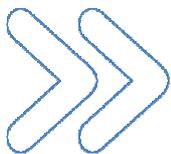




Firma Grafometrica Provincia di Trento



Descrizione della soluzione di Firma Elettronica Avanzata in modalità grafometrica Provincia Autonoma di Trento



Sommario

1	Scopo e contenuto del documento	3
2	Introduzione.....	4
3	Identificazione del firmatario e adesione al Servizio di Firma Grafometrica PAT.....	6
4	Sottoscrizione del documento.....	7
5	Il processo di Firma Grafometrica	8
6	Caratteristiche del sistema realizzato nel rispetto delle regole tecniche	9
7	Obblighi a carico della Provincia Autonoma di Trento	11
8	Caratteristiche delle tecnologie utilizzate.....	14





1 Scopo e contenuto del documento

Scopo del documento è descrivere la soluzione di Firma Elettronica Avanzata erogata in modalità grafometrica dalla Provincia Autonoma di Trento in linea con le Regole Tecniche dettate dal Decreto del Presidente del Consiglio dei Ministri del 22 febbraio 2013.

Il presente documento è pubblicato sul sito internet istituzionale dell'ente.





2 Introduzione

La Provincia autonoma di Trento (PAT) ha introdotto la firma grafometrica applicandola ad alcuni processi che richiedono la firma di documenti che regolano il rapporto diretto tra cittadino/impresa e Pubblica Amministrazione in presenza di un funzionario o di un addetto.

La firma elettronica avanzata erogata in modalità grafometrica è ottenuta realizzando una soluzione tecnologica e organizzativa, che prevede l'utilizzo di strumentazione sofisticata per rilevare l'insieme dei dati biometrici (ritmo, pressione, velocità, inclinazione, ecc.) della firma autografa del sottoscrittore, tramite una penna elettronica su una tavoletta digitale.

I dati biometrici raccolti sono legati indissolubilmente al documento e cifrati al suo interno, al fine di scongiurare il riuso degli stessi o una loro elaborazione che porti al risultato di falsificare o riprodurre la firma su altri documenti, che di conseguenza risulterebbero sottoscritti in assenza della volontà del firmatario.

La soluzione di firma biometrica adottata dalla PAT garantisce il non riutilizzo dei dati biometrici presenti nel modello firmato e la chiave per la decifrazione è conservata, con elevato livello di sicurezza, presso l'Ufficio Informatica della PAT.

Esattamente come nel mondo cartaceo, nel caso di contenzioso o ripudio della firma da parte del sottoscrittore, sarà necessario effettuare una perizia calligrafica, verificando attraverso la strumentazione in dotazione le caratteristiche della firma, mediante il confronto tra il documento in analisi, che contiene la firma, e i dati biometrici raccolti da un perito calligrafo o altro esperto del settore: solo in questo caso si potrà utilizzare la chiave di decifrazione e accedere ai dati biometrici contenuti nel documento oggetto di contenzioso.

La PAT ha realizzato la soluzione di Firma Elettronica Avanzata in modalità Grafometrica per i propri uffici e attivato progressivamente sul territorio delle postazioni, per consentire al cittadino di firmare i documenti con questa modalità e nel rispetto dei requisiti tecnici e normativi richiesti dal Codice dell'Amministrazione Digitale (CAD) e dal Decreto del Presidente del Consiglio dei Ministri del 22 febbraio 2013.

2.1 Attuali ambiti di utilizzo ed evidenza di quanto sottoscritto

2.1.1 ICEF TRENINO

I soggetti erogatori della soluzione sono ICEF TRENINO presso Sportelli CAAF, Patronati e Sportelli periferici PAT.

Le tipologie documentali coinvolte sono:

- ✓ Dichiarazioni sullo stato reddituale per persona fisica (ICEF)
- ✓ Domanda Unica per contributo su mense, trasporti, famiglie numerose e assegno regionale al nucleo familiare
- ✓ Domanda di reddito di garanzia.

Il consenso per l'utilizzo del servizio viene effettuato una tantum all'atto della firma del primo documento da parte del cittadino.

Copia del documento sottoscritto è consultabile dal cittadino accedendo al portale dei servizi (www.servizionline.provincia.tn.it).



2.1.2 CONTRATTI del PERSONALE DELLA SCUOLA

Presso gli Uffici del Dipartimento della Conoscenza e presso i Circoli di coordinamento pedagogico sono invece sottoscritti i CONTRATTI del PERSONALE DELLA SCUOLA, composti da due tipologie documentali:

- ✓ Contratto assunzioni in ruolo
- ✓ Assunzione a tempo determinato su graduatorie provinciali

Il consenso per l'utilizzo del servizio viene raccolto oralmente dal dirigente o funzionario PAT.

Copia del documento sottoscritto è consegnato all'atto della sottoscrizione e su richiesta può essere inviato tramite e-mail.





3 Identificazione del firmatario e adesione al Servizio di Firma Grafometrica PAT

Il firmatario è riconosciuto dall'addetto allo sportello o dal funzionario mediante la presentazione di un documento d'identità valido e aderisce al servizio di firma grafometrica provinciale dopo aver preso visione dell'informativa e sottoscritto con firma autografa il modulo di consenso predisposto dalla Provincia. Tale consenso è custodito negli archivi provinciali per venti anni, unitamente alla fotocopia del documento di identità, ed è valido per tutti i servizi, attuali e futuri, messi a disposizione dalla PAT per il cittadino che si presenta allo sportello.

Il consenso all'adesione può essere revocato in qualunque momento, inviando una mail all'indirizzo uff.informatica@pec.provincia.tn.it con oggetto "Richiesta revoca consenso servizio di firma grafometrica PAT", indicando il codice fiscale e allegata la fotocopia del documento d'identità.

Solo in presenza di un dirigente PAT, o di un suo delegato, nel caso in cui il firmatario instauri un rapporto diretto e continuativo con la Provincia, il consenso è richiesto e fornito oralmente.

Il firmatario può richiedere una copia dell'adesione o della revoca al servizio, inviando una mail all'indirizzo uff.informatica@pec.provincia.tn.it con oggetto "Richiesta copia adesione/revoca servizio di firma grafometrica PAT", indicando il codice fiscale e allegata la fotocopia del documento d'identità.

Nel caso in cui il cittadino si opponga all'utilizzo di tale tecnologia, è comunque possibile sottoscrivere i documenti con firma autografa semplicemente stampando il PDF prodotto.



4 Sottoscrizione del documento

Il cittadino in presenza dell'addetto allo sportello o del funzionario PAT, verifica il documento da firmare su un apposito schermo e appone la firma grafometrica sulla tavoletta grafica, con un gesto naturale molto simile alla firma autografa. Il modello attualmente in uso e distribuito sul territorio è la tavoletta WACOM STU-520. La tavoletta viene collegata direttamente al PC tramite la sua interfaccia USB con cifratura dei dati.

Nella medesima modalità l'addetto o funzionario PAT appone, in presenza del cittadino, la propria firma grafometrica.

Al termine del processo di firma il documento sottoscritto non è modificabile e ne viene garantita l'integrità e la leggibilità nel tempo. All'interno del documento sono custoditi in modo sicuro tutti gli elementi necessari per successive verifiche giudiziarie.





5 Il processo di Firma Grafometrica

Su ogni postazione fisica, adibita alla firma grafometrica, viene installata una tavoletta digitale (Wacom STU-520) e un software certificato per la cattura dei dati biometrici (SignDoc di SoftPro <http://www.softpro.de/en/>).

Il sistema gestionale, dopo l'inserimento dei dati da parte dell'addetto o del funzionario PAT, produce un documento in formato PDF predisposto con i campi firma specifici sia per l'addetto che per il sottoscrittore (cittadino). I firmatari prendono atto del documento, visualizzato su monitor, e appongono la propria firma sulla tavoletta.

I dati raccolti sono inseriti nel documento e non possono essere modificati: l'immagine della firma è visibile nel campo firma predisposto (un campo per ogni firma prevista), mentre i dati biometrici (ritmo, pressione, velocità, inclinazione, ecc.) sono archiviati in modo cifrato (RSA a 2048 bit).

Al termine della cattura dei dati biometrici, la tavoletta viene automaticamente spenta, assicurando in questo modo la cancellazione definitiva di qualsiasi dato temporaneo. Dopo l'applicazione della firma al documento i buffer di memoria del sistema di firma SigDoc vengono resettati, in modo da cancellare definitivamente eventuali dati temporanei residui.

Il PDF firmato con firma grafometrica conforme allo standard PAdES (documento ETSI TS 102 778) è inviato al sistema di protocollo provinciale (P.I.Tre) oppure firmato digitalmente (firma automatica massiva), marcato temporalmente e inviato al sistema di conservazione a norma presso InfoCert.

I documenti sono disponibili per la consultazione da parte del sottoscrittore, ma le informazioni biometriche sono cifrate e non consultabili. Tali informazioni possono essere rese accessibili solo su richiesta dell'Autorità Giudiziaria in presenza di un perito nominato dal tribunale e solo dopo aver recuperato la chiave privata di cifratura e la password associata.

La chiave di decifratura è conservata presso l'Ufficio Informatica della PAT.



6 Caratteristiche del sistema realizzato nel rispetto delle regole tecniche

<i>Caratteristiche delle soluzioni di firma elettronica avanzata Art. 56 comma 1</i> <i>Le soluzioni di firma elettronica avanzata garantiscono:</i>	<i>Considerazioni</i>
Lettera a) l'identificazione del firmatario del documento;	Il firmatario che si presenta allo sportello, predisposto e dotato dell'attrezzatura idonea per effettuare la firma grafometrica, viene riconosciuto mediante esibizione di un documento di identità valido.
Lettera b) la connessione univoca della firma al firmatario;	Il firmatario, utilizzando l'apposito stilo, traccia la propria firma sul documento. Contemporaneamente, il pad acquisisce i dati biometrici statici (coordinate grafiche e la pressione) consentendo con essi di elaborare quelli dinamici (accelerazione, velocità, ritmo, inclinazione della penna). La raccolta dei dati biometrici consente di identificare univocamente la firma di una persona; un'altra persona che cerchi di imitare la firma originale fa rilevare con elevatissima probabilità parametri diversi.
Lettera c) il controllo esclusivo del firmatario del sistema di generazione della firma, ivi inclusi i dati biometrici eventualmente utilizzati per la generazione della firma medesima;	I dati sono cifrati con una chiave simmetrica all'interno del pad e sono inviati all'infrastruttura che governa il processo; i dati sono decifrati e nuovamente cifrati con una chiave asimmetrica (pubblica), indi inseriti nel PDF. Contemporaneamente, la forma grafica della firma è inserita all'interno del documento.
Lettera d) la possibilità di verificare che il documento informatico sottoscritto non abbia subito modifiche dopo l'apposizione della firma;	All'atto della conferma della firma sulla tavoletta da parte del firmatario, è generata una prima impronta del documento con i dati cifrati, mediante l' algoritmo SHA-256; il tutto viene memorizzato nel documento, permettendo così di verificarne agevolmente l'integrità. Una seconda impronta del documento con i dati in chiaro è calcolata, sempre con algoritmo SHA-256, e memorizzata nel documento, elemento necessario in caso di contenzioso legale.



Lettera e) la possibilità per il firmatario di ottenere evidenza di quanto sottoscritto;	Il pad o il monitor permette sempre la visione del documento da parte del firmatario, inoltre è sempre possibile averne copia così come indicato nel paragrafo 2.1 <i>Attuali ambiti di utilizzo ed evidenza di quanto sottoscritto</i>
Lettera f) l'individuazione del soggetto di cui all'art. 55, comma 2, lettera a);	La provincia Autonoma di Trento eroga la soluzione di firma grafometrica avvalendosi della sua società di sistema individuata in Informatica trentina S.p.A. Per la realizzazione della soluzione di firma grafometrica è stato utilizzato il software prodotto da Soft Pro E-SIGNING (http://www.softpro.de).
Lettera g) l'assenza di qualunque elemento nell'oggetto della sottoscrizione atto a modificarne gli atti, fatti o dati nello stesso rappresentati;	Il documento sottoscritto viene inserito nel sistema federato di protocollo provinciale (PiTre) oppure firmato con firma digitale automatica, marcato temporalmente e inviato in conservazione.
Lettera h) la connessione univoca della firma al documento sottoscritto.	Il documento da sottoscrivere è generato in formato PDF, statico e non modificabile, e visualizzato al firmatario su un apposito monitor a questi visibile. Sul display del pad appare il campo "firma". Il documento firmato è auto consistente perché contiene i dati biometrici crittografati che tecnicamente non possono essere estratti e apposti su altri documenti.



7 Obblighi a carico della Provincia Autonoma di Trento

Art. 57 Obblighi a carico dei soggetti che erogano soluzioni I soggetti di cui all'art. 55, comma 2, lettera a) devono:	Considerazioni
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;	Il firmatario viene informato e riconosciuto presso l'ufficio preposto. La dichiarazione di accettazione è sottoscritta una tantum con firma autografa e conservata cartacea unitamente alla copia del documento di identità valido. Solo alla presenza di un dirigente PAT, o di un suo delegato, nel caso in cui il firmatario instauri un rapporto diretto e continuativo con la Provincia, il consenso è richiesto e fornito oralmente.
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;	Il modulo analogico è conservato presso gli archivi provinciali.
c) fornire liberamente e gratuitamente copia della dichiarazione e le informazioni di cui alla lettera b) al firmatario, su richiesta di questo;	Richiedibile gratuitamente alla mail uff.informatica@pec.provincia.tn.it
d) rendere note le modalità con cui effettuare la richiesta di cui al punto c), pubblicandole anche sul proprio sito internet;	Pubblicate al sito www.servizionline.provincia.tn.it www.vivoscuola.it
e) rendere note le caratteristiche del sistema realizzato atte a garantire quanto	Pubblicate sul sito istituzionale di PAT.



prescritto dall'articolo 56, comma 1;	
f) specificare le caratteristiche delle tecnologie utilizzate e come queste consentono di ottemperare a quanto prescritto;	Pubblicate sul sito istituzionale di PAT.
g) pubblicare le caratteristiche di cui alle lettere e) ed f) sul proprio sito internet;	Pubblicate sul sito.
h) assicurare, ove possibile, la disponibilità di un servizio di revoca del consenso all'utilizzo della soluzione di firma elettronica avanzata e un servizio di assistenza.	Servizio disponibile gratuitamente alla mail uff.informatica@pec.provincia.tn.it
<p>Art. 58 I soggetti che offrono una soluzione di firma elettronica avanzata alle pubbliche amministrazioni, devono essere in possesso della certificazione di conformità del proprio sistema di gestione per la sicurezza delle informazioni ad essi relative:</p> <ul style="list-style-type: none">• alla norma ISO/IEC 27001• alla norma ISO 9001 e successive modifiche o a norme equivalenti.• possono far certificare la propria soluzione secondo la norma ISO/IEC 15408, livello EAL 1 o superiore	 <p>Informatica trentina SpA (http://www.infotn.it) è certificata :</p> <ul style="list-style-type: none">• Qualità UNI EN ISO 9001:2008 per il seguente campo applicativo: “Progettazione ed erogazione di servizi di telecomunicazioni, data center, desktop management ed assistenza; progettazione, sviluppo, commercializzazione ed assistenza di software applicativo per la pubblica amministrazione”.• Sicurezza delle Informazioni in conformità ai requisiti della norma UNI CEI ISO/IEC 27001:2006 per il seguente campo applicativo: “Progettazione, realizzazione, avviamento ed erogazione continuativa di servizi applicativi, tecnologici, di sicurezza erogati alle Amministrazioni Trentine, ed esecuzione delle attività di supporto per l'erogazione degli stessi”.



7.1 Copertura assicurativa della Provincia Autonoma di Trento (DCPM 22.2.2.013 art.57 comma 3)

La copertura assicurativa già in possesso della PAT è a garanzia di eventuali danni derivanti da inadeguate soluzioni tecniche che incidano sul corretto utilizzo dei dati biometrici.





8 Caratteristiche delle tecnologie utilizzate

La soluzione tecnologica utilizzata si compone di tre macro-elementi: la postazione dell'incaricato con il pad di raccolta di firma, le applicazioni di creazione del documento e la piattaforma di firma grafometrica di Informatica trentina e partner, integrata con i servizi di certificazione digitale e conservazione del documento informatico di InfoCert.

8.1 Postazione dell'incaricato allo sportello

La postazione dell'incaricato è dotata di tablet per poter raccogliere la firma grafometrica. La soluzione tecnologica prescelta utilizza dispositivi hardware dotati di tecnologia touch in grado di rilevare i principali parametri della firma dell'utente.

8.2 Applicazioni

Le applicazioni consentono la creazione del documento in formato PDF che è trasmesso in modalità sicura alla piattaforma di firma grafometrica per la creazione della sottoscrizione.

8.3 Piattaforma di firma grafometrica

La postazione dell'incaricato e le applicazioni colloquiano con la piattaforma di firma grafometrica installata presso il datacenter di Informatica Trentina che svolge le seguenti operazioni:

- Raccolta dati biometrici rilevati dal dispositivo;
- Cifratura dei dati biometrici;
- Inserimento sicuro dei dati nel documento;
- Invio al sistema di protocollo Informatico Trentino (PiTre)
 - Oppure per i documenti non protocollati in PiTre
 - Firma digitale del documento tramite il sistema di firma automatica di InfoCert;
 - Marcatura temporale del documento a validazione dell'istante di firma;
 - Invio del documento firmato con firma grafometrica al sistema di Conservazione digitale offerto da InfoCert.
- Restituzione alle applicazioni del documento firmato;

La piattaforma di firma grafometrica è erogata da Informatica Trentina e integrata con i servizi di certificazione per quanto riguarda l'apposizione della firma digitale a chiusura del documento e il servizio di conservazione a norma erogati dal certificatore accreditato InfoCert.

8.3.1 Servizio di firma digitale automatica e marcatura

A chiusura del processo di firma grafometrica, per i documenti non protocollati in PiTre, grazie al servizio di firma digitale automatica, la Provincia autonoma di Trento appone la firma digitale attraverso una procedura automatica, a presidio dell'integrità del documento e dei dati biometrici crittografati.



Le chiavi dei titolari dei certificati di firma digitale sono generate e conservate presso InfoCert, su dispositivi sicuri ad alte prestazioni (Hardware Security Module HSM).

Sui documenti firmati è apposta una marca temporale utilizzando il servizio di InfoCert. La marca temporale consiste nella generazione, da parte di una terza parte fidata, di una firma elettronica del documento alla quale è associata l'informazione relativa ad una data e ad un'ora certa.

Il server InfoCert che genera le marche temporali ricava il tempo, con riferimento al Tempo Universale Coordinato (UTC), da un ricevitore radio sintonizzato (preventivamente tarato e certificato) con il segnale emesso dall'Istituto Nazionale di Ricerca Metrologica di Torino (INRIM).

La marca temporale è emessa automaticamente da un sistema elettronico sicuro (server della Time Stamping Authority o TSA) dell'Ente Certificatore InfoCert. Le marche temporali emesse da InfoCert hanno una validità di 20 anni, ovvero il maggior tempo di conservazione della marca stessa.

8.3.2 Servizio di conservazione a norma

I documenti firmati con firma grafometrica che non sono stati inviati a PiTre, sono inviati al sistema di conservazione InfoCert, per la garanzia dell'inalterabilità, della leggibilità e della disponibilità nel tempo dei documenti informatici.

Il servizio garantisce il pieno rispetto della normativa vigente in materia di conservazione elettronica dei documenti; la PAT ha delegato ad InfoCert le responsabilità previste dalla normativa vigente sul procedimento di conservazione elettronica dei documenti.

InfoCert, in qualità di responsabile del processo di conservazione, garantisce il soddisfacimento di tutti i requisiti necessari per preservare la validità legale nel tempo dei documenti conservati. La PAT invia in conservazione anche opportuni metadati di ricerca associati ai documenti, in modo da rendere più efficaci ed agevoli le attività di ricerca della documentazione conservata, che avviene da parte degli addetti PAT in modalità sicura e profilata.

Il servizio offre inoltre agli addetti apposite funzioni di esibizione che consentono di consultare, oltre al contenuto del documento, le attestazioni relative al buon esito del processo di conservazione, che costituiscono una esibizione valida e non opponibile in caso di verifiche, controlli ed ispezioni da parte della Pubblica Autorità.