Caratteristiche generali del prodotto “Firma grafometrica”

La firma grafometrica consiste in un processo informatico che, nel rispetto dei quanto previsto dal CAD, implementa un particolare tipo di firma elettronica avanzata.

La firma grafometrica è una definizione comunemente usata per indicare una modalità di firma elettronica realizzata con un gesto manuale del tutto analogo alla firma autografa su carta. I dati di una firma si raccolgono mediante un dispositivo in grado di acquisire dinamicamente il movimento di uno stilo - azionato direttamente dalla mano di una persona - su una superficie sensibile (emulando una penna sulla carta).

Questa tipologia di firma si ottiene rilevando alcuni dati biometrici del firmatario, nel momento in cui egli appone la firma su di un tablet, legandoli in maniera indissolubile al documento oggetto di firma

In funzione della tecnologia impiegata si possono ottenere diversi livelli di qualità: risoluzione posizionale, frequenza dei campioni nell'unità di tempo, disponibilità del dato relativo alla pressione dello stilo sulla superficie, inclinazione, ecc.

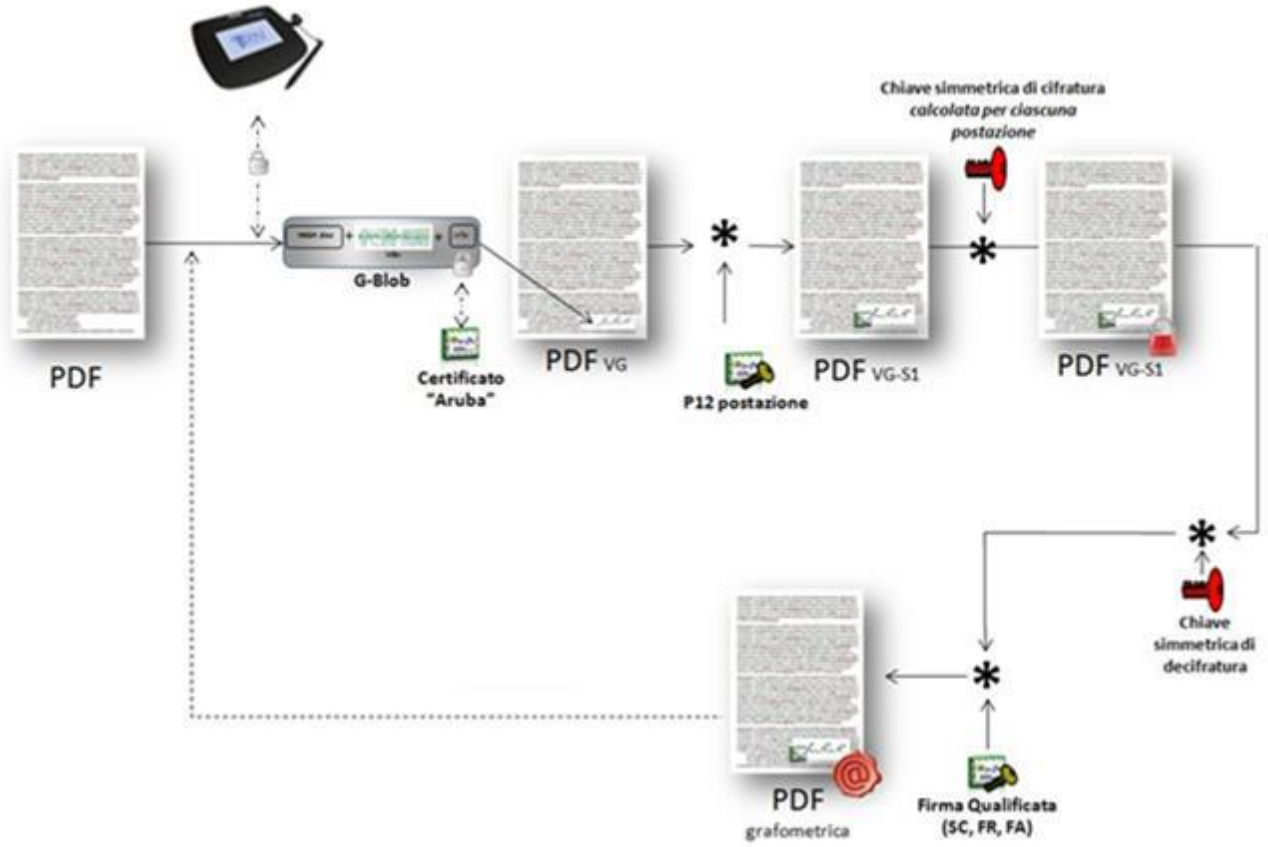
Ferma restando la modalità di acquisizione del gesto della firma, esistono diverse linee principali di applicazione di questa tecnologia.

In questo documento verrà trattata l’applicazione della Grafometria quale strumento di **Firma Elettronica Avanzata Grafometrica**, ovvero quel tipo di FEA in cui i dati della firma acquisita sono associati univocamente al documento (in genere PDF) oggetto di sottoscrizione, cifrati per renderli inaccessibili per un utilizzo con altri documenti, quindi inseriti in un normale campo di firma elettronica che ne protegge l'integrità.

La firma associata al documento è poi verificabile, in caso di disconoscimento, da parte di un grafologo che la esamina esattamente come nel caso cartaceo.

Questa modalità, in particolare, grazie al valore legale conferito dalle ultime modifiche al Codice dell'Amministrazione Digitale (soddisfacimento pieno del requisito della forma scritta), è particolarmente interessante: permette infatti di estendere la dematerializzazione anche nei casi in cui sia richiesta una firma ad un utente non provvisto di strumenti per la Firma Digitale.

Dal punto di vista logico/applicativo il flusso descritto sopra è rappresentato dall'immagine che segue:



Come mostrato, la procedura di firma grafometrica di un documento si compone delle seguenti macro-fasi:

1. Acquisizione del documento di identità del firmatario e del consenso firmato all'utilizzo del sistema di firma grafometrica;
2. Acquisizione del documento da firmare grafometricamente. Il documento "originale" ossia il documento che s'intende sottoporre al processo di firma grafometrica dovrà avere un formato tale da non contenere macroistruzioni al suo interno (es PDF-A);
3. Acquisizione protetta dei Vettori grafometrici dalla tavoletta grafica (Vg);
4. Creazione di un G-blob (Graphometric-blobl), ossia di una strutta dati costituita da:
    - **HASH** del documento oggetto di firma grafometrica;
    - Vettori grafometrici (Vg);
    - Informazioni identificative della tavoletta grafica utilizzata (ID univoco, marca, modello, ..);
    - Time-stamp;
    - Extra-info;
    - Cifratura del G-blob con il certificato digitale (X509 v3) "Aruba" hard-coded nella libreria AGI.

5. Inserimento del G-blob nel documento. In questa fase si ottiene il documento originale al quale è stata apposta la firma grafometrica (PDFVG) ma che non è stato ancora “reso immodificabile” tramite l’applicazione della firma digitale d’integrità;
6. Firma elettronica d’integrità (PADES) del documento. Immediatamente dopo l’inserimento del G-blob (operazione “t=0”) viene apposta una firma digitale con il P12 creato appositamente per la postazione ed inviato alla stessa tramite l’hand-shake protetto di licensing. Il documento prodotto PDFVG-S1 offre garanzia di integrità ed immodificabilità del contenuto binario del documento;
7. Cifratura del PDFVG-S1 per la memorizzazione sicura del documento stesso sul file system;
8. De-cifratura del documento per la successiva elaborazione del documento stesso, che potrà essere una delle seguenti operazioni:

    • Apposizione di una nuova firma grafometrica sul documento. In questo caso, il file PDFVG-S1 verrà rielaborato dal processo di firma grafometrica seguendo il processo applicato al documento originale. In particolare, l’operazione di decifratura del file file PDFVG-S1 e l’avvio di una nuova operazione di firma grafometrica avverranno in “t=0”, ossia saranno operazioni atomiche che non consentiranno l’introduzione di altre operazioni da parte di altri processi;

    • “Chiusura” del documento con firma qualificata dell’Operatore. In questo caso l’Operatore che avrà provveduto, nell’ambito del processo di firma grafometrica, all’identificazione dell’Utente procederà alla firma qualificata del documento PDFVG-S1 tramite uno degli strumenti di firma qualificata previsti ed integrati nella soluzione offerta (smart card, token USB, Firma remota/automatica). In particolare, le operazionI di decifratura del file PDFVG-S1 e la firma qualificata del documento decifrato stesso avverranno in modalità “t=0” ossia senza che alcun altro processo possa subentrare tra la prima operazione e la seconda. Sarà inoltre possibile, qualora il processo lo preveda e comunque su indicazione dell’Operatore, apporre una marca temporale immediatamente dopo aver firmato con firma qualificata il documento.

In generale, le componenti software coinvolte in tutti i processi descritti non memorizzano mai le quantità di sicurezza critiche trattate (come ad esempio i vettori grafometrici). Nel caso di utilizzo e gestione di tali dati, questi vengono gestiti sempre in maniera cifrata e, terminata la specifica operazione, vengono cancellati dalla memoria del dispositivo in uso.

In aggiunta le chiavi di cifratura sono diverse e generate ad-hoc documento per documento.

A maggiore garanzia dell’utente, oltre che per l’irrobustimento dell’intero processo di firma elettronica avanzata, verranno memorizzati all’interno della libreria di firma grafometrica gli HASH dei vettori grafometrici, immediatamente prima che questi vengano inseriti nel G-blob.

In questo modo il processo può garantire che, almeno all'interno di una sessione di firma, i vettori grafometrici siano differenti e quindi non sia possibile utilizzare lo stesso set di vettori grafometrici per apporre più firme allo stesso documento.