



eBook_ Gestione di un processo di Firma Grafometrica e/o Firma Elettronica Avanzata in assenza di operatore o con operatore presente da remoto con strumenti di Unified Communication

Gruppo di Lavoro AIFAG 2014-03

Gestione di un processo di Firma Grafometrica e/o Firma Elettronica Avanzata in assenza di operatore o con operatore presente da remoto con strumenti di Unified Communication

Coordinatore: *Stefano Flaim (HiT Internet Technologies S.p.A)*

Hanno contribuito alla redazione del documento finale:

Stefano Caporali (Postel S.p.A.)

Roberta Chelotti (Svib S.r.l.)

Marco Cuniberti (Studio Legale Costa Cuniberti)

Sandro Fontana (GT50 S.r.l.)

Giovanni Manca (Comitato Scientifico AIFAG)

Mauro Mattioli (Unimatica S.p.A.)

Franco Ruggieri (Consiglio Direttivo AIFAG)

Andrea Sasseti (Aruba Pec S.p.A.)

Eugenio Stucchi (Direttore del Comitato Scientifico AIFAG e notaio)



eBook_ Gestione di un processo di Firma Grafometrica e/o Firma Elettronica Avanzata in assenza di operatore o con operatore presente da remoto con strumenti di Unified Communication



eBook_ Gestione di un processo di Firma Grafometrica e/o Firma Elettronica Avanzata in assenza di operatore o con operatore presente da remoto con strumenti di Unified Communication

Sommario

1	Introduzione	4
1.1	Prefazione	4
1.2	Firma Elettronica Avanzata grafometrica.....	4
1.3	Motivazione dello studio	5
1.4	Sessioni di Unified Communication	7
2	Definizioni ed abbreviazioni	8
3	Processo di Firma Grafometrica e dematerializzazione	8
4	Elementi di Unified Communication utili a supporto della raccolta di una firma FG.....	12
4.1	Tipologie di sessioni.....	13
4.2	Sicurezza delle sessioni e registrazione	13
4.3	Scenario di sottoscrizione dei documenti con firma FG	16
5	Scenari di Firma Grafometrica remota	17
5.1	Operatore e firmatario utilizzano strumenti di Unified Communication	18
5.2	Interazioni per la firma del documento	21
5.3	Possibili scenari di impiego	22
6	Criticità di gestione del processo di raccolta di una FG remota	25
6.1	Proposta di semplificazione: informativa FEA in modalità elettronica.....	28
6.2	Proposta di chiarimento: processo di identificazione via webcam	29
6.3	Proposta di integrazione: inserimento nell'xml extended delle informazioni del totem	30
7	Prospettive future.....	31
8	Bibliografia e riferimenti	34



eBook_ Gestione di un processo di Firma Grafometrica e/o Firma Elettronica Avanzata in assenza di operatore o con operatore presente da remoto con strumenti di Unified Communication

1 Introduzione

1.1 Prefazione

L'associazione AIFAG (Associazione Italiana Firma elettronica Avanzata, Grafometrica e biometrica) ha avviato nel novembre del 2014 un Gruppo di Lavoro sul tema della raccolta di Firme Grafometriche con modalità remote, allo scopo di creare una bozza di proposta di best practice e studi in merito alle peculiarità operative, organizzative e di sicurezza. Il prodotto del gruppo di lavoro è questo documento, rilasciato nel giugno del 2015.

Le domanda di partenza del GdL è stata: la norma ci aiuta e comprende anche il caso di raccolta di una FEA tra due persone non presenti contemporaneamente nello stesso luogo, e quindi de-visu?

Sono stati presi in considerazione i tre aspetti fondamentali di un processo di questo tipo:



1.2 Firma Elettronica Avanzata Grafometrica

Si richiama l'attenzione sulla definizione di Firma Elettronica Avanzata (nel prosieguo FEA) che è un particolare tipo di firma elettronica prevista dall'ordinamento italiano ed europeo, che permette ad una persona fisica di apporre su un documento informatico alcune informazioni, che sono di sua esclusiva proprietà, e che tramite la ricombinazione con dati univoci del documento ne permettono la verificabilità nel tempo.



eBook_ Gestione di un processo di Firma Grafometrica e/o Firma Elettronica Avanzata in assenza di operatore o con operatore presente da remoto con strumenti di Unified Communication

La firma cosiddetta Grafometrica (nel proseguo FG) o “scritta a mano”, è una firma elettronica prodotta da una persona tramite l’impiego di penne elettroniche e tablet o schermi abilitati, che permette di raccogliere varie informazioni del tratto e non solo quelle grafiche.

Tramite le FG è possibile raccogliere firme di tipo FEA su documenti informatici.

Il GDL si è occupato in questa prima fase dello studio ed in questo documento delle FEA di tipo Grafometrico.

Per ulteriori dettagli sulla raccolta di FG si rimanda allo studio del GDL 2014-001 di AIFAG che ne approfondisce gli aspetti tecnologici e normativi ed anche le tematiche di interoperabilità dei documenti con essa sottoscritti.

1.3 Motivazione dello studio

Una soluzione documentale digitale che preveda l’apposizione di Firme Elettroniche Avanzate, anche di tipo Grafometrico, consta di diversi task o step che devono essere svolti dagli attori, operatore di front-end e firmatari, rispettando più normative a partire dall’identificazione del soggetto firmatario fino a quella delle firme elettroniche e della conservazione a norma dei documenti digitali.

L’emanazione delle norme tecniche riguardanti le Firme Elettroniche con il DPCM 22 febbraio 2013, ha scatenato una legittima richiesta da parte del mercato di poter raccogliere Firme Elettroniche (nel proseguo FE) nelle più disparate modalità.

In particolare la FEA nella sua implementazione come Firma Grafometrica FG, è quella su cui il mercato ha prestato maggior attenzione in quanto viene vista come una firma molto “naturale” seppur svolta tramite strumenti informatici, perché si possono adoperare device quali penne elettroniche con cui effettuare dei gesti su schermo, che ricordano molto da vicino ciò che accade con le penne ad inchiostro e la carta.

La digitalizzazione del documento e della firma, combinate con la possibilità di trasmettere le informazioni tramite reti informatiche, hanno subito fatto emergere come possibilità concreta la modalità di creazione del documento e raccolta delle firme in modalità remota. Ovvero, la fattibilità di effettuare in forma digitale da sedi remote quei processi che,



eBook_ Gestione di un processo di Firma Grafometrica e/o Firma Elettronica Avanzata in assenza di operatore o con operatore presente da remoto con strumenti di Unified Communication

attualmente con mezzi analogici, prevedono l'incontro fisico tra le parti coinvolte dal legame giuridico del documento.

Si pensi ad esempio allo scenario tipico cliente-fornitore ove le sedi siano dislocate su tutto il territorio italiano e ove nel rapporto tra le parti vi sia la necessità di sottoscrivere contratti, accordi, deleghe, ...anche di una certa rilevanza giuridica.

Questo presuppone l'impiego di strumenti idonei all'utilizzo di Unified Communications nell'interazione tra attori di processi. Strumenti informatici che sono sempre più integrati ed a disposizione degli utenti dei computer sia in ambito professionale che retail. Dispositivi quali webcam, microfoni e cuffie fanno parte da qualche anno della dotazione standard di computer portatili, tablet e device mobili quali gli smartphone.

Osservando il mercato dell'hardware si può rilevare la stessa tendenza per gli strumenti adatti alla raccolta di firme FEA di tipo grafometrico e cioè la disponibilità di penne elettroniche ed EMR già a bordo dei computer o dei device mobili. Possiamo pensare che questa prassi delle aziende produttrici di hardware, abbinata alla produzione di penne esterne e tablet USB di facile reperibilità da abbinare ai device che ne sono sprovvisti, prosegua con sempre maggior diffusione.



eBook_ Gestione di un processo di Firma Grafometrica e/o Firma Elettronica Avanzata in assenza di operatore o con operatore presente da remoto con strumenti di Unified Communication

1.4 Sessioni di Unified Communication

Generalmente si è abituati ad utilizzare il termine videoconferenza per indicare una sessione di comunicazione Audio-Video tra due o più persone.

Questa può avvenire tramite l'impiego di strumenti hardware/software integrati e dedicati o tramite l'impiego di computer e programmi che governano webcam, microfono e cuffie in modo da favorire la comunicazione in varie modalità.

Per questo sempre più spesso si parla di Unified Communication, ovvero Comunicazione Unificata. I tool di UC mettono a disposizione in un'unica interfaccia modalità una volta riservate a differenti programmi quali ad esempio la chat o l'istant messaging e lo scambio file.

Nel caso delle sessioni UC con hw e sw dedicati, vengono impiegati strumenti molto somiglianti a dei videotelefoni o centraline, che sono posizionate in sale riunioni o sulle scrivanie esclusivamente in ambito professionale. In questi scenari spesso si impiegano canali trasmissivi dedicati e con protocolli differenti da quelli tradizionali utilizzati su internet o in intranet.

Il GDL si è occupato prevalentemente, in questa prima fase dello studio ed in questo documento, degli strumenti di UC che impiegano software utilizzabili tramite computer tradizionali, device mobili quali tablet e smartphone.



eBook_ Gestione di un processo di Firma Grafometrica e/o Firma Elettronica Avanzata in assenza di operatore o con operatore presente da remoto con strumenti di Unified Communication

2 Definizioni ed abbreviazioni

FE: **Firme Elettroniche**

FES: **Firma Elettronica Semplice**, intendendo una FE senza la valenza di FEA, Firma Elettronica Qualificata o Firma Digitale

FEA: **Firma Elettronica Avanzata**, un particolare tipo di firma elettronica definito in Regolamento UE 910/2014 e nella norma italiana nel CAD e dal DPCM 22 febbraio 2013

FG: **Firma Grafometrica**, termine con cui genericamente si identifica un particolare tipo di firma elettronica avanzata basato sulla rilevazione di parametri biometrici del firmatario, idonei al suo riconoscimento, anche ex post, quali: posizione xy, pressione, accelerazione, velocità,

UC: **Unified Communication**, in generale si intende con questo termine, l'insieme di strumenti hw/sw e di telecomunicazioni atti a consentire la comunicazione tra soggetti remoti condividendo i canali voce/video/chat/presence/condivisione file/condivisione desktop/....

EMR: **Electro-Magnetic Resonance**, termine con cui vengono indicati i dispositivi elettronici di rilevazione del movimento delle penne elettroniche sugli schermi dei tablet grafometrici o dei tablet PC con penne integrate

VESA: **Video Electronics Standards Association** associazione di standardizzazione di imprese produttrici di monitor e non solo. Con il termine attacco VESA si identificano standard di ancoraggio ai mobili, dei monitor e televisori

VPN: **Virtual Private Network**, in telecomunicazioni una VPN o Virtual Private Network è una rete di telecomunicazioni privata, instaurata tra soggetti che utilizzano un sistema di trasmissione pubblico e condiviso, come per esempio Internet. Normalmente una VPN è resa sicura mediante meccanismi di cifratura.

Processo di Firma Grafometrica e dematerializzazione



eBook_ Gestione di un processo di Firma Grafometrica e/o Firma Elettronica Avanzata in assenza di operatore o con operatore presente da remoto con strumenti di Unified Communication

Nella realizzazione di un processo di Firma Grafometrica (FG) che si voglia qualificare come soluzione di Firma Elettronica Avanzata (FEA) dovranno essere rispettati i capisaldi fissati dal CAD (Codice dell'Amministrazione Digitale - Dlgs 82/2005) e dalle regole Tecniche relative (DPCM 22 febbraio 2013).

Queste norme fissano il quadro della gestione dei documenti digitali e gli adempimenti necessari perché una soluzione informatica possa rientrare nelle definizioni di FEA, quindi acquistare tutti i caratteri e le valenze legali corrispondenti.

Trattandosi poi di un processo che coinvolge il trattamento di dati biometrici comportamentali, cioè la registrazione del gesto di firma, si dovranno tenere in considerazione anche le prescrizioni in materia del Garante dei dati personali (Provvedimento n. 513/2014 del 12 novembre 2014). In particolare questo provvedimento fissa alcune caratteristiche aggiuntive della soluzione che, se soddisfatte, possono esimere il soggetto che la realizza dal richiedere approvazione specifica al Garante tramite una verifica preliminare.

Senza voler entrare in questo documento nell'esame di tutti gli aspetti derivanti da questo quadro normativo, ci si limiterà ad esaminare come avviene tipicamente un processo di FG, cercando in particolare di evidenziare i punti che potrebbero presentare differenze in un processo remoto.

Le Regole Tecniche fissano una serie di obblighi per il soggetto erogatore della soluzione di FEA che comprendono tra l'altro l'obbligo di (Art. 57 - 1 a) *"identificare in modo certo l'utente tramite un valido documento di riconoscimento, informarlo in merito agli esatti termini e condizioni relative all'uso del servizio, compresa ogni eventuale limitazione dell'uso, subordinare l'attivazione del servizio alla sottoscrizione di una dichiarazione di accettazione delle condizioni del servizio da parte dell'utente"*.

Viene anche specificato (Art. 57 - 1 b) che il soggetto dovrà *"conservare per almeno venti anni copia del documento di riconoscimento e la dichiarazione [...] garantendone la disponibilità, integrità, leggibilità e autenticità"*.

Queste prescrizioni portano a dover rendere diverso il processo per l'acquisizione della prima firma grafometrica dalle eventuali sottoscrizioni successive. Tipicamente la prima volta che l'utente si avvicina alla soluzione di FG il soggetto proponente dovrà garantirsi che il suo incaricato:



eBook_ Gestione di un processo di Firma Grafometrica e/o Firma Elettronica Avanzata in assenza di operatore o con operatore presente da remoto con strumenti di Unified Communication

1. identifichi l'utente, producendo una copia del documento d'identità valido che sarà sottoposta a conservazione per 20 anni,
2. informi correttamente e con completezza l'utente sui termini e le condizioni della soluzione,
3. raccolga la sottoscrizione su una dichiarazione di accettazione, anch'essa da conservare per 20 anni.

In merito al punto 1, in un contesto di promozione della dematerializzazione quale quello in cui ci troviamo, la soluzione più coerente è tipicamente quella di acquisire la copia in formato digitale (tramite scanner o immagine fotografica) e di procedere alla conservazione sostitutiva in formato elettronico.

Anche rispetto alla dichiarazione di cui al punto 3, in molti contesti applicativi, è stato scelto di considerare sufficiente una "firma elettronica semplice" sulla dichiarazione (non potendo definirsi ancora FEA per ovvia auto-referenzialità). La firma elettronica semplice essendo in realtà una firma grafometrica apposta con la stessa tecnologia di tutte le firme successive, ma in carenza della dichiarazione stessa.

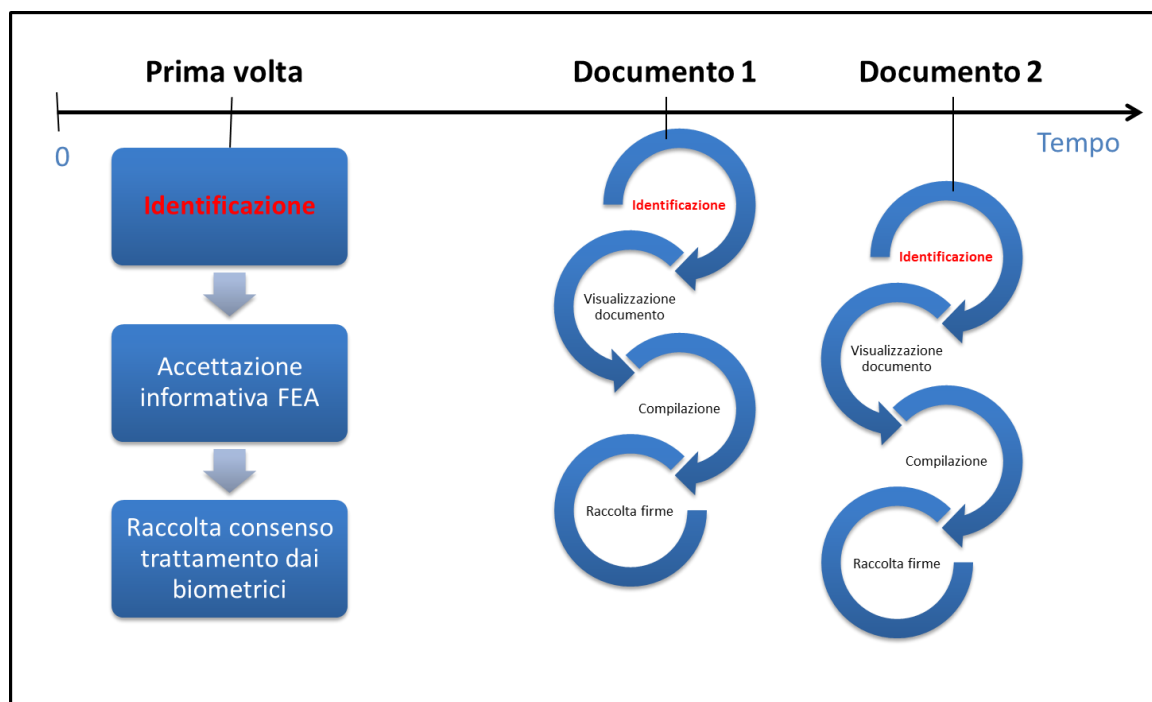
Ovviamente, laddove questo approccio non sia giudicato sufficiente, si deve ancora ricorrere all' "ultima firma cartacea", anziché partire con la "prima firma elettronica". Il documento cartaceo della dichiarazione sarà eventualmente acquisito poi con scanner per essere inviato in conservazione sostitutiva.

Avendo realizzato questo processo per l'attivazione di un rapporto con l'utente per l'uso della FG, il soggetto promotore della soluzione potrà, nella prima come nelle successive occasioni di firma di documenti, avvalersi dell'identificazione, informazione e raccolta del consenso già effettuate preliminarmente e limitare le attività a quelle specifiche della firma, in questo perfettamente analoghe ad una normale sottoscrizione autografa con carta e penna, e cioè:

- compilazione dei dati specifici per il documento alla firma (collaborazione tra l'operatore e l'utente),
- valutazione del documento finale (da parte dell'utente),
- apposizione delle firme (utente ed eventualmente operatore).



eBook_ Gestione di un processo di Firma Grafometrica e/o Firma Elettronica Avanzata in assenza di operatore o con operatore presente da remoto con strumenti di Unified Communication



Da questa descrizione appare evidente come molte delle attività componenti il processo potrebbero essere svolte anche in un contesto di UC.

In particolare sembrano essere tutte facilmente gestibili anche da remoto le attività per le firme, mentre le attività legate al primo contatto sembrano necessitare di alcuni approfondimenti, perché, come si cercherà di illustrare in seguito, vanno chiariti gli aspetti legati a:

- l'identificazione dell'utente non "de visu",
- la trasmissione della copia di documento di riconoscimento,
- la sottoscrizione della dichiarazione di consenso e sua trasmissione (solo nel caso si ritenesse opportuno acquisirla in modo cartaceo, altrimenti ricade nello scenario di FG).



eBook_ Gestione di un processo di Firma Grafometrica e/o Firma Elettronica Avanzata in assenza di operatore o con operatore presente da remoto con strumenti di Unified Communication

3 Elementi di Unified Communication utili a supporto della raccolta di una firma FG

Come già anticipato nella prefazione, si è abituati ad utilizzare il termine videoconferenza per indicare una sessione di comunicazione Audio-Video tramite il computer tra due o più persone.

Data l'evoluzione tecnologica di questi strumenti, ed alla convergenza di diverse tecniche di comunicazione digitale in un'unica suite di programmi, oramai si parla di Unified Communication ovvero Comunicazione Unificata. Con questo termine si intende in particolare l'impiego di un'unica suite di programmi che mette a disposizione diversi metodi di comunicazione tra gli attori impiegando gli stessi canali trasmissivi.

Questi canali sono le reti informatiche impiegate dai computer per la comunicazione internet o intranet ed i protocolli TCP-IP o UDP.

Alcuni di essi favoriscono la possibilità di scambiarsi informazioni e documenti a distanza tra due o più persone collegate da una relazione di conoscenza o fiducia. Questa relazione è correlata ad uno scambio reciproco di richieste di accettazione su un Dominio di Autenticazione.

Tra le metodologie di comunicazione si citano nel seguito quelle principalmente coinvolte da una sessione tipica:

- ✓ **Presence:** con questo strumento è possibile sapere lo stato di uno dei contatti cui sono collegato da una relazione di fiducia
- ✓ **Instant messaging:** con questa funzione è possibile lo scambio immediato di informazioni tra i contatti. Viene detto anche "chat"
- ✓ **Conferencing** (audio, Web and video): con questi strumenti è possibile per i contatti vedersi e parlarsi tramite la webcam, microfono e cuffie
- ✓ **Collaboration tools:** tramite strumenti quali ad esempio, condivisione del desktop, lavagne interattive condivise, file transfer, calendario condiviso...

Le parti in contatto possono scambiarsi dati e documenti da una postazione all'altra restando all'interno del perimetro applicativo del tool di videoconferenza, oppure condividere quelli di una postazione permettendo di utilizzarli dall'altra



eBook_ Gestione di un processo di Firma Grafometrica e/o Firma Elettronica Avanzata in assenza di operatore o con operatore presente da remoto con strumenti di Unified Communication

3.1 Tipologie di sessioni

Considerando gli strumenti di videocomunicazione attuali e di tipologia prevalentemente software, esistono fondamentalmente due modalità di connessione tra i partecipanti alla sessione:

1. punto a punto
2. con server centrale

Nel primo caso, tutti i programmi di UC in uso dai partecipanti si connettono uno all'altro. Nel secondo, sicuramente il più diffuso ed il più interessante, i partecipanti sono collegati ad un server che svolge diversi compiti.

Il server di UC garantisce la connettività tra gli attori della chiamata permettendogli di svolgere le seguenti tipologie di sessioni:

- I. uno a uno: rientra in questo scenario la classica videochiamata tra due persone simile alla call telefonica ma con la possibilità di impiegare anche la chat, la condivisione, il video, ...
- II. uno a molti: questo scenario denominato **Conference**, permette ad una persona detta master di contattarne molte altre e di farle interagire o solo con lui o anche tra di loro, in ogni caso moderandone l'interazione in base alle sue esigenze. Il caso tipico è la formazione in cui il docente fa da master ed i partecipanti possono interagire per alzata di mano o solo con il docente in forma privata oppure anche con tutti in forma pubblica
- III. molti a molti: questo scenario che estende la numerosità dei partecipanti potenzialmente all'infinito è denominata **Meeting**. La sessione che viene comunque avviata da una sola persona, ne coinvolge molte altre che sono però paritetiche nello scambio dei contenuti (al contrario della conference)

3.2 Sicurezza delle sessioni e registrazione

La sessione di comunicazione deve poter garantire diversi profili di sicurezza, in modo da potersi adattare ove richiesto anche a standard molto elevati. Gli elementi su cui può intervenire il sistema di Unified Communication sono principalmente tre:

1. gestione utenti e profili



eBook_ Gestione di un processo di Firma Grafometrica e/o Firma Elettronica Avanzata in assenza di operatore o con operatore presente da remoto con strumenti di Unified Communication

2. protocollo di comunicazione dei dati
3. possibilità di registrazione della sessione

La gestione utenti di un sistema di Unified Communication con server centralizzato, equivale alla gestione di User Directory di un sistema operativo. Tutti gli utenti sono censiti nel server con possibilità di associare loro differenti profili d'uso degli strumenti quali ad esempio la quantità di banda da poter utilizzare, la possibilità o meno di condividere contenuti,

L'intreccio dei permessi di comunicare tra utenti varia molto da contesto a contesto e da sistema a sistema.

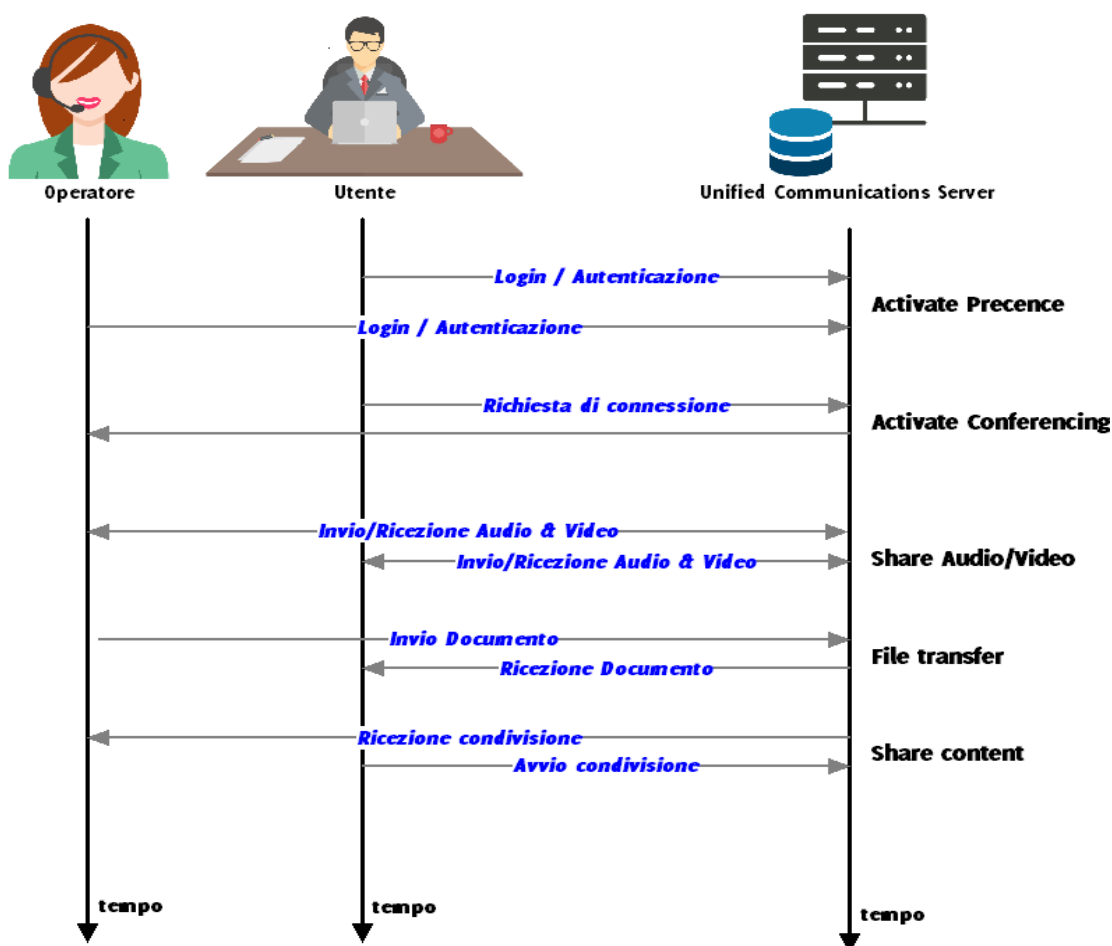
Nei sistemi di video conferenza ad uso libero, gli utenti fanno tutti parte di un unico **dominio** anche se non si conoscono e non sono automaticamente collegati tra loro. Possono creare una relazione di **trust** previa richiesta di contatto e di fiducia da far pervenire da parte di uno o dell'altro tramite una ricerca più o meno anonima tra i contatti censiti nell'intero dominio. In questo modo si crea un reticolo di collegamenti tra utenti che però si conoscono personalmente solo tra i contatti diretti.

In ogni caso la comunicazione può avvenire solo tra contatti che prima hanno manifestato ed accettato la relazione di trust.

Nei sistemi professionali, il dominio generalmente contiene utenti che sono già ritenuti degni di trust e quindi possono procedere ad instaurare una sessione di comunicazione immediatamente vedendosi già nella **presence** in modo automatico.



eBook_ Gestione di un processo di Firma Grafometrica e/o Firma Elettronica Avanzata in assenza di operatore o con operatore presente da remoto con strumenti di Unified Communication



Il server UC, a seconda delle implementazioni, può erogare i servizi in modalità condivisa tra più domini o erogarli in modo privato per un singolo dominio.

Si pensi ad esempio ad una azienda che desidera creare un dominio di utenti dei propri dipendenti: lo può creare su un server dedicato solo a loro o su un server condiviso in cloud tra più clienti. Ai fini della sicurezza, Il server in quest'ultimo caso deve garantire l'isolamento quantomeno logico tra i dati e le informazioni scambiate durante le sessioni di videocomunicazione dei singoli domini.

Una sessione di comunicazione è come una stanza riunioni tra gli attori e per questo viene spesso denominata **room**: ad una room possono accedere solo utenti registrati al dominio oppure, previa autorizzazione del gestore della sessione, si può permettere l'accesso anche



eBook_ Gestione di un processo di Firma Grafometrica e/o Firma Elettronica Avanzata in assenza di operatore o con operatore presente da remoto con strumenti di Unified Communication

ad utenti anonimi o utenti che si presentano all'accesso della room con delle credenziali atte a farsi riconoscere: nome cognome e numero di telefono, una login temporanea, ...

Durante la sessione, i dati scambiati provengono da tutti i metodi implementati nel sistema:

- audio
- video
- condivisione di contenuti in esecuzione sul computer/device
- flipchart
- messaging
- scambio file

Il server, su richiesta del gestore della sessione, può fornire un servizio di **registrazione** di tutte queste informazioni ad uso principalmente dei partecipanti salvo in casi eccezionali in cui si vuol dividerla con persone esterne.

Il protocollo di comunicazione dei dati scambiati tra i programmi client ed il server, può essere **criptato** per questioni di sicurezza.

3.3 Scenario di sottoscrizione dei documenti con firma FG

Per gli scopi dello scenario di sottoscrizione dei documenti con firme FG che verrà approfondito nel capitolo seguente e di cui si è occupato il GDL, particolare attenzione è stata posta sui seguenti elementi:

- I. autenticazione degli utenti sul dominio del server UC
- II. possibilità di condivisione dei contenuti sui PC/device
- III. limitazione del profilo d'uso degli strumenti per gli utenti che partecipano al processo di firma
- IV. cifratura del canale di comunicazione
- V. registrazione della sessione.

Questi elementi, rimappati sulle esigenze di gestione del processo di firma, permetteranno di garantire rispettivamente i seguenti aspetti:

- a. garantire che la connessione in videoconferenza stia avvenendo tra utenti noti fino ad arrivare a garantire l'identificazione certa magari in forma digitale degli stessi



eBook_ Gestione di un processo di Firma Grafometrica e/o Firma Elettronica Avanzata in assenza di operatore o con operatore presente da remoto con strumenti di Unified Communication

- b. condividere i contenuti, il che può permettere di sovrintendere il processo di firma che avviene sul PC/device remoto oppure può permettere di condividere strumenti di firma ed utilizzo del documento dalla postazione dell'operatore di backoffice
- c. gestire i profili d'uso degli utenti che, anziché non averne controllo, permette di disegnare un processo certo che garantisca l'impiego di determinate funzioni nei momenti giusti
- d. attivare la cifratura del canale che aggiunge ovvie misure di sicurezza in ambito di riservatezza delle informazioni scambiate durante la sessione e di riservatezza dei dati presenti nei documenti eventualmente sottoscritti nel caso sia avvenuta la loro firma
- e. attivare la registrazione della sessione che permette ad esempio di mettere la stessa in un sistema di conservazione a norma per dare supporto alle eventuali fasi di contenzioso che potranno verificarsi tra le parti coinvolte anche dopo diverso tempo.

4 Scenari di Firma Grafometrica remota

Come già anticipato nell'introduzione, con la frase Firma Grafometrica remota intendiamo lo scenario in cui gli attori del processo FEA, operatore di frontend e firmatario, non siano presenti contemporaneamente nello stesso luogo davanti al PC/device utilizzato per raccogliere le firme di tipo FG sui documenti informatici.

Normativamente o come definizione tecnica, non esiste questo tipo di distinzione, locale o remota, come invece accade per la firma digitale.

Come descritto nei capitoli precedenti, il processo di raccolta di una FG prevede l'interazione tra gli utenti per assolvere almeno alle seguenti azioni:

1. identificazione dei firmatari da parte del soggetto che eroga la soluzione di FG
2. raccolta delle firme FG sui documenti elettronici

In un processo FG tradizionale, il soggetto erogatore della soluzione, propone al terzo firmatario lo strumento di firma che ha scelto per il processo stesso. Questo è composto da software e hardware che lavorando in combinazione come descritto anche nel documento del GDL AIFAG 2014-001, sono in grado di raccogliere i dati legati all'esecuzione della firma, di proteggerli, di utilizzarli per la costruzione delle strutture dati della firma elettronica, ed infine di collegarli in modo univoco e verificabile nel documento.



eBook_ Gestione di un processo di Firma Grafometrica e/o Firma Elettronica Avanzata in assenza di operatore o con operatore presente da remoto con strumenti di Unified Communication

Il fatto che le due persone non si incontrino de visu, fa ipotizzare che le ipotesi di condizione d'uso degli strumenti debbano cambiare o per meglio dire, debbano essere supportate da altri strumenti quali quelli di UC che permettono di "ravvicinare" gli utenti che li usano.

Appare evidente che con il supporto della UC il processo diventi molto simile a quello tradizionale, quantomeno per l'interazione umana. Tuttavia, a seconda di come venga erogato il supporto hardware/software di firma e gestione documentale, vi possono essere delle differenze sostanziali.

Anche l'apporto video delle riprese via webcam non può garantire le stesse condizioni che vi sono di persona; a titolo di esempio si pensi al controllo di un documento di identità che non potrà avvalersi del tatto dell'operatore, né potrà garantire di avere la stessa percezione visiva essendo questa limitata dalla webcam.

La raccolta della firma FG, addirittura senza l'apporto di webcam o più in generale di software per UC, introduce un ulteriore grado di complessità in particolare in fase di identificazione, step necessario ed imposto dalle norme tecniche del DPCM 22 febbraio 2013.

In questo scenario si potrà sicuramente avvalersi di supporti tecnico-normativi forniti ad esempio dal regolamento europeo eIDAS e SPID che vengono trattati nell'ultimo capitolo di questo documento.

Il GDL per ora, ha approfondito in particolare il caso di processo presidiato con strumenti di videoconferenza.

4.1 Operatore e firmatario utilizzano strumenti di Unified Communication

In questa modalità, particolare attenzione va posta soprattutto a questi elementi:

- il programma o il componente software in grado di elaborare il documento e la firma
- un dispositivo hardware in grado di rilevare i dati biometrici comportamentali
- lo scambio del documento tra le due figure

Ipotizzando che i due protagonisti non siano davanti allo stesso computer ma ognuno su uno diverso, possiamo distinguere due possibili scenari:



eBook_ Gestione di un processo di Firma Grafometrica e/o Firma Elettronica Avanzata in assenza di operatore o con operatore presente da remoto con strumenti di Unified Communication

- A. la raccolta della firma avviene sul computer/device utilizzato dal firmatario, che è di proprietà dell'organizzazione owner della FEA. Nel prosieguo chiameremo questo scenario **TOTEM** in quanto il caso d'uso più rappresentativo è appunto una postazione remota rispetto al perimetro fisico del proponente;
- B. la raccolta della firma avviene su un computer/device utilizzato dal firmatario ma che, al contrario del totem, è di sua proprietà. Chiameremo questo scenario **BYOD** - Bring Your Own Device.

La modalità Totem è molto utile in impieghi di tipo istituzionale in cui vi sia necessità di allocare in posizione remota una "presenza" seppur virtuale di un ufficio presidabile, in luogo noto ed in qualche modo controllabile, su cui vi sia la necessità di raccogliere documenti compilati e sottoscritti da una utenza che può essere:

- Fidelizzata ed abituale, già nota
- Avventori, non noti in precedenza e alle volte senza probabilità di ritorno.

La modalità BYOD invece, è idonea per remotizzare solo una funzione organizzativa di una organizzazione, in cui vi sia la necessità di raccogliere firme su documenti da far compilare a persone dislocate sul territorio senza costringerle a muoversi per raggiungere un ufficio fisico o remotizzato con totem.

Possiamo riassumere queste necessità nella seguente Tabella 1

	Totem	BYOD
Interesse dell'azienda di avere una propria postazione remota	X	
Interesse per l'azienda a remotizzare la funzione	X	X
Controllo sull'hardware ed il sistema operativo	X	
Localizzazione geografica fissa della postazione	X	
Riduzione dei costi della postazione remota		X
Libertà d'uso degli strumenti da parte dell'utente		X



eBook_ Gestione di un processo di Firma Grafometrica e/o Firma Elettronica Avanzata in assenza di operatore o con operatore presente da remoto con strumenti di Unified Communication

Dallo studio del GDL si evidenzia che nello scenario BYOD la matrice delle responsabilità nell'espletamento del processo FG può raggiungere complessità piuttosto elevate, soprattutto tenendo presenti le limitazioni o indicazioni indotte da:

- I. art. 60 del DPCM 22 febbraio 2013, presente nelle regole tecniche sulle firme, che limita l'uso della FEA ai rapporti giuridici intercorrenti tra il sottoscrittore e il soggetto di cui all'art. 55, comma 2, lettera a)
- II. provvedimento generale del Garante in tema di biometria del 12/11/2014 che semplifica le azioni necessarie nell'adozione di procedimenti di raccolta di dati biometrici nel caso di Firme Elettroniche Avanzate di tipo grafometrico.

Si pensi al caso di un professionista dotato di un Tablet-PC con penna integrata, un software di raccolta per la FG proprio, ed eventualmente anche una MasterKey propria, che potrebbe ricevere il documento da firmare ad esempio da un suo cliente/fornitore/PA. Collegandosi con la videoconferenza all'operatore di front-end dell'organizzazione che ha disegnato un proprio processo FEA, l'utente potrebbe sottomettere in modalità elettronica un documento firmato con FG?

L'articolo 60 succitato, salvo intervenire con specifiche deleghe da parte dell'organizzazione che adotta la soluzione di FG potrebbe diventare un vincolo nell'utilizzo di strumenti hardware/software per raccogliere la firma sui propri documenti differenti da quelli da essa descritti nelle relazioni tecniche. Possiamo riassumere nella matrice rappresentata di seguito in Tabella 2, a chi, tra organizzazione e firmatario potrebbero essere in capo alcune responsabilità di compliance della soluzione, nel caso di scenari BYOD .

	Organizzazione con FG	Firmatario
Hardware + Sistema Operativo L'azienda che fa firmare il documento accetta i rischi di un hardware che potrebbe non essere adeguato oppure agisce con software in push in grado di rilevare la non conformità.		X
Software di video conferenza fornito in push dall'azienda In questo caso l'azienda si prende carico di una fornitura in outsourcing del software, anche solo per	X	



eBook_ Gestione di un processo di Firma Grafometrica e/o Firma Elettronica Avanzata in assenza di operatore o con operatore presente da remoto con strumenti di Unified Communication

quell'operazione. Il server di comunicazione UC è protetto essendo di proprietà dell'azienda.		
Software di video conferenza di proprietà di ciascuno In questo caso viene condiviso il server ma non il client, quindi vi è compatibilità tra di loro. Il rischio di anomalie è ripartito tra azienda e utenti, ma per l'azienda significa usare un server UC non completamente in proprio dominio.	X	X
Software per la sottoscrizione FG fornito in push dall'azienda In questo caso l'azienda si prende carico di una fornitura in outsourcing del software, che però gira nell'ambiente dell'utente. Essendovi un trattamento di dati biometrici, il Garante nel provvedimento generale di novembre 2014 ha delineato il perimetro entro il quale è possibile fare una relazione per FG anziché richiedere l'interpello. Per l'azienda potrebbe essere complesso estendere il controllo del runtime del software su un sistema non in proprio dominio.	X	
Software per FG di proprietà dell'utente In questo caso, l'Azienda accetta che l'utente diventi il fornitore del software per fare la FG. Per l'azienda potrebbe essere complesso ed antieconomico il procedimento di verifica dell'accettabilità della soluzione, soprattutto se non conosce l'utente	X	X

4.2 Interazioni per la firma del documento

Per la sottoscrizione del documento utilizzando la videoconferenza sono possibili diverse forme di interazione tra operatore di front end ed utenti firmatari.

Gli elementi che possono fare la differenza sono:

- I. il computer/device su cui gira l'applicazione di firma
- II. il canale di comunicazione utilizzato per far veicolare il documento da sottoscrivere

Tra gli strumenti UC, quelli che possono aiutare l'interazione sono la condivisione del desktop o delle maschere di una applicazione ed il file transfer. Per condivisione si intende generalmente la visualizzazione delle interfacce GUI e del controllo del mouse e della tastiera che normalmente sono gestibili dall'owner della videoconferenza.

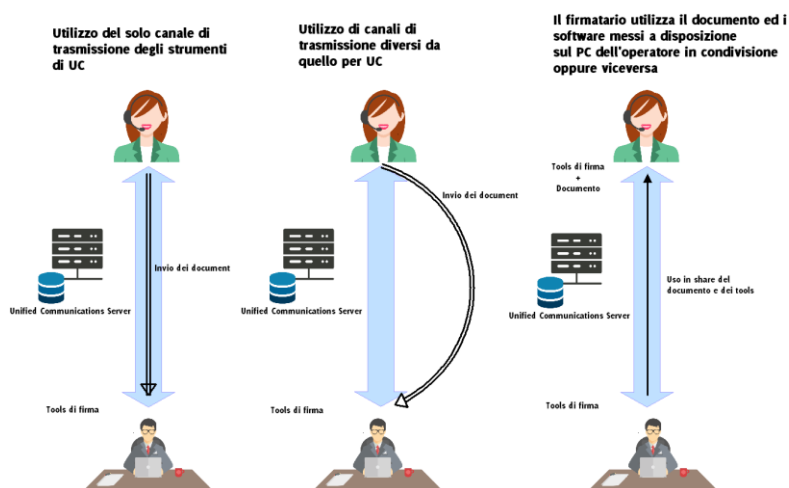


eBook_ Gestione di un processo di Firma Grafometrica e/o Firma Elettronica Avanzata in assenza di operatore o con operatore presente da remoto con strumenti di Unified Communication

Utilizzando lo strumento di Unified Communication di condivisione, il software per la FG può girare sul device dell'utente il quale è condiviso con l'operatore in modo che possa sovrintendere il processo di completamento del documento. In questo modo si avrebbe il vantaggio che il software può interagire direttamente con i device di raccolta del tratto grafometrico che devono necessariamente essere presenti dal lato utente.

Oppure al contrario, può girare sul computer dell'operatore ed essere condiviso con l'utente. In questo caso è evidente che il software di firma dovrà poter interagire con i componenti di controllo dei tablet di firma o EMR integrati dell'utente. Questo potrà avvenire con una soluzione per FG adhoc che tenga conto delle criticità di passaggio dei dati biometrici comportamentali proteggendoli con opportuni algoritmi di criptazione.

Le informazioni, quali ad esempio il documento da firmare, possono essere veicolate attraverso il canale della UC, se questo lo consente. Oppure possono essere veicolate da workflow distribuiti che permettono ad esempio all'operatore di sottomettere la richiesta di firma alla soluzione FG, ovunque essa giri, ed anche al documento di raggiungere il software di raccolta e composizione, anch'esso ovunque sia in esecuzione.



4.3 Possibili scenari di impiego

L'impiego della raccolta di una sottoscrizione di un documento con firme FG ed operatore remoto, apre scenari non possibili prima del giugno 2013. Ricordiamo che un documento firmato con Firma Elettronica Avanzata di tipo grafometrico, ha una validità giuridica a tutti



eBook_ Gestione di un processo di Firma Grafometrica e/o Firma Elettronica Avanzata in assenza di operatore o con operatore presente da remoto con strumenti di Unified Communication

gli effetti equivalente alla firma tradizionale con penna su carta ai sensi dell'art. 2702 del codice civile, cioè della sottoscrizione privata.

Questo aspetto è quello che permette di pensare ad una remotizzazione di una funzione organizzativa, anche ove questa necessiti di raccogliere dati e firme da parte dell'utenza.

Nel GDL si sono anche individuati possibili casi d'uso per l'impiego di questa modalità di raccolta della FG. E' interessante notare che in ognuno di questi scenari sarebbero impiegabili sia la modalità Totem che la modalità BYOD con alcune predilezioni per l'una o l'altra a seconda della spinta alla remotizzazione del processo specifico.

In particolare per la sanità e gli uffici pubblici sarebbero possibili realizzazioni di Totem in uffici periferici o presso strutture pubbliche o private in cui effettuare operazioni "quasi dal vivo" con operatori anche multilingue che agevolano quindi lo scambio di documenti anche a stranieri.

Qui di seguito ne forniamo un breve elenco.

Sanità

- Sportelli al paziente con fornitura di operatori differenziati multilingue
- Ritiro/Consegna documentazione decentralizzato
- Carrelli mobili in reparto per raccolta di consensi

Banche

- Sportelli virtuali con operatività completa
- Estensione del servizio POS e Bancomat

Assicurazioni

- Rilascio di polizze ad eventi, negli hub di trasporto,
- Raccolta e consegna documentazione

Accoglienza turistica

- Accettazione in Hotel
- Consegna di ticket e documentazione per prenotazioni di servizi
- Noleggi

Uffici Pubblici

- Decentramento dei servizi



eBook_ Gestione di un processo di Firma Grafometrica e/o Firma Elettronica Avanzata in assenza di operatore o con operatore presente da remoto con strumenti di Unified Communication

- Potenziamento dei servizi anche in zone remote

Eventi

- Accettazione
- Consegna attestati

Trasporti

- Scambio e produzione di documentazione nei porti
- Postazioni nelle stazioni, aeroporti, ...

I Totem vengono utilizzati oramai da diversi anni ma per permettere l'interazione documentale tra l'utente e l'azienda che lo propone, essi avevano a bordo almeno una stampante ed uno scanner. Questi dispositivi ora servirebbero solo per due scopi accessori ed opzionali alla gestione di documenti informatici con validità legale.

Stampare una ricevuta dei documenti per quegli utenti che desiderano ancora la carta, al posto della ricezione di una ricevuta elettronica via email o scaricabile dal portale di home banking, home insurance, home health, ...

Scannerizzare pagine di carta su un totem, può servire ora per permettere all'utente di consegnare allegati da abbinare al documento elettronico in fase di firma, quali ad esempio: copie del documento di identità, denunce di sinistri, documentazione accessoria per un contratto, ...

Con l'evoluzione dell'ottica delle attuali webcam, la scannerizzazione può avvenire direttamente con l'impiego di un unico strumento usato sia per la videoconferenza che per riprendere le immagini fisse.



eBook_ Gestione di un processo di Firma Grafometrica e/o Firma Elettronica Avanzata in assenza di operatore o con operatore presente da remoto con strumenti di Unified Communication

5 Criticità di gestione del processo di raccolta di una FG remota

In questo tipo di processo sono state individuate le seguenti categorie di criticità di cui tener conto in fase di progettazione:

- Criticità insite nel processo FEA
- Criticità dovuta alla fisicità delle postazioni remote
- Criticità già evidenziate nel GDL AIFAG 2014-001 sull'interoperabilità
- Criticità sulla conservazione digitale a norma

Di queste criticità nel seguito il GDL ha evidenziato alcuni possibili interventi o proposte per superarle.

Come descritto nei capitoli precedenti, il processo FG prevede degli step d'esecuzione che devono essere garantiti dall'organizzazione e dall'impiego di opportuni hardware e software.

E' evidente che l'obiettivo di questi processi è la dematerializzazione all'origine dei documenti, ovvero la realizzazione di documenti informatici dalla loro creazione fino alla loro conservazione ed alienazione. Per questo, il ricorso a procedimenti non digitalizzabili neanche con strumenti di UC sarebbe un limite nel loro impiego e quindi una sconfitta nell'applicazione dell'innovazione digitale.

In particolare lo studio del GDL si è concentrato sugli aspetti di raccolta dell'informativa FEA e dell'identificazione, che non sono agevolati dalla non presenza *de visu* del firmatario: l'impiego della videoconferenza ed un chiarimento sull'interpretazione normativa potrebbero fare molto per rendere più chiara e deterministica l'adozione di questi processi.

Infatti, come previsto dalle vigenti regole tecniche, al fine di attivare il servizio di firma elettronica avanzata (con tecniche grafometriche) il soggetto che eroga la soluzione deve (DPCM 22/2/2013, Art. 57 comma 1, lettera a e b):

a) identificare in modo certo l'utente tramite un valido documento di riconoscimento, informarlo in merito agli esatti termini e condizioni relative all'uso del servizio, compresa ogni eventuale limitazione dell'uso, subordinare l'attivazione del servizio alla sottoscrizione di una dichiarazione di accettazione delle condizioni del servizio da parte dell'utente



eBook_ Gestione di un processo di Firma Grafometrica e/o Firma Elettronica Avanzata in assenza di operatore o con operatore presente da remoto con strumenti di Unified Communication

b) conservare per almeno venti anni copia del documento di riconoscimento e la dichiarazione di cui alla lettera a) ed ogni altra informazione atta a dimostrare l’ottemperanza a quanto previsto all’articolo 56, comma 1, garantendone la disponibilità, integrità, leggibilità e autenticità”

L’identificazione inoltre, interviene anche in fase di raccolta della firma ad ogni documento.

Per quel che riguarda invece le criticità di tipo fisico-logistico delle postazioni remote, gli scenari TOTEM o BYOD sono completamente differenti. Mentre nel primo l’organizzazione erogatrice della soluzione di FG può intervenire per la messa in sicurezza dei device e del luogo in cui gli apparati operano, nel secondo la messa in sicurezza dipende principalmente dall’utente che li fornisce. In questo secondo caso, il software e l’impiego della ripresa video potrebbero servire per migliorarne la sicurezza.

Queste sono alcune delle voci, utilizzando le quali il sistema UC può fare molto per innalzare la sicurezza:

1. l’adozione di **webcam** da entrambi i lati ad **elevata definizione ed angolo di visuale**
2. l’adozione di **webcam brandizzabili da remoto** tramite lo stesso tool di UC sulla postazione totem, in modo da riprendere anche spazi non direttamente visibili dalla prospettiva frontale dell’utente
3. l’adozione di un software di UC in grado di permettere all’operatore di non violare la privacy del firmatario, **permettendogli ad esempio di attivare e disattivare la ripresa** se questa riprende particolari non funzionali alla raccolta della FG
4. l’adozione di **microfoni ad alto guadagno e direzionalità** per limitare i disturbi derivanti ad esempio da ambienti aperti e garantire buona qualità audio anche per garantire buoni criteri di accessibilità dell’utenza (anziani, persone con inabilità, ...)
5. l’adozione di **criptazione del canale UC** con adeguati criteri ed algoritmi di cifratura
6. l’adozione di tool UC in grado di **registrare la sessione** tra operatore e utente
7. la descrizione del server UC, del suo dominio d’uso e del canale e dei tool utilizzati per il processo di FG, deve essere nota



eBook_ Gestione di un processo di Firma Grafometrica e/o Firma Elettronica Avanzata in assenza di operatore o con operatore presente da remoto con strumenti di Unified Communication

Anche le penne elettroniche e gli eventuali tablet esterni impiegati per la rilevazione della firma grafometrica sono da proteggere con maggior cura di una installazione tradizionale su desk dell'azienda in house. Le cause accidentali o dolose di danneggiamento sono molte di più potendo essere ad esempio i totem presenti in spazi non governati da sistemi di sicurezza attivi quali ad esempio stanze dedicate e presidiate da badge di entrata o locali di pertinenza comunque dell'azienda.

I tablet o EMR, se non già protetti dal fatto che sono integrati con lo schermo, potranno essere protetti contro la loro sottrazione tramite l'impiego di stand o box costruiti ad arte oppure tramite l'ancoraggio con attacchi standard di tipo VESA ai mobili.

Per le penne si deve garantire che siano facili da usare per tutta l'utenza e "leggere", ma che siano anche dotate di meccanismi di collegamento con il mobile del totem con cavetti di difficile asportazione, ad esempio d'acciaio e/o con cavetti per cui sia possibile identificarne la loro sostituzione o manomissione.

Il GDL AIFAG 2014 003 ha lavorato in stretto accordo con il GDL 001 che mira a proporre un documento di standardizzazione della sicurezza e interoperabilità delle soluzioni di firma FG. L'impiego di quest'ultima su scenari remoti apre molte possibilità d'impiego anche con una utenza non necessariamente di nazionalità italiana e quindi la garanzia di interoperabilità e sicurezza delle soluzioni e dei documenti così sottoscritti, è anche una esigenza sentita per le FG da remoto. Inoltre il GDL ha individuato una proposta di integrazione che verrà presentata nel prosieguo.

La raccolta di una firma FG da remoto con strumenti UC prevede che la costruzione del documento informatico da mettere in protezione avvenga sicuramente su una postazione collegata all'azienda per il tramite di connettività internet ed i suoi protocolli tipici. E' evidente che l'impiego di protocolli di sicurezza di tipo https e connessioni protette quali ad es. le VPN, molto possono fare per aumentare il profilo di sicurezza generale.

Ma il fattore di inserimento del documento nel sistema di conservazione è un elemento da rafforzare maggiormente. E' infatti altresì evidente che un documento preso in carico dal sistema di conservazione debba garantire che la sua costruzione è avvenuta nel rispetto del progettato processo FEA nel suo complesso e non da una fonte non attendibile.

Seguono alcune proposte su questi argomenti che potrebbero essere avanzate agli opportuni organi nazionali, per il pronunciamento di un chiarimento generale.



eBook_ Gestione di un processo di Firma Grafometrica e/o Firma Elettronica Avanzata in assenza di operatore o con operatore presente da remoto con strumenti di Unified Communication

5.1 Proposta di semplificazione: informativa FEA in modalità elettronica

La raccolta dell'informativa FEA in modalità cartacea, rappresenta una barriera all'ingresso per un sistema che vuol permettere il passaggio al digitale dei più tradizionali processi documentali. Per garantire a tutti i proponenti soluzioni di FEA di poter effettuare la raccolta di questo atto in modalità elettronica, il GdL ha avanzato due proposte operative.

Questa prassi, permetterebbe di raccogliere anche una copia elettronica del documento di identità e di mantenere il tutto in conservazione a norma digitale per i 20 anni previsti dalle norme tecniche, eliminando così ogni ambiguità interpretativa della norma ed eliminando altresì l'impiego definitivo della carta.

Ipotesi 1

La sottoscrizione del consenso all'utilizzo della soluzione FG da parte dei soggetti firmatari, avviene in due passaggi:

1. Il sottoscrittore, con una firma elettronica erogata in modalità anche diverse dall'impiego della grafometria sul tablet, avanza l'informativa FEA come documento informatico al proponente la soluzione di FG (soggetto A del DPCM sulle firme);
2. Successivamente, il soggetto erogante la soluzione di FEA, richiederà all'utente di ribadire tale accettazione sottoscrivendo nuovamente il documento informatico indicato nel punto 1, stavolta apponendovi una FG, subordinando a tale "seconda accettazione" l'attivazione del servizio per ogni altro utilizzo.

Ipotesi 2

La sottoscrizione del consenso all'utilizzo della soluzione FEA da parte dei soggetti firmatari, avviene tramite una firma elettronica, acquisita per mezzo della medesima soluzione di Firma Elettronica Avanzata del soggetto proponente A, della quale l'utente sta fornendo il consenso all'uso, ereditandone quindi il processo e le caratteristiche di sicurezza della soluzione di FEA stessa.

Nota



eBook_ Gestione di un processo di Firma Grafometrica e/o Firma Elettronica Avanzata in assenza di operatore o con operatore presente da remoto con strumenti di Unified Communication

Nell'ipotesi 1 il sottoscrittore appone una firma elettronica sull'informativa FEA dell'organizzazione e gliela fa pervenire. Questo attiverà presso l'organizzazione la raccolta di una firma FG sullo stesso documento informatico che gli è nel frattempo arrivato. Una volta apposta questa firma, il sottoscrittore utilizzerà la soluzione per qualsiasi altro documento.

Nell'ipotesi 2, il sottoscrittore con la stessa soluzione di firma FG, sottoscrive l'informativa FEA in modo elettronico. La firma elettronica sarà FES solo perché sta ancora espletando l'ultima incombenza normativa per usare la FG con quell'organizzazione".

5.2 Proposta di chiarimento: processo di identificazione via webcam

Al fine di espletare l'identificazione certa del richiedente, molto interessante è la modalità che prevede una fase di identificazione online attraverso una sessione audio/video che dovrà essere registrata e, successivamente, conservata a norma.

In tale modalità l'identificazione e la registrazione vengono effettuate mediante l'ausilio di un sistema di videoconferenza e prevede che il firmatario sia dotato di una webcam correttamente collegata ad un PC con sistema audio funzionante. Alternativamente, qualora la soluzione di videoconferenza lo consenta, sarà possibile utilizzare anche device mobili quali tablet e/o smartphone.

La procedura di identificazione online (con Webcam) rappresenta, come possiamo tutti intuire, un'enorme opportunità per la semplificazione del processo di identificazione propedeutico all'attivazione del servizio di firma elettronica avanzata, ma devono essere tenuti presenti alcuni accorgimenti volti a garantire l'autenticità della richiesta in corso e che l'Operatore dovrà aver cura di effettuare.

Naturalmente ogni soluzione di videoconferenza che i vari soggetti potranno utilizzare potrà avere delle caratteristiche e funzionalità differenti, ma si consiglia almeno il soddisfacimento di quanto di seguito riportato.

Tale procedura dovrà prevedere anche un'opportuna gestione dei dati sensibili raccolti durante la sessione audio/video, ad esempio l'operatore, al momento dell'identificazione dovrà richiedere al Titolare di confermare:

- l'accettazione delle condizioni contrattuali e del trattamento dei dati personali per l'attivazione del servizio di firma



eBook_ Gestione di un processo di Firma Grafometrica e/o Firma Elettronica Avanzata in assenza di operatore o con operatore presente da remoto con strumenti di Unified Communication

- i dati identificativi ed anagrafici registrati che verranno utilizzati anche per l'emissione del documento che si accinge a sottoscrivere con firma FG
- Inoltre, per garantire la tutela e la gestione dei propri dati personali in piena aderenza al DLGS 196/2003, ad ogni richiedente dovrà essere preventivamente fornita l'informativa sulla privacy chiedendo il consenso alla videoregistrazione ed al trattamento dei dati.

Durante la sessione di videoconferenza l'Operatore che effettua l'identificazione si accerterà dell'identità del Titolare tramite la verifica di un documento di riconoscimento in corso di validità, purché munito di fotografia recente e riconoscibile del Titolare, firma autografa del Titolare e di timbro, rilasciato da un'Amministrazione dello Stato.

Ma non solo, al fine di garantire una corretta ed autentica identificazione l'operatore dovrebbe chiedere al Titolare di compiere delle azioni che possano escludere la presenza di robot, quali ad esempio:

1. Richiedere di muovere la webcam e di muovere una mano o di alzarsi in piedi
2. Richiedere di leggere l'ora esatta
3. Su base opzionale ed a discrezione dell'Operatore, richiedere all'interlocutore di effettuare un'azione volta a garantire la presenza fisica dell'interlocutore stesso, ad esempio di "leggere la prima notizia su una specifica pagina web"
4. altro

Naturalmente quanto sopra descritto rappresenta alcuni possibili accorgimenti che il Soggetto che eroga il servizio potrà adottare per garantire l'identificazione certa del Titolare. In generale dovrà essere garantita all'operatore la facoltà di rifiutare il riconoscimento nel caso in cui giudichi non adeguata la registrazione o abbia dubbi sulla reale identità del richiedente.

Infine, una volta terminata la sessione di videoconferenza il risultante filmato audio/video (e relativi metadati) dovrà essere inviato al sistema di conservazione che li archiverà per un periodo non inferiore a 20 anni.

5.3 Proposta di integrazione: inserimento nell'xml extended delle informazioni del totem



eBook_ Gestione di un processo di Firma Grafometrica e/o Firma Elettronica Avanzata in assenza di operatore o con operatore presente da remoto con strumenti di Unified Communication

La fase di eventuale disconoscimento di una firma di tipo FEA è un evento da gestire con il maggior numero di informazioni possibili, raccolte in tempo reale durante l'espletamento del processo. Nel documento del GDL AIFAG 2014-001 è emersa l'opportunità di rafforzare la perizia aggiungendo al pacchetto di firma storicizzato nel documento informatico un file xml di informazioni di contesto.

Si propone di approfondire in una evoluzione di questi studi, quali informazioni sia meglio memorizzare nel caso di raccolta di una FG da remoto.

In prima redazione si può ipotizzare queste categorie di informazioni:

- tipo di collegamento tra operatore e utente: de visu, remoto
- se utilizzato uno strumento di UC:
 - dati identificativi del software e degli account utilizzati
 - tipo di canale impiegato
 - dati identificativi della webcam, microfono, casse, ...
 - se la sessione è stata registrata
- dati del totem
- altro

6 Prospettive future

L'impatto delle Regole eIDAS (Regolamento UE 910/2014 in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la Direttiva 1999/93/CE nel seguito indicato come Regolamento) ha poca influenza al tempo di stesura del presente documento sui temi trattati.

La FEA è presente nel Regolamento con una definizione simile a quella della Direttiva 1999/93/CE ma senza regole sui formati e sull'interoperabilità, essa rimane un principio giuridico.

La piena applicazione sarebbe possibile solo con la disponibilità di regole tecniche che possano soddisfare quanto stabilito nell'articolo 27 dell'eIDAS in materia di interoperabilità transnazionale.



eBook_ Gestione di un processo di Firma Grafometrica e/o Firma Elettronica Avanzata in assenza di operatore o con operatore presente da remoto con strumenti di Unified Communication

Per quanto attiene specificamente alla grafometrica in ambito ETSI e CEN si sta valutando l'idea di recepire una proposta di standardizzazione sviluppata all'interno del documento AIFAG su sicurezza e interoperabilità.

Per quanto attiene al Sistema Pubblico di Identità Digitale per cittadini e imprese (SPID) possiamo ipotizzare che la disponibilità di credenziali omogenee per l'accesso ai servizi pubblici e privati favorisca alcuni meccanismi di identificazione remota (come il riconoscimento via webcam).

E' bene precisare che le regole di SPID non sono direttamente applicabili in eIDAS, ma SPID è stato disegnato normativamente e tecnicamente per avere tutte le carte in regola per essere accettato come schema di identificazione notificato (artt. 7 e 9 del Regolamento).

Tra l'altro il Regolamento indica esplicitamente che mezzi di identificazione a distanza sono pienamente accettabili in questi contesti.

La disponibilità di credenziali "buone" per l'identità digitale permette di superare le fasi di riconoscimento preliminare nella FEA, favorendo anche l'utilizzo di postazioni di FEA non presidiate. Ovviamente in questo caso ci si può chiedere se non sia il caso di utilizzare meccanismi di sottoscrizione a chiave pubblica piuttosto che di firma grafometrica, ma questa analisi non è generalizzabile.

Dipende dal contesto, dalla volontà di facilitare la *user experience* o da specifiche esigenze ambientali.

Concludendo possiamo senz'altro affermare che:

- a. eIDAS nel medio periodo non influenza le tematiche legali, tecniche e di mercato della FEA italiana e in particolare della grafometrica;
- b. SPID ha le carte in regole per entrare tra i sistemi notificati nell'ambito degli schemi di identificazione elettronica;
- c. è possibile associare dei sistemi grafometrici a credenziali di identità SPID.

Non si può ignorare il fatto che SPID garantisce l'accesso a servizi tramite le credenziali "validate" dal sistema stesso. Questo può avere impatti negativi sulla diffusione di servizi di sottoscrizione tradizionale anche se in modalità elettronica. Questo perché sarebbero più efficienti sistemi di firma elettronica avanzata basati su infrastrutture a chiave pubblica (PKI) e utilizzati in modalità remota (FEA PKI remota).



eBook_ Gestione di un processo di Firma Grafometrica e/o Firma Elettronica Avanzata in assenza di operatore o con operatore presente da remoto con strumenti di Unified Communication

7 Bibliografia e riferimenti

- Dlgs 82/2005 - Codice dell'amministrazione digitale – Decreto legislativo 7 marzo 2005, n. 82
- DPCM 22/2/2013 – DECRETO DEL PRESIDENTE DEL CONSIGLIO DEI MINISTRI 22 febbraio 2013 - Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali, ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma 3, lettera b) , 35, comma 2, 36, comma 2, e 71 del Dlgs 82/2005
- DPCM 3/12/2013 - DECRETO DEL PRESIDENTE DEL CONSIGLIO DEI MINISTRI 3 dicembre 2013 – Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3 e 5-bis, 23-ter, comma 4, 43, commi 1 e 3, 44 , 44-bis e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005
- DPCM 13/11/2014 - DECRETO DEL PRESIDENTE DEL CONSIGLIO DEI MINISTRI 3 dicembre 2013 – Regole tecniche sulla formazione del documento informatico
- PROVVEDIMENTO del Garante dei dati personali n. 513/2014 del 12 novembre 2014 - Provvedimento generale prescrittivo in tema di biometria
- Regulation (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC
- <http://www.agid.gov.it/agenda-digitale/infrastrutture-architetture/spid>
- <http://www.aifag.it>
- <http://www.agid.gov.it/>
- <http://www.garanteprivacy.it/>