presente articolo e all'articolo 36 siano rispettati ove un sigillo elettronico avanzato soddisfi dette norme. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.IT L 257/104 Gazzetta ufficiale dell'Unione europea 28.8.2014

5. Entro il 18 settembre 2015, e tenendo conto delle prassi, delle norme e degli atti giuridici dell'Unione vigenti, la Commissione, mediante atti di esecuzione, definisce i formati di riferimento dei sigilli elettronici avanzati o i metodi di riferimento nel caso in cui siano utilizzati formati alternativi. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.

Articolo 38

Certificati qualificati di sigilli elettronici

1. I certificati qualificati di sigilli elettronici soddisfano i requisiti di cui all'allegato III.

2. I certificati qualificati di sigilli elettronici non sono soggetti a requisiti obbligatori oltre ai requisiti di cui all'allegato III.

3. I certificati qualificati di sigilli elettronici possono includere attributi specifici aggiuntivi non obbligatori. Tali attributi non pregiudicano l'interoperabilità e il riconoscimento dei sigilli elettronici qualificati.

4. Qualora un certificato qualificato di un sigillo elettronico 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 dei certificati qualificati di sigilli elettronici:

a) in caso di temporanea sospensione di un certificato qualificato di sigillo elettronico, 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. La Commissione può, mediante atti di esecuzione, stabilire i numeri di riferimento delle norme applicabili ai certificati qualificati di sigilli elettronici. Si presume che i requisiti di cui all'allegato III siano stati rispettati ove un certificato qualificato di sigillo elettronico risponda a dette norme. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.

Articolo 39

Dispositivi per la creazione di un sigillo elettronico qualificato

1. L'articolo 29 si applica mutatis mutandis ai requisiti per i dispositivi per la creazione di un sigillo elettronico qualificato.

2. L'articolo 30 si applica mutatis mutandis alla certificazione dei dispositivi per la creazione di un sigillo elettronico qualificato.

3. L'articolo 31 si applica mutatis mutandis alla pubblicazione di un elenco di dispositivi per la creazione di un sigillo elettronico qualificato certificati.

Articolo 40

Convalida e conservazione dei sigilli elettronici qualificati

Gli articoli 32, 33 e 34 si applicano mutatis mutandis alla convalida e alla conservazione dei sigilli elettronici qualificati.IT 28.8.2014 Gazzetta ufficiale dell'Unione europea L 257/105

Poi il sigillo viene ulteriormente referenziato nell'articolo 42, paragrafo 1, lettera c)

c) è apposta mediante una firma elettronica avanzata o sigillata con un sigillo elettronico avanzato del prestatore di servizi fiduciari qualificato o mediante un metodo equivalente.

Nell'articolo 44, paragrafo 1, lettera d)

d) l'invio e la ricezione dei dati sono garantiti da una firma elettronica avanzata o da un sigillo elettronico avanzato di un prestatore di servizi fiduciari qualificato in modo da escludere la possibilità di modifiche non rilevabili dei dati;

Nell'allegato I lettere g), h)

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;

Infine, l'Allegato III è dedicato ai Requisiti per i certificati qualificati dei sigilli elettronici.

ALLEGATO III

REQUISITI PER I CERTIFICATI QUALIFICATI DEI SIGILLI ELETTRONICI

I certificati qualificati dei sigilli elettronici contengono:

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

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 appaiono nei documenti ufficiali,*
- *per una persona fisica: il nome della persona;*

c) almeno il nome del creatore del sigillo e, se del caso, il numero di registrazione quali appaiono nei documenti ufficiali;

d) i dati di convalida del sigillo elettronico che corrispondono ai dati per la creazione di un sigillo elettronico;

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 un sigillo elettronico connessi ai dati di convalida del sigillo elettronico siano ubicati in un dispositivo per la creazione di un sigillo elettronico qualificato, un'indicazione appropriata di questo fatto, almeno in una forma adatta al trattamento automatizzato.IT 28.8.2014 Gazzetta ufficiale dell'Unione europea L 257/113.