TITOLO DOCUMENTO:	Firma Elettronica Qualificata – Descrizione del Servizio	
TIPO DOCUMENTO:	Descrizione del servizio	
EMESSO DA:	Telecom Italia Trust Technologies S.r.l.	
DATA EMISSIONE	N. ALLEGATI:	STATO:
22/01/2014	0	Rilasciato

REDATTO:	F. Galetta				
VERIFICATO:	A. Tommasone	A.M. Fino			
APPROVATO:	G. Allegrezza	E. Cavallo			
LISTA DI DISTRIBUZIONE:	Documento pubblico				

REGISTRO DELLE MODIFICHE		
REVISIONE	DESCRIZIONE	EMISSIONE
00	Prima emissione (ricodifica del doc. CERTQUAL.IT.SODS092595.03 - Firma Digitale Qualificata Descrizione del servizio)	22/01/2014

Indice degli argomenti

1 Generalità sul documento

Questo documento descrive il servizio **FirmaSicura** (servizio di Certificazione della Firma Elettronica Qualificata) erogato da Telecom Italia Trust Technologies S.r.l. (in breve TI Trust Technologies o Ente Certificatore) e le procedure per la sua gestione.

È liberamente disponibile per la consultazione ed il download sul nostro sito internet: http://www.trusttechnologies.it.

2 Quadro generale di riferimento

2.1 Firma Elettronica Qualificata

La **Firma Elettronica Qualificata** è il risultato della procedura informatica che consente a chi firma un documento digitale di rendere manifesta la sua volontà e di garantire:

- l'***autenticità***, cioè che il documento è originale, redatto dal titolare del certificato di firma digitale con il quale è stato firmato;
- il ***non ripudio***, la firma digitale si presume riconducibile al titolare del dispositivo di firma, salvo che lui ne dimostri prova contraria;
- l'***integrità***, ovvero che il documento non sia stato soggetto a modifiche di alcun tipo dopo essere stato firmato;

La Firma Elettronica Qualificata conferisce al documento **validità legale**. Il documento informatico sottoscritto con Firma Elettronica Qualificata (nel rispetto della normativa vigente) soddisfa il requisito legale della forma scritta che garantisce l'identificabilità dell'autore e l'integrità del documento.

La **Firma Elettronica Qualificata** è un particolare tipo di Firma Elettronica Avanzata[1] basata su un certificato qualificato emesso da un Certificatore Accreditato[2] e basata sull'utilizzo di un dispositivo sicuro per la creazione della firma.

La Firma Elettronica Qualificata costituisce quindi l'equivalente elettronico di una tradizionale firma autografa apposta su carta, ed ha il suo stesso valore legale. Attraverso l'apposizione della Firma Elettronica Qualificata è possibile nei confronti di un documento informatico:

- sottoscriverne il contenuto;
- assicurarne la provenienza;
- garantire l'inalterabilità delle informazioni che contiene.

Possono dotarsi della Firma Elettronica Qualificata tutte le persone fisiche.

[1] La Firma Elettronica Avanzata, di più recente specificazione rispetto alle altre tipologie di firma, è definita come un insieme di dati in forma elettronica allegati oppure connessi a un documento informatico che consentono l'identificazione del firmatario del documento e garantiscono la connessione univoca al firmatario, creati con mezzi sui quali il firmatario può conservare un controllo esclusivo, collegati ai dati ai quali detta firma si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati.

[2] Per essere Certificatore Accreditato è necessario aver ottenuto l'autorizzazione, a svolgere l'attività, presso l'Agenzia per l'Italia Digitale – AgID (ex DigitPA). L'accreditamento comporta l'inclusione in un apposito elenco pubblicato sul sito http://www.digitpa.gov.it, liberamente consultabile.

2.2 Il processo di Firma

Secondo la normativa in vigore, la Firma Elettronica Qualificata è un particolare tipo di firma elettronica avanzata che possieda **i requisiti seguenti**:

a) basata su un certificato qualificato;
b) generata mediante un dispositivo sicuro di firma;
c) basata sulla crittografia asimmetrica a chiave pubblica e a chiave privata.

In generale, il processo di **firma elettronica** avviene in tre fasi:

1 **Generazione dell'impronta digitale**: nella prima fase viene applicata al documento originale una funzione di *hash*, ossia uno specifico algoritmo matematico che permette di ottenere, a partire da una sequenza di bit di lunghezza qualunque, un'altra sequenza di bit di lunghezza prefissata chiamata **impronta** (*hash*). Tale impronta è univoca e non reversibile, pertanto uno specifico documento genererà sempre e solo quella stessa impronta e dall'impronta generata non sarà mai possibile risalire al contenuto del documento che l'ha generata.

L'analogia con le impronte digitali è molto forte: le impronte digitali, infatti, consentono l'identificazione di una persona anche se non contengono alcuna informazione sull'individuo stesso. Dalle impronte digitali non è possibile ricostruire, ad esempio, "il profilo" psicologico della persona così come dall'impronta digitale non si può risalire al contenuto del documento.

La peculiarità più interessante delle funzioni di hash normalmente impiegate dalla tecnologia della firma elettronica, consiste nel fatto che due diverse sequenze di bit originarie, anche se differiscono fra loro di un solo bit, producono impronte diverse. Da questo deriva l'unicità dell'impronta e le sue caratteristiche di sicurezza.

Inoltre, data la complessità dell'algoritmo matematico utilizzato, in base allo stato dell'arte è ritenuto assolutamente impossibile risalire alla sequenza di bit originaria partendo dall'impronta.

L'uso delle funzioni di hash consente di evitare che, per la generazione della firma, sia necessario applicare l'algoritmo di cifratura (vedere al punto successivo), che è intrinsecamente inefficiente (e dunque molto lento), all'intero testo che può essere molto lungo. Inoltre consente l'autenticazione, da parte di un terzo soggetto fidato e riconosciuto, della sottoscrizione di un documento senza che questa venga a conoscenza del suo contenuto.

2 **Generazione della firma**: La seconda fase del processo consiste nella cifratura, con la propria chiave privata, dell'impronta del documento generata in precedenza. In questo modo la firma risulta legata, da un lato (attraverso la chiave privata usata per la generazione) al soggetto sottoscrittore, e dall'altro (per il tramite dell'impronta) al testo sottoscritto. Questo dualismo lega inequivocabilmente e indissolubilmente la firma al soggetto ed al documento. Una specifica firma sarà sempre e solo legata ad un solo soggetto ed un solo documento.

In realtà, per completezza di informazione, l'operazione di cifratura viene effettuata, anziché sulla sola impronta, su una struttura di dati che la contiene insieme con altre informazioni utili, quali ad esempio l'indicazione della funzione hash usata per la sua generazione. Sebbene tali informazioni possano essere fornite separatamente rispetto alla firma, la loro inclusione nell'operazione di codifica ne garantisce l'autenticità e allo stesso tempo semplifica il sistema di trasmissione e successiva verifica del documento firmato (viene trasmesso un unico messaggio contenente tutte le informazioni necessarie per la verifica).

3 **Apposizione e verifica della firma**: Nell'ultima fase, la firma elettronica generata precedentemente viene aggiunta al testo del documento (che di solito è in chiaro) in una posizione predefinita all'interno

di una speciale "busta informatica". Insieme con la firma vera e propria, viene allegato al documento anche il certificato del firmatario da cui è possibile recuperare il valore della chiave pubblica in fase di verifica. I formati delle buste informatiche utilizzabili nella Firma Elettronica Qualificata in Italia sono stabiliti dalla norma e sono basati su standard europei.

Per l'operazione di **verifica** della Firma Elettronica Qualificata (e quindi della originalità del documento firmato) è sufficiente disporre della chiave pubblica del firmatario. Questa in genere viene resa disponibile direttamente tramite il suo certificato qualificato che viene incluso nel documento firmato.

La verifica viene effettuata ricalcolando, con la medesima funzione di hash usata nella fase di firma, il valore dell'impronta del documento (hash calcolato); poi si decifra con la chiave pubblica del firmatario la firma (hash firmato) controllando che il valore così ottenuto coincida con l'hash calcolato (coincidenza degli hash).

Per poter generare firme digitali è necessario essere dotati di:

- un certificato qualificato di sottoscrizione;
- un dispositivo sicuro per la generazione delle firme (per es. smart card o token USB) che custodisce la chiave privata corrispondente al certificato qualificato;
- un apposito lettore nel caso in cui si utilizzi una smart card;
- i codici riservati necessari per utilizzare il certificato (PIN, PUK);
- un software in grado di interagire con il dispositivo sicuro di firma. Tale software effettua in maniera automatica le operazioni di generazione e di verifica della firma sopra elencate.

2.3 Obiettivi del servizio e vantaggi per gli utilizzatori

Dalle caratteristiche proprie della Firma Elettronica Qualificata (autenticità, integrità, non ripudiabilità, valore legale), scaturiscono una serie di **vantaggi** per gli utilizzatori, che possono avere importanti ripercussioni economiche:

- notevole **semplificazione dei rapporti tra le aziende** e tra queste e la pubblica amministrazione;
- **dematerializzazione** di gran parte dei documenti cartacei presenti in azienda e loro conservazione sotto forma di registrazione digitale, ciò grazie alla possibilità di archiviare su supporti informatici i documenti firmati da conservare in originale;
- estrema **facilità di fruizione**, anche remota, dei documenti conservati e archiviati su supporti informatici (anche centralizzati quali sono i sistemi di storage) rispetto a documenti cartacei;
- **inalterabilità della documentazione** archiviata su supporti informatici nel tempo (utilizzando apposite tecniche i supporti informatici non sono soggetti, o lo sono molto meno, all'usura che il tempo e la conservazione impropria introduce sui documenti cartacei);
- **razionalizzazione degli spazi dedicati all'archiviazione** dei documenti (un supporto informatico occupa, a parità di documentazione conservata, molto meno spazio rispetto ad un archivio cartaceo);
- **eliminazione di timbri e simili** in quanto, ai sensi del DPR 445/2000, articolo 23 R, comma 6 "l'apposizione di firma digitale integra e sostituisce, ad ogni fine previsto dalla normativa vigente, l'apposizione di sigilli, punzoni, timbri, contrassegni e marchi di qualsiasi genere";
- possibilità di apposizione di uno speciale 'bollo' firmato da un ente certificatore e chiamato **marcatura temporale** che attesta in modo certo ed opponibile a terzi il **momento temporale** di sottoscrizione di un documento;
- **tempestività nella stipula**, giuridicamente vincolante, di rapporti contrattuali anche a grandi distanze, senza necessità di spostamenti di persone o di spedizioni di materiale.

A fronte degli innegabili vantaggi, la Firma Elettronica Qualificata non è esente da alcuni **punti di debolezza** che mantengono però un basso impatto rispetto agli aspetti positivi:

- la Firma Elettronica Qualificata è una stringa che viene creata crittografando un'impronta del documento informatico che si sottoscrive ed è quindi univocamente associata ad esso. È possibile che il documento originario, una volta aperto, modifichi se stesso in base al codice in esso contenuto, per esempio uno script o delle funzioni automatizzate (es. per mezzo di macroistruzioni o simili) o, caso tipico, un campo che contiene la data attuale di sistema. *Per garantire l'integrità del documento sottoscritto la normativa tecnica richiede di apporre firme digitali solo a formati statici di documento, tali formati presentano sempre lo stesso contenuto informativo a chiunque li visualizzi nel tempo*;
- la Firma Elettronica Qualificata è basata su speciali algoritmi crittografici sicuri ma, in linea di principio è possibile risalire, per tentativi, alla chiave privata di una persona o di un ente partendo dalla sua chiave pubblica. Al momento, la potenza computazionale richiesta per un'operazione del genere è ipotizzabile solo su sistemi di dimensioni, prestazioni e costi elevatissimi, cioè su sistemi imponenti di computer collegati assieme che sfruttano le singole capacità di calcolo sommandole per ottenere potenze di computazione non ottenibili normalmente.
  Esistono appositi comitati internazionali di tecnici e di specialisti che tengono sotto osservazione la ricerca internazionale e prevedono opportuni piani di accrescimento dei parametri utilizzati (es. lunghezza minima delle chiavi) oppure l'utilizzo di nuovi algoritmi di hash. L'AgID ha in Italia, attraverso apposite Deliberazioni, la responsabilità di indicare i parametri tecnologici da utilizzare per la sicurezza della Firma Digitale.

2.4 Quadro normativo di riferimento

La storia italiana del documento informatico e della firma elettronica inizia con l'articolo 15, comma 2 della Legge 15 marzo 1997, n. 59 secondo il quale i "documenti formati dalla pubblica amministrazione con strumenti informatici o telematici nonché la loro archiviazione e trasmissione con strumenti informatici sono validi e rilevanti a tutti gli effetti di legge".

A partire da allora, una serie di provvedimenti legislativi hanno conferito valore giuridico al documento informatico e alla firma elettronica. Inoltre il processo legislativo ha anche fornito delle indicazioni sulle tecnologie da impiegare per ottenere delle firme elettroniche che possono ritenersi equivalenti a quelle autografe.

La Firma Elettronica Qualificata è lo strumento abilitante per l'intero sistema della "dematerializzazione" della documentazione cartacea. Può essere pienamente utilizzata come strumento che garantisce autenticità, paternità e integrità, non solo per la sottoscrizione del documento informatico, ma anche nella conservazione documentale sostitutiva, nella fatturazione elettronica, nello scambio di documenti informatici in procedimenti amministrativi che hanno eliminato la carta.

2.4.1 Normative

Le norme ad oggi in vigore, su cui si fonda la regolamentazione normativa della Firma Elettronica Qualificata, sono elencate nella tabella sottostante che riporta anche una breve descrizione dei contenuti e dei punti rilevanti della norma stessa.

Norma	Descrizione
Legge 15 marzo 1997, n. 59 (G.U. del 17 marzo 1997, n. 63), "Delega al Governo per il conferimento di funzioni e compiti alle regioni ed enti locali, per la riforma della Pubblica Amministrazione e per la semplificazione	Stabilisce che "*gli atti, dati e documenti formati dalla pubblica amministrazione e dai privati con strumenti informatici o telematici, i contratti stipulati nelle medesime forme, nonché la loro archiviazione e trasmissione con strumenti informatici, sono validi a tutti gli effetti di legge*".

amministrativa"	
D. Lgs. del 7 marzo 2005, n. 82 (G.U. del 16 maggio 2005, n. 93), "Codice dell'amministrazione digitale (CAD)" e successive modifiche	Costituisce il principale strumento giuridico per le applicazioni delle nuove tecnologie alla Pubblica Amministrazione. In particolare, in merito alla firma, il decreto: • sancisce che il documento informatico, sottoscritto con firma digitale o con un altro tipo di Firma Elettronica Qualificata, ha l'efficacia prevista dall'articolo 2702 del codice civile (*firma autografa*): "*La scrittura privata fa piena prova, fino a querela di falso (Cod. Proc. Civ. 221 e seguenti), della provenienza delle dichiarazioni da chi l'ha sottoscritta, se colui contro il quale la scrittura è prodotta ne riconosce la sottoscrizione, ovvero se questa e legalmente considerata come riconosciuta*"; • sancisce che l'apposizione ad un documento informatico di una firma digitale o di un altro tipo di Firma Elettronica Qualificata basata su un certificato elettronico revocato, scaduto o sospeso equivale a mancata sottoscrizione; • stabilisce che la firma digitale deve riferirsi in maniera univoca ad un solo soggetto ed al documento o all'insieme di documenti cui e' apposta o associata; • distingue fra tre tipi di firma: o Firma elettronica; o Firma Elettronica Qualificata; o Firma digitale. Il decreto attribuisce solo alle ultime due tipologie massima efficacia probatoria in quanto conferiscono al documento su cui sono apposte, le caratteristiche di integrità, non modificabilità e di sicurezza. Invece un documento informatico su cui e' apposta una firma elettronica, e' liberamente valutabile in giudizio. • distingue fra due tipi di certificato: o elettronico (non qualificato); o qualificato. • distingue fra due tipologie di certificatori: o certificatori qualificati; o certificatori accreditati.
DPCM 30 MARZO 2009 *"Regole Tecniche in materia di generazione, apposizione e verifica delle firma digitali e validazione temporale dei documenti informatici."* (G.U. del 6 giugno 2009, n. 129)	Sostituisce il DPCM 13 gennaio 2004. "*Stabilisce le regole tecniche per la generazione, apposizione e verifica delle firme elettroniche qualificate e per la validazione temporale, nonché per lo svolgimento delle attività dei certificatori qualificati*". In particolare il decreto: • definisce le modalità di generazione e conservazione delle chiavi; • definisce i requisiti dei dispositivi sicuri di firma e le procedure per la generazione della firma; • stabilisce l'onere per i certificatori che rilasciano certificati

	qualificati di indicare almeno un sistema che consenta di effettuare la verifica delle firme digitali; • definisce le modalità operative e procedurali delle attività di revoca e sospensione dei certificati qualificati; identifica i requisiti e gli obblighi dei certificatori che rilasciano certificati qualificati.

Tale quadro normativo è completato dalla documentazione prodotta dall'ente di vigilanza (Circolari, Raccomandazioni e Norme Integrative emesse da DigitPA), che dispone in materia di regolamentazione e standardizzazione tecnico operativa, che, in sintesi:

1. indica le linee guida per garantire l'omogeneità operativa e la corretta interazione tra gli utenti che utilizzano la firma digitale e la massima diffusione ed efficienza dei processi connessi alla firma digitale (Circolare n. AIPA/CR/22 del 19 giugno 2000, G.U. 30 giugno 2000, n. 151);
2. stabilisce le regole tecniche in materia di formazione e conservazione di documenti informatici delle pubbliche amministrazioni, in particolare prevede che i formati dei documenti informatici adottati dalla PA, possiedano almeno i requisiti di non alterabilità del documento durante le fasi di accesso e conservazione e di immutabilità nel tempo del contenuto e della sua struttura. A tale fine i documenti informatici non devono contenere macroistruzioni o codice eseguibile, tali da attivare funzionalità che possano modificarne la struttura o il contenuto (Deliberazione CNIPA del 23 novembre 2000, n.51/2000);
3. indica le linee guida per l'utilizzo della firma digitale, fornendo le differenze sostanziali fra le varie tipologie di firme elettroniche, le indicazioni per le procedure di firma digitale di un singolo documento e di firma con procedure automatiche, le modalità con cui è possibile dotarsi di un dispositivo di firma digitale, come effettuare la verifica di una firma digitale e gli utilizzi pratici (Linee guida per l'utilizzo della Firma Digitale, maggio 2004);
4. stabilisce le regole per il riconoscimento e la verifica del documento informatico (Deliberazione CNIPA 17 febbraio 2005 – Deliberazione n.4/2005, GU del 3 marzo 2005, n.51);
5. indica le modalità con le quali i soggetti (pubblici e privati) devono presentare domanda di accreditamento (Circolare CNIPA 6 settembre 2005, n.48, G.U. 13 settembre 2007, n. 213);
6. definisce le regole tecniche per la definizione dei formati standard di busta crittografica per la firma digitale in linguaggio XML (Deliberazione CNIPA 18 maggio 2006 – Deliberazione n.34/06, GU del 3 ottobre 2006, n.230);
7. stabilisce i principi essenziali che regolano lo svolgimento delle "funzioni di vigilanza e controllo sull'attività dei certificatori qualificati e accreditati" di cui all'articolo 31 del decreto legislativo 7 marzo 2005, n. 82, "Codice della amministrazione digitale".(G.U. 23 febbraio 2007, n. 45) (Circolare CNIPA 15 febbraio 2007, n.52, G.U. 23 febbraio 2007, n. 45);
8. impone (Deliberazione n. 45/2009, GU 3 dicembre 2009 n. 282):
    - il passaggio dall'algoritmo di hash denominato SHA-1 a quello denominato SHA-256 in tutti gli utilizzi previsti per il primo (certificati, firma, marca temporale, etc.).
    - il passaggio dall'attuale associazione della marca temporale dell'intero documento alla marcatura temporale della singola firma apposta al documento in maniera contestuale ad essa. La marcatura dell'intero documento originale è ancora possibile ma con uno specifico nuovo formato;
    - il passaggio ai formati di firma (buste crittografiche) conformi agli standard europei, nelle diverse loro varianti: CAdES per il PKCS#7, PAdES per il PDF e XAdES per l'XML.

      La Deliberazione n. 45/2009 è stata successivamente integrata dalla Determinazione Commisariale n° 69/2010 del 28 luglio 2010, GU 17/08/2010 che, tra le altre cose, proroga dal 31/08/2010 al 31/12/2010 il termine ultimo per l'adeguamento del formato di firma digitale (passaggio all'algoritmo SHA-256) e stabilisce la validità delle firme digitali basate sulle regole vigenti prima dell'entrata in vigore della deliberazione stessa, purché generate entro il 30 giugno 2011.

3 Descrizione del servizio di Firma Elettronica Qualificata di TI Trust Technologies

FirmaSicura è il servizio di Firma Elettronica Qualificata che TI Trust Technologies offre in qualità di Certificatore Accreditato presso AgID (ex DigitPA) sin dall'aprile del 2000.

Il servizio prevede l'emissione e la gestione di certificati digitali di sottoscrizione in linea con le policy di certificazione (Manuale Operativo) pubblicate sul sito http://www.digitpa.gov.it.

Gli utenti vengono dotati di Firma Elettronica Qualificata mediante un preventivo processo di registrazione presso TI Trust Technologies, che ha la responsabilità di identificare chi richiede un certificato digitale e di procedere alla corretta registrazione dei suoi dati.

All'utente (il Titolare) del servizio **FirmaSicura** viene fornito un kit così composto:

- un **certificato di Firma Elettronica Qualificata "FirmaSicura"**, con scadenza dipendente dal livello di servizio acquistato;
- un dispositivo sicuro per la creazione della firma: la **smart card o il token USB**;
- un **lettore di smart card** (nel solo caso di utilizzo della smart card);
- il **software client di firma e verifica** corredato di manuale d'uso;

Per ciascun Titolare di FirmaSicura, sono garantite le seguenti attività:

- generazione delle chiavi di sottoscrizione con l'eventuale personalizzazione del dispositivo di firma;
- emissione del certificato qualificato;
- presidio telefonico H24 7x7 per la gestione delle richieste di sospensione cautelativa del certificato;
- supporto tecnico per la risoluzione dei problemi nell'utilizzo dei dispositivi HW e SW forniti (smart card, lettori, ecc.) oppure nel servizio di registrazione.

3.1 Punti di forza

3.1.1 Servizio di identificazione e formazione a domicilio

Preliminarmente all'emissione di un certificato di Firma Elettronica Qualificata è necessario che il Certificatore identifichi e registri il richiedente. Le informazioni raccolte in questa fase sono essenziali sia per tenere traccia dell'associazione tra gli utenti e loro chiavi crittografiche, sia per poterne autenticare, in un secondo tempo, le richieste di rilascio, di revoca e di rinnovo dei certificati.

La legge prescrive che il riconoscimento del richiedente sia effettuata con certezza da parte del Certificatore stesso o da una persona da questo delegata.

Al fine di agevolare i propri clienti, TI Trust Technologies offre la possibilità di effettuare le operazioni di **identificazione e registrazione dei richiedenti *on site***, presso le loro sedi su tutto il territorio nazionale. Contestualmente all'operazione di identificazione e di registrazione, il personale che cura l'operazione effettua tutte le installazioni necessarie e fornisce al cliente tutte le informazioni essenziali per l'uso del servizio.

3.1.2 Possibilità di supporti alternativi alla smart card

Come descritto in precedenza, il supporto tipico utilizzato per l'apposizione della Firma Elettronica Qualificata è la smart card. Tale dispositivo, che richiede un apposito lettore, è tipicamente scelto da

clienti per cui è importante la personalizzazione grafica della smart card stessa (es. utilizzo della smart card anche come tesserino di riconoscimento all'interno della propria azienda/organizzazione).

TI Trust Technologies offre due alternative ai clienti che necessitano di dispositivi differenti a seconda del contesto d'uso o per esigenze specifiche:

1. l'utilizzo di **smart card con formato SIM**, cioè smart card simili (nella forma) alle SIM del telefono cellulare, da inserire in lettori di smart card (forniti da TI Trust Technologies) aventi formato del tipo di dispositivi di memoria USB e tipicamente uno spazio di memoria di massa di alcuni GByte.

   Questi dispositivi consentono la sottoscrizione di un documento da qualsiasi postazione di lavoro senza la necessità di installare alcun driver o software.
2. l'utilizzo di **token USB**, ovvero dispositivi che hanno la caratteristica di contenere il certificato di firma. L'utilizzo di questi dispositivi prevede l'installazione, sul PC del titolare, di driver per l'utilizzo del token e del software di firma.

TI Trust Technologies offre, infine, su base progettuale e non, ulteriori alternative per il servizio di Firma Elettronica, quali i servizi di Firma Elettronica Avanzata:

- Firma Sicura Mobile;
- Firma Remota Massiva;
- Firma Remota Biometrica.

3.1.3 Software di firma e verifica

TI Trust Technologies distribuisce ai Titolari del servizio Firma Sicura un software di firma e verifica conforme ai requisiti della legge italiana.

Il software possiede queste caratteristiche:

- gestione della procedura di Firma Elettronica Qualificata, conformemente ai requisiti della normativa vigente in materia di Firma Elettronica Qualificata e documento informatico;
- possibilità di firmare con semplicità d'uso qualsiasi tipo di documento elettronico originale;
- nessun limite alla dimensione del documento da firmare;
- possibilità di associare più firme ad uno stesso documento;
- apposizione e verifica delle marche temporali;
- verifica di tutte le firme digitali e le marche temporali presenti in un documento;
- interoperabilità con i diversi Certificatori accreditati;
- funzionamento con i più diffusi ambienti operativi: Microsoft Windows, Linux, Apple Mac OSX.

3.1.4 Supporto tecnico

I titolari del servizio FirmaSicura possono rivolgersi ad un help-desk in grado di risolvere problematiche di tipo tecnico. Il supporto è erogato, infatti, da un team specialistico che aiuta il cliente durante tutto il ciclo di vita del servizio; dai problemi che possono sorgere in fase di attivazione/configurazione del servizio stesso fino ad interventi con carattere di urgenza quali, ad esempio, il ripristino del servizio oppure la sospensione cautelativa di un certificato.

L'help-desk è raggiungibile tramite il numero verde nazionale **800.28.75.24** ed ha le seguenti caratteristiche:

1. servizio di segnalazione inconvenienti: 24 ore su 24, 7 giorni su 7;
2. servizi di sospensione cautelativa dei certificati: 24 ore su 24, 7 giorni su 7.
3. servizi di assistenza di altro genere (commerciale, informativa, ecc.): dal lunedì al sabato, dalle 8.00 alle 16.30, festivi esclusi;

Le procedure di accesso ai servizi di supporto tecnico prevedono l'identificazione del cliente mediante codici di riconoscimento e/o password. Questa prima fase di identificazione ha il duplice scopo di

impedire un utilizzo fraudolento e di fornire ai tecnici la specifica esatta del servizio sottoscritto dal cliente per il quale si richiede supporto.

Terminata la fase di identificazione, i tecnici provvedono ad una prima analisi dell'anomalia segnalata (analisi di 1° livello), assegnando un grado di severità e un codice di priorità. Questa fase prevede l'apertura di uno specifico "cartellino di guasto" (trouble-ticket) per il tracciamento storico ed una successiva analisi comparativa dei guasti e delle loro cause al fine di adottare azioni correttive.

Nel corso dell'analisi di 1° livello è anche possibile, qualora non siano necessari ulteriori interventi da parte di specialisti, la immediata risoluzione del problema. In caso contrario l'anomalia verrà fatta scalare ai tecnici specialistici di 2° livello.

Alla soluzione dell'anomalia il cliente viene avvisato del ripristino completo del servizio e guidato nella verifica della funzionalità al fine di chiudere la segnalazione.

3.2 Servizi Accessori ed Opzionali

3.2.1 Marcatura Temporale (Time Stamping)

La **marca temporale** è un importante strumento che assegna data ed ora certa ad un documento informatico.

TI Trust Technologies, in qualità di Certificatore Accreditato, eroga nel rispetto di una rigida normativa e regolamentazione tecnica un servizio di marcatura temporale che è basato su orologi molto precisi (scarto massimo inferiore a 1 secondo rispetto al ***tempo universale coordinato*** ufficiale, **UTC**).

In genere il soggetto che desidera una marca temporale trasmette all'ente certificatore l'impronta della firma che ha appena apposto a un documento informatico.

Il server di marcatura temporale aggiunge all'impronta l'informazione relativa alla data e all'ora dell'istante in cui elabora la richiesta, quindi calcola su tale insieme di informazioni una Firma Elettronica Qualificata tramite una propria *chiave di marcatura temporale* dedicata (per legge il tempo impiegato per la risposta non deve eccedere il minuto dalla ricezione della richiesta).

Il server restituisce quindi la marca temporale firmata.

Il soggetto allega la marca temporale alla firma del documento. Poiché la marca contiene la Firma Elettronica Qualificata di **un'autorità esterna** e contiene altresì l'impronta del documento, non sarà più possibile negare l'esistenza del documento in tale data ed ora. La marca temporale è un'informazione opponibile a terzi ai sensi della normativa vigente.

3.3 Caratterizzazione del servizio

3.3.1 Cosa comprende la fornitura

La fornitura del servizio di FirmaSicura comprende i seguenti elementi:

- Emissione dei certificati qualificati di sottoscrizione con validità temporale specifica (anni);
- Smart card e relativo lettore USB (o Token USB) contenente le chiavi crittografiche e i certificati;
- Credenziali per l'accesso ai certificati (busta oscurata con PIN, PUK e codice di emergenza);
- Software client per la firma e la verifica dei documenti informatici;
- Numero Verde per l'assistenza ai Clienti (800-287524);
- Servizio di Marcatura Temporale (opzionale);
- Servizio di Identificazione on-site dei Titolari (opzionale).

3.3.2 Cosa è escluso dalla fornitura

Nella fornitura del servizio standard di FirmaSicura è escluso lo sviluppo di eventuali interfacce software necessarie all'integrazione automatizzata di applicativi esterni con il servizio.

I servizi opzionali descritti nel paragrafo 2.2 sono esclusi dalla configurazione di base del servizio.

3.3.3 Integrazione con gli altri servizi di TI Trust Technologies

Il servizio di Firma Elettronica Qualificata denominato **FirmaSicura** può essere integrato con gli altri servizi di certificazione offerti da TI Trust Technologies, quali:

- la **Posta Elettronica Certificata (PEC)**, ovvero il servizio in grado di conferire pieno valore legale alla trasmissione di un messaggio e-mail da un mittente ad un destinatario, in quanto fornisce al mittente la documentazione elettronica, con valenza legale, che attesta l'invio e la consegna di documenti informatici;
- il servizio di **Marcatura Temporale**, mediante il quale si accerta l'esistenza e la validità del documento sottoscritto ad una certa data. Si tratta di un elemento importante del servizio, oggettivamente essenziale, perché in caso di mancata apposizione della marca temporale, la verifica della validità della firma effettuata successivamente alla scadenza del certificato con il quale il documento è stato sottoscritto darà esito negativo, compromettendo la validità del documento stesso.
- il servizio di **Conservazione Sostitutiva**, ovvero la soluzione che consente di conservare in formato elettronico, senza l'obbligo della stampa cartacea, documenti di cui la legge richiede la conservazione (es. fatture, libri bollati, registri IVA, …).

L'insieme di questi servizi (firma elettronica, marcatura temporale, PEC e conservazione sostitutiva) permette la gestione in elettronico di tutte le fasi del ciclo di vita di un documento informatico. Dalla sua creazione, la sua consultazione e trasmissione, fino alla sua conservazione per tutto il tempo necessario, consentendo in tal modo la **dematerializzazione** del documento cartaceo.

4 Cosa fare per ...

Le procedure sotto descritte prevedono le seguenti figure:

Certificatore	Il soggetto che eroga il servizio (TI Trust Technologies).
Cliente	Il soggetto che acquista il servizio per l'utilizzo da parte di soggetti (Titolari) ad esso afferenti.
Referente del Cliente	Il soggetto che cura le fasi di pre-sales e sales ed è coinvolto nella prima fase di delivery del servizio al Cliente. In generale Telecom Italia.
Titolare	La persona che richiede e utilizza il servizio di firma.
Incaricato della identificazione e della consegna delle buste	La persona, appartenente in genere all'organizzazione del cliente, a cui il Certificatore ed il Cliente delegano formalmente le attività di identificazione e registrazione dei titolari e di consegna delle informazioni per l'utilizzo del servizio.
Incaricato del Certificatore	La persona, appartenente in genere all'organizzazione del Certificatore, che effettua l'identificazione e la registrazione dei titolari e consegna loro le informazioni per l'utilizzo del servizio (figura prevista solo nel caso di procedura diretta di attivazione).

4.1 ... attivare il servizio

I clienti che sottoscrivono il servizio di FirmaSicura di TI Trust Technologies hanno la possibilità di scegliere tra due diverse **procedure di attivazione del servizio**, che, in sostanza, si differenziano per le modalità di identificazione dei Titolari. In particolare, si distingue tra:

1. **Procedura Indiretta**: prevede che le attività di identificazione e registrazione dei Titolari, nonché di consegna loro delle informazioni per l'utilizzo del servizio sia effettuata da **personale interno all'organizzazione del cliente (**Incaricato dell'identificazione e della consegna delle buste). Tali **Incaricati** sono a loro volta identificati da TI Trust Technologies presso la sede della stessa TI Trust Technologies.

   In tal caso, per soddisfare specifiche esigenze del cliente, è possibile prevedere inoltre una sorta di gerarchizzazione degli Incaricati, distinguendo in:

   - **PRIMI Incaricati, *identificati da TI Trust Technologies*:** incaricati "supervisori" con il compito di gestire (anche nei confronti di TI Trust Technologies) tutti gli altri eventuali propri Incaricati ed i Titolari;
   - **ALTRI Incaricati**, ***identificati dai PRIMI Incaricati***: che hanno il compito di identificare i Titolari e richiedere per loro l'attivazione del servizio.

2. **Procedura Diretta**: prevede che le attività di identificazione e registrazione dei Titolari, nonché di consegna loro delle informazioni per l'utilizzo del servizio, siano effettuate dal Certificatore o da altra società specificamente incaricata, e si svolgano presso la sede TI Trust Technologies ovvero quella del Titolare.

4.1.1 Procedura Indiretta senza gerarchizzazione degli Incaricati

L'attivazione del servizio di FirmaSicura prevede che siano completate le seguenti macro fasi:

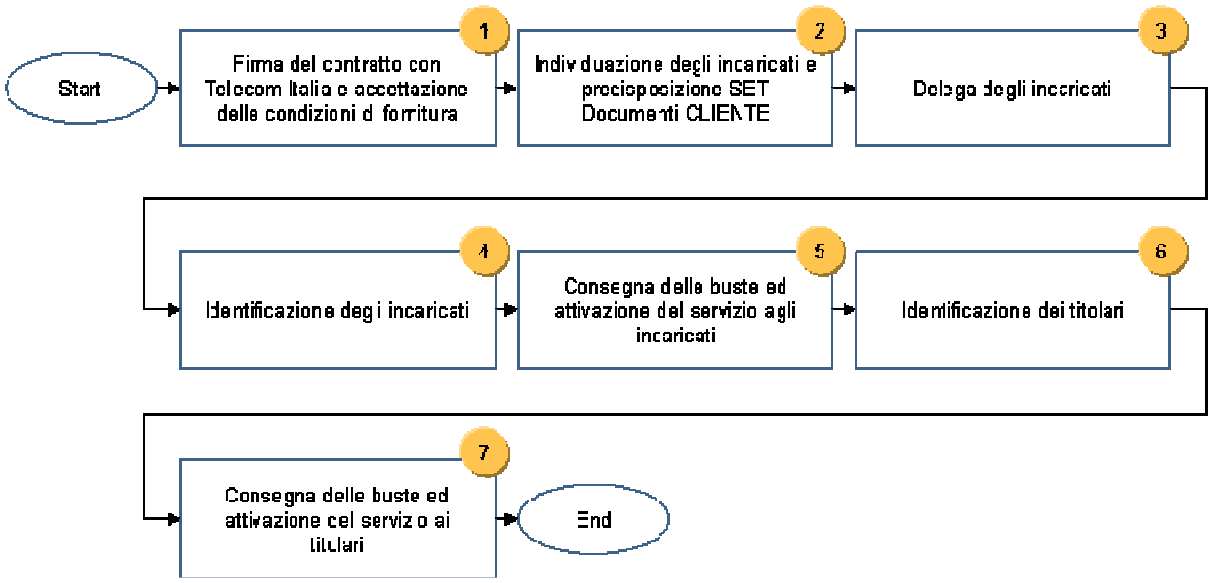
1. firma del contratto di fornitura fra il Cliente e il Referente del Cliente (Telecom Italia) e delle condizioni di fornitura del servizio;
2. identificazione ed attivazione degli Incaricati;

3. identificazione ed attivazione dei Titolari.

La procedura prevede inoltre la compilazione e la sottoscrizione di tre SET di documenti:

1. **SET DOCUMENTI CLIENTE** che comprende:
   - Lettera di incarico
   - Scheda di attivazione
   - Informativa trattamento dati
   - Condizioni di utilizzo del servizio
2. **SET DOCUMENTI INCARICATO** che comprende:
   - Lettera di delega
   - Scheda di attivazione incaricato
3. **SET DOCUMENTI TITOLARE** che comprende
   - Informativa trattamento dati
   - Condizioni di utilizzo del servizio
   - Richiesta emissione del certificato digitale
   - Modulo di registrazione, nel caso in cui il Titolare utilizzi la firma come persona giuridica, contiene i dati del terzo interessato

La figura sottostante rappresenta, schematicamente, il macro processo di attivazione del servizio nella modalità indiretta:



Id	Macro Fase	Descrizione
1	Firma del contratto con Telecom e accettazione delle condizioni di fornitura	Il cliente firma il contratto con Telecom Italia, accetta le condizioni di fornitura del servizio richiedendone l'attivazione stessa.

2	Individuazione Incaricati per l'identificazione e la consegna delle buste e degli eventuali dispositivi di firma e predisposizione SET DOCUMENTI CLIENTE	Il cliente (referente) individua le risorse interne che agiranno in qualità di incaricati dell'identificazione e della consegna delle buste, compila e sottoscrive i documenti del SET DOCUMENTI CLIENTE e li anticipa via fax/mail all'ente certificatore. Oltre al SET DOCUMENTI CLIENTE, il cliente (referente) invia all'ente certificatore le fotocopie dei documenti di identità e del codice fiscale degli incaricati per l'identificazione e la consegna delle buste oscurate e degli eventuali dispositivi di firma.
3	Delega formale degli incaricati	L'ente certificatore, ricevuto il SET Documenti CLIENTE, predispone una lettera di delega e la invia al cliente (referente) perché la faccia sottoscrivere dal proprio incaricato. Tale documento delega formalmente gli incaricati all'espletamento delle attività di identificazione e consegna delle informazioni per l'utilizzo del servizio.
4	Identificazione degli incaricati	Gli incaricati, previo appuntamento, si recano presso la sede dell'ente certificatore per l'identificazione. In tale contesto vengono consegnati all'ente certificatore i documenti originali e sottoscritti del SET DOCUMENTI CLIENTE. Raccolta la documentazione l'ente certificatore procede all'identificazione degli incaricati.
5	Consegna delle buste e degli eventuali dispositivi di firma ed attivazione degli incaricati	Il funzionario dell'Ente Certificatore consegna agli incaricati le buste contenenti le informazioni per l'utilizzo del servizio e per la successiva attivazione dei titolari e gli eventuali dispositivi di firma. Gli incaricati immettono e sottoscrivono la richiesta di attivazione dei certificati connettendosi al sito di provisioning del servizio di Firma Elettronica Qualificata. Il funzionario dell'Ente Certificatore approva la richiesta e procede con la produzione dei certificati. N.B. E' prevista una modalità di provisioning, definita "*Face to Face*", nella quale la richiesta è approvata direttamente dagli incaricati e la produzione dei certificati viene effettuata in *auto-enrollment* direttamente dagli incaricati stessi.
6	Identificazione dei titolari	I titolari si presentano dall'incaricato per l'identificazione.
7	Consegna delle buste e degli eventuali dispositivi di firma ed attivazione dei titolari	Ciascun incaricato consegna ai titolari le buste contenenti le informazioni per l'utilizzo del servizio e gli eventuali dispositivi di firma. L'incaricato immette e sottoscrive sul sistema di provisioning una richiesta di emissione dei certificati. Il titolare, a sua volta, sottoscrive in formato cartaceo o in formato digitale la richiesta di attivazione dei certificati. Successivamente si procederà con l'attivazione del certificato di firma.

4.1.2 Procedura indiretta con gerarchizzazione degli incaricati

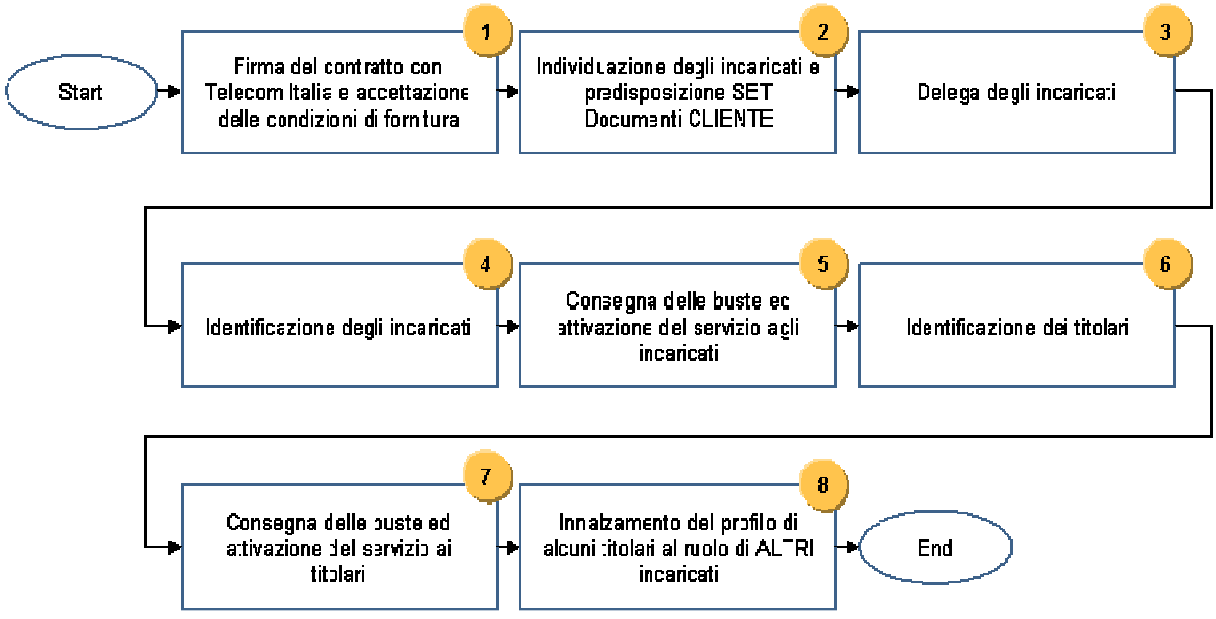
L'attivazione del servizio di Firma Elettronica Qualificata prevede che siano completate le seguenti macro fasi:

1. firma del contratto di fornitura fra il cliente (organizzazione cui appartiene il titolare) e Telecom Italia e delle condizioni di fornitura del servizio;
2. identificazione ed attivazione del primo incaricato;
3. identificazione ed attivazione dei titolari;
4. innalzamento di alcuni titolari al ruolo di ALTRI Incaricati.

La procedura prevede inoltre la compilazione e la sottoscrizione di tre SET di documenti cartacei:

4. **SET DOCUMENTI CLIENTE** che comprende:
   - Lettera di incarico
   - Scheda di attivazione
   - Informativa trattamento dati
   - Condizioni di utilizzo del servizio
5. **SET DOCUMENTI INCARICATI (PRIMO ED ALTRI)** che comprende:
   - Lettera di delega
   - Scheda di attivazione incaricato
6. **SET DOCUMENTI TITOLARE** che comprende:
   - Informativa trattamento dati
   - Condizioni di utilizzo del servizio
   - Richiesta emissione del certificato digitale
   - Modulo di registrazione, nel caso in cui il Titolare utilizzi la firma come persona giuridica, contiene i dati del terzo interessato

La figura sottostante rappresenta, schematicamente, il macro processo di attivazione del servizio nella modalità indiretta:



Id	Macro Fase	Descrizione
1	Firma del contratto con Telecom e accettazione delle condizioni di fornitura	Il cliente firma il contratto con Telecom Italia, accetta le condizioni di fornitura del servizio richiedendone l'attivazione stessa.
2	Individuazione Incaricati per l'identificazione e la consegna delle buste e degli eventuali dispositivi di firma e predisposizione SET DOCUMENTI CLIENTE	Il cliente (referente) individua le risorse interne che agiranno in qualità di incaricati dell'identificazione e della consegna delle buste, compila e sottoscrive i documenti del SET DOCUMENTI CLIENTE e li anticipa via fax/mail all'ente certificatore. Oltre al SET DOCUMENTI CLIENTE, il cliente (referente) invia all'ente certificatore le fotocopie dei documenti di identità e del codice fiscale degli incaricati per l'identificazione e la consegna delle buste oscurate e degli eventuali dispositivi di firma.
3	Delega formale degli incaricati	L'ente certificatore, ricevuto il SET Documenti CLIENTE, predispone una lettera di delega e la invia al cliente (referente) perché la faccia sottoscrivere dal proprio incaricato. Tale documento delega formalmente gli incaricati all'espletamento delle attività di identificazione e consegna delle informazioni per l'utilizzo del servizio.
4	Identificazione degli incaricati	Gli incaricati, previo appuntamento, si recano presso la sede dell'ente certificatore per l'identificazione. In tale contesto vengono consegnati all'ente certificatore i documenti originali e sottoscritti del SET DOCUMENTI CLIENTE. Raccolta la documentazione l'ente certificatore procede contestualmente con l'attivazione degli incaricati.
5	Consegna delle buste e degli eventuali dispositivi di firma ed attivazione degli incaricati	Il funzionario dell'Ente Certificatore consegna agli incaricati le buste contenenti le informazioni per l'utilizzo del servizio e per la successiva attivazione dei titolari e gli eventuali dispositivi di firma. Gli incaricati immettono e sottoscrivono la richiesta di attivazione dei certificati connettendosi al sito di provisioning del servizio di Firma Elettronica Qualificata. Il funzionario dell'Ente Certificatore approva la richiesta e procede con la produzione dei certificati. N.B. E' prevista una modalità di provisioning, definita "*Face to Face* ", nella quale la richiesta è approvata direttamente dagli incaricati e la produzione dei certificati viene effettuata in *auto-enrollment* direttamente dagli incaricati stessi.
6	Identificazione dei titolari	I titolari si presentano all'incaricato per l'identificazione.
7	Consegna delle buste e degli eventuali dispositivi di firma ed attivazione dei titolari	Ciascun incaricato consegna ai titolari le buste contenenti le informazioni per l'utilizzo del servizio e gli eventuali dispositivi di firma. L'incaricato immette e sottoscrive sul sistema di provisioning una richiesta di emissione dei certificati. Il titolare, a sua volta, sottoscrive la richiesta di attivazione dei certificati connettendosi al sito di provisioning.

8	Innalzamento del profilo di alcuni titolari al ruolo di ALTRI incaricati	Il PRIMO incaricato individua gli ALTRI Incaricati tra gli utenti a cui è stato già attivato il servizio come titolari. Dopo aver espletato le formalità di delega, l'utenza di incaricato è da considerarsi attiva.

4.1.3 Procedura diretta

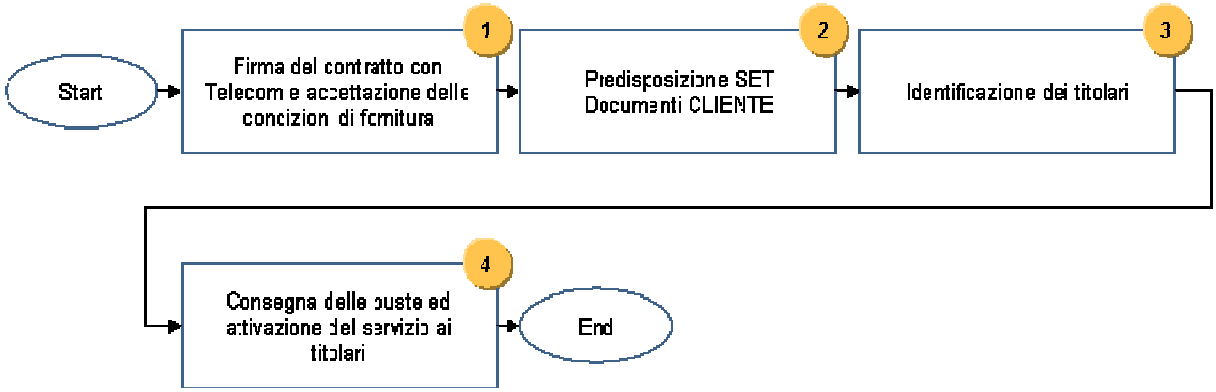
L'attivazione del servizio di Firma Elettronica Qualificata prevede che siano completate le seguenti macro fasi:

1. firma del contratto di fornitura fra il cliente (organizzazione cui appartiene il titolare) e Telecom Italia e delle condizioni di fornitura del servizio
2. identificazione ed attivazione dei titolari.

La procedura prevede inoltre la compilazione e la sottoscrizione di tre SET di documenti cartacei:

7. **SET DOCUMENTI CLIENTE** che comprende:
   - Scheda di attivazione cliente
   - Informativa trattamento dati
   - Condizioni di utilizzo del servizio
8. **SET DOCUMENTI TITOLARE** che comprende
   - Richiesta emissione del certificato digitale
   - Modulo di registrazione, nel caso in cui il Titolare utilizzi la firma come persona giuridica, contiene i dati del terzo interessato
   - Informativa trattamento dati
   - Condizioni di utilizzo del servizio

La figura sottostante rappresenta, schematicamente, il macro processo di attivazione del servizio nella modalità diretta:



Id	Macro Fase	Descrizione
1	Firma del contratto con Telecom e accettazione delle condizioni di fornitura	Il cliente firma il contratto con Telecom Italia, accetta le condizioni di fornitura del servizio richiedendone l'attivazione stessa

2	Predisposizione SET DOCUMENTI CLIENTE	Il cliente (referente) compila e sottoscrive i documenti del SET DOCUMENTI CLIENTE e li anticipa via fax/mail all'ente certificatore. Successivamente il cliente (referente) provvede all'invio degli originali dei documenti via posta.
3	Identificazione dei titolari	Il funzionario di TI Trust Technologies identifica i titolari, previo appuntamento concordato.
4	Consegna delle buste e degli eventuali dispositivi di firma ed attivazione dei titolari	Il funzionario TI Trust Technologies consegna ai titolari le buste contenenti le informazioni per l'utilizzo del servizio e gli eventuali dispositivi di firma. Il funzionario TI Trust Technologies immette e sottoscrive sul sistema di provisioning una richiesta di emissione dei certificati.

4.2 ... rinnovare il servizio

La normativa vigente non prevede la certificazione di chiavi che siano state già certificate, pertanto allo scadere del periodo di validità del certificato è necessaria la sostituzione delle chiavi con nuove coppie di chiavi e quindi l'emissione di un nuovo certificato.

La sostituzione delle chiavi si svolge in modo analogo alla prima emissione per cui si rimanda al relativo paragrafo. In particolare, se i dati utilizzati per l'emissione del certificato e per le comunicazioni con il titolare non sono variati, è necessario solo compilare il modulo di rinnovo certificato.

L'emissione del nuovo certificato è richiesto normalmente dal Titolare.

4.2.1 Tempi di rinnovo del certificato

Il **rinnovo del certificato**, e quindi la sostituzione delle chiavi scadute, deve essere **richiesto con un anticipo di almeno 90 giorni rispetto alla scadenza** del periodo di validità del certificato.

4.3 ... cessare il servizio

La **revoca del certificato** determina l'immediata e definitiva cessazione della sua validità, indipendentemente dalla data di scadenza del certificato stesso. La revoca non influisce sulla validità del certificato e delle firme apposte con esso nel periodo precedente la revoca.

Ai sensi della normativa in vigore, nel caso in cui il Certificatore non abbia la possibilità di accertare in tempo utile l'autenticità della richiesta di revoca, procede alla sospensione cautelativa del certificato.

Di seguito un elenco delle casistiche che, ai sensi della normativa vigente, richiedono la revoca del certificato:

- cessazione dell'attività del Certificatore;
- richiesta da parte del Titolare;
- richiesta da parte del "Terzo Interessato" dal quale derivano i poteri del titolare;
- perdita di possesso del dispositivo sicuro di firma delle informazioni necessarie al suo utilizzo;
- provvedimento dell'Autorità Giudiziaria;
- acquisizione della conoscenza di cause limitative della capacità del Titolare;
- sospetti di abusi e/o falsificazioni.

Il Certificatore può procedere alla revoca del certificato nei seguenti casi:

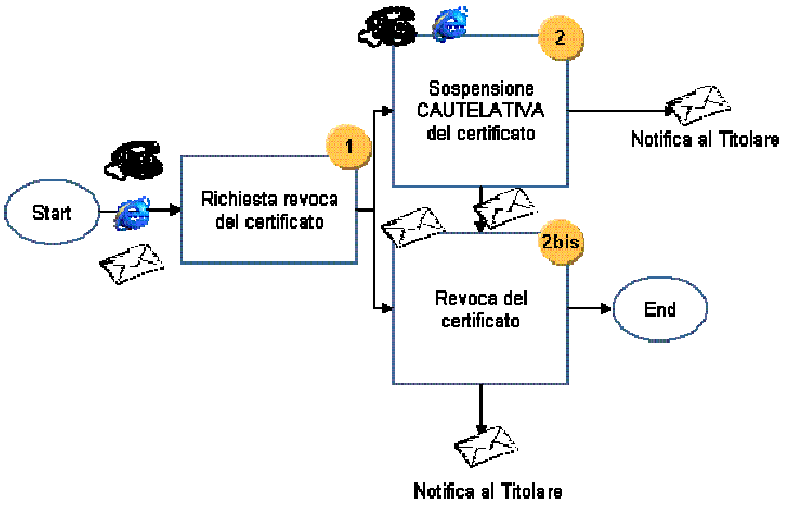
- possibile compromissione della chiave privata;

- richiesta di revoca da terzo interessato, secondo la normativa vigente;
- modifica o scadenza del rapporto che intercorre tra il Titolare e l'organizzazione per conto di cui il certificato viene utilizzato (il Cliente);
- decadere del titolo, della carica o del ruolo inerente i poteri di rappresentanza o la qualifica professionale in nome di cui il certificato viene utilizzato;
- ritiro della procura o della delega da parte del rappresentato;
- riscontro che il certificato non è stato rilasciato secondo le modalità previste dalla normativa vigente;
- riscontro che uno dei prerequisiti per l'accettazione della registrazione del titolare è venuto meno;
- sopravvenuta modifica di dati personali del titolare o di altri elementi riportati sul certificato;
- riscontro che il titolare del certificato ha infranto uno degli obblighi assunti al momento della richiesta di registrazione, previsti dalla normativa e riportati nel presente Manuale Operativo;
- compromissione della chiave di certificazione che ha firmato il certificato in questione;
- eventuale richiesta motivata e documentata dell'Autorità Giudiziaria.

4.3.1 Macro-processo di revoca del certificato

La revoca viene effettuata con la registrazione nel database del Certificatore e resa pubblica mediante l'inserimento del numero di serie univoco del certificato nella lista dei certificati revocati (CRL - Certificate Revocation List). La CRL è pubblicata con cadenza periodica ed è liberamente raggiungibile su internet. La pubblicazione della CRL determina il momento a partire dal quale il certificato si considera revocato.

La figura sottostante rappresenta, schematicamente, il macro processo di revoca dei certificati.



Di seguito sono descritte sinteticamente le singole fasi del processo.

Id	Macro Fase	Descrizione
1	Richiesta revoca	La richiesta di revoca da parte del Titolare o dell'Incaricato dell'Identificazione può pervenire mediante comunicazione telefonica, utilizzando il canale web sicuro messo a disposizione dell'ente certificatore, oppure per iscritto, tramite fax, con allegata fotocopia della denuncia di smarrimento/furto. La richiesta da parte del terzo interessato può pervenire solo per iscritto.

2	Sospensione cautelativa del certificato	Nel caso in cui la richiesta di revoca pervenga al Certificatore per via telefonica o tramite canale web, l'ente certificatore provvede dapprima a sospendere cautelativamente il certificato in attesa della ricezione della richiesta scritta. Anche i certificati sospesi sono segnalati nella CRL. La sospensione ha effetto dal momento della pubblicazione della stessa. Quando l'ente certificatore riceve la richiesta scritta di revoca il certificato viene revocato definitivamente. La CRL contiene anche l'informazione relativa allo stato di sospensione o revoca del certificato.
2 bis	Revoca del certificato	Nel caso in cui la richiesta di revoca pervenga all'ente certificatore per iscritto, il Certificatore provvede a revocare il certificato inserendolo nella CRL. La revoca ha effetto dal momento della pubblicazione della stessa. Nel caso in cui la richiesta sia pervenuta dal terzo interessato o sia iniziativa del Certificatore, l'intenzione di revocare il certificato viene notificata preventivamente al Titolare, salvo casi di motivata urgenza. L'avvenuta revoca di un certificato viene notificata al Titolare tramite un qualsiasi mezzo considerato idoneo dal certificatore.

4.3.2 Tempi di revoca del certificato

Il Certificatore si impegna a compiere le attività previste con la massima tempestività, al fine di rispettare i tempi di decorrenza della revoca riportati sulla relativa richiesta. Nei casi di compromissione della chiave privata, furto o smarrimento del dispositivo, il Certificatore si impegna ad eseguire la **revoca tempestivamente** all'atto della ricezione della richiesta.

4.4 ... chiedere supporto a

TI Trust Technologies mette a disposizione dei Titolari del servizio di FirmaSicura un help-desk in grado di risolvere problematiche di tipo tecnico.

Il Titolare è supportato da un team specialistico durante tutto il ciclo di vita del servizio.

L'help-desk è raggiungibile tramite il numero verde nazionale **800.28.75.24** ed è erogato alle seguenti condizioni:

1. servizi di assistenza ai titolari: dal lunedì al sabato, dalle 8 alle 16.30, festivi esclusi;
2. servizi di segnalazione inconvenienti: 24 ore su 24, 7 giorni su 7;
3. servizi di sospensione cautelativa dei certificati: 24 ore su 24, 7 giorni su 7.

4.5 FAQ

4.5.1 FAQ Tecniche

Che cosa è la crittografia?

La crittografia è una tecnica che, utilizzando speciali funzioni matematiche, consente la trasformazione (cifratura) di informazioni leggibili in informazioni non decifrabili da parte di terzi. Cifratura e decifratura richiedono in genere una formula matematica o algoritmo ed una chiave, per convertire i dati da una forma leggibile ad un formato in codice e viceversa. La chiave è un valore numerico o una sequenza arbitraria di lettere e cifre che, combinata con il messaggio originale, produce il messaggio cifrato.

Che cosa è una chiave?

La chiave è un valore numerico o una sequenza arbitraria di lettere e cifre che, combinata con il messaggio originale, produce il messaggio cifrato. In un algoritmo a chiave simmetrica, la medesima

chiave è utilizzata sia per la cifratura che per la decifratura. In un algoritmo a chiave asimmetrica, vengono utilizzate due diverse chiavi: se si utilizza la prima chiave per cifrare un messaggio è necessario avvalersi della seconda chiave per decifrarlo e viceversa. In tutti i casi è indispensabile far pervenire al destinatario la chiave da utilizzare per la decifratura con notevoli problemi di sicurezza. Nel caso dell'utilizzo di chiavi asimmetriche una delle due chiavi viene resa *disponibile pubblicamente* (chiave pubblica) e l'altra tenuta segreta (chiave privata). Non c'è necessità di proteggere la chiave pubblica. Per questo motivo il termine "crittografia asimmetrica" è spesso sostituito dalla più nota dizione **crittografia a chiave pubblica** o PKI (*Public Key Infrastructure*).

Che cosa è la marcatura temporale?

La marcatura temporale consiste nella generazione, da parte di una terza parte fidata, di un documento informatico firmato che contiene l'impronta relativa alla firma apposta a un documento e l'informazione relativa ad una data e ad un'ora certa. La marcatura temporale consente quindi di stabilire l'esistenza di un documento informatico a partire da un certo istante temporale e di opporlo a terzi.

Chi è il Certificatore?

E' la terza parte di fiducia che garantisce l'identità dei soggetti che utilizzano la Firma Elettronica Qualificata.

Qual è il ruolo del certificatore?

Il Certificatore svolge, tra gli altri, i seguenti compiti fondamentali:

- verifica dell'identità del Titolare ed eventualmente la veridicità di una serie di altre informazioni da esso fornite;
- fornisce al Titolare il dispositivo sicuro di firma;
- stabilisce il termine di scadenza dei certificati;
- pubblica il certificato e la chiave pubblica;
- gestisce le liste dei certificati revocati o sospesi.

Che cos'è un certificato digitale?

Un certificato digitale è un file che contiene la chiave pubblica del sottoscrittore (sia esso una persona fisica o un dispositivo hardware) firmata digitalmente dalla chiave privata di un Certificatore. Un certificato digitale può essere paragonato ad un passaporto, o ad una carta di identità, cioè ad un documento di riconoscimento rilasciato da un'Autorità universalmente nota, accettata e riconosciuta come affidabile, e utilizzata per autenticare l'identità di una persona.

Oltre alla chiave pubblica di crittografia del soggetto certificato, all'interno del certificato digitale sono contenute altre informazioni: i dati identificativi del soggetto che viene certificato, la validità temporale del certificato stesso, l'identità e la Firma Elettronica Qualificata del Certificatore.

Che differenza c'è tra Firma Elettronica Qualificata e firma elettronica?

La Firma Elettronica Qualificata deve essere emessa da una Certification Authority ed è la sola che conferisce al documento informatico il pieno valore legale. La firma elettronica può essere utilizzata nell'ambito di gruppi di soggetti che siano d'accordo sull'attribuire ad essa un qualche valore convenzionale, ma non conferisce valore legale al documento firmato.

In quali circostanze si può utilizzare una Firma Elettronica Qualificata?

La Firma Elettronica Qualificata può essere apposta su qualunque documento informatico. Alcuni esempi di casi d'uso:

- bilanci e atti societari;
- fatture elettroniche;
- notificazioni al Garante della Privacy;

- iscrizione al registro dei revisori contabili;
- comunicazioni degli operatori finanziari con l'Agenzia delle Entrate;
- contratti e scritture private

Chi può usare il certificato di firma per firmare documenti?

Esclusivamente il Titolare per firmare documenti sui cui contenuti, apponendo la firma, intenda esprimere il consenso e la paternità.

E' possibile affidare la smart card al proprio commercialista?

La normativa sulla Firma Elettronica Qualificata non prevede sanzioni per l'affidamento del dispositivo a un terzo, ma il combinato disposto di una serie di norme indica chiaramente l'impossibilità di uso del dispositivo da parte di chi non ne sia il legittimo titolare. Di fatto affidare a terzi il proprio dispositivo di firma ed il relativo PIN è una gravissima imprudenza. Infatti la falsificazione di una firma autografa è quasi sempre verificabile con una perizia calligrafica, mentre una Firma Elettronica Qualificata è sempre "vera". La responsabilità della Firma Elettronica Qualificata è del suo Titolare e un tale comportamento contravviene all'obbligo che egli sottoscrive al momento del rilascio di conservarne il controllo esclusivo.

L'Incaricato delegato può delegare a sua volta la propria attività?

L'Incaricato non può delegare nessuna delle attività che gli sono già state personalmente delegate dal Certificatore.

Il documento firmato è anche cifrato?

No. Per effettuare l'operazione di cifratura, l'autore deve possedere apposite chiavi e un certificato di cifratura, diverso da quello di firma. Se si vuole cifrare il documento in modo che solo un'altra determinata persona lo possa decifrare, egli deve conoscere e utilizzare a tale scopo la chiave pubblica di cifratura del destinatario.

Che cosa serve per firmare un documento elettronico?

Nel caso si opti per il servizio **FirmaSicura** è previsto l'utilizzo di un kit composto da:

- un dispositivo di generazione della firma (smart card);
- un lettore di smart card;
- un software di firma e verifica.

Quali sono i requisiti minimi di sistema per l'installazione del software di Firma?

Il software client di firma utilizzabile con Smart Card è in grado di funzionare sui più diffusi ambienti operativi in commercio:

- Microsoft Windows
- Linux*
- Apple Mac OSX*

Il software client di firma utilizzabile con il prodotto Firma Sicura Key ha i seguenti requisiti di sistema:

- Microsoft Windows 2000, XP, Vista o superiore
- Linux
- MAC OSX 10.5.x o superiore
- USB 2.0 full speed

* la compatibilità della funzionalità di firma è legata al tipo di smart card acquistata.

Entrambi i software sono forniti da TI Trust Technologies.

Quali tipi di lettori di smart card sono supportati dal servizio FirmaSicura?

Il servizio supporta almeno i lettori distribuiti da TI Trust Technologies, ovvero:

- Gemplus Twin (dotato di interfaccia USB).

E' possibile scaricare, dal sito internet di TI Trust Technologies, il software per la Firma Elettronica Qualificata?

Si.

Dal sito è possibile scaricare anche i driver dei lettori smart card?

Si.

Quali applicativi sono necessari per leggere i documenti firmati?

Per quanto riguarda la visualizzazione dei documenti sottoscritti con Firma Elettronica Qualificata, sono utilizzabili i differenti software di firma e verifica resi disponibili dai certificatori. Tali prodotti, oltre a consentire la visualizzazione del documento, permettono anche di effettuare la verifica della validità delle firme con le quali il documento è sottoscritto.

TI Trust Technologies distribuisce ai Titolari del proprio servizio un software che consente l'apposizione della firma con marca temporale e la verifica dei documenti nei formati previsti dalla normativa.

La Smart Card può smagnetizzarsi accidentalmente?

No, perché non viene utilizzata una tecnologia basata su banda magnetica, ma su un chip con microprocessore resistente ai campi elettromagnetici ai quali può in genere essere sottoposta la smart card (es. nelle vicinanze di un telefono cellulare, *gate* di un aeroporto, ecc.)

E' possibile lanciare un'unica sessione di firma per firmare più documenti?

Il software client di firma e verifica consente di firmare anche più di un documento alla volta.

Per i Clienti che necessitano di sottoscrivere contemporaneamente un gran numero di documenti (per es. fatturazione elettronica), TI Trust Technologies mette a disposizione il servizio di **Firma Massiva** che permette all'utente di apporre le firme elettroniche tramite un applicativo server.

La firma può essere verificata anche quando non è presente la connessione ad internet?

La connessione ad internet permette di verificare la firma a fronte della versione più recente della Certificate Revocation List (CRL), che contiene tutti i certificati revocati.

Di conseguenza, se si effettua la verifica della firma quando non è presente il collegamento, la verifica è solo parziale, e può dirsi valida "salvo buon fine", in quanto può fare riferimento a una versione della CRL presente in locale sul computer, verosimilmente non è la versione più recente e non offre lo stesso livello di garanzia.

Che documentazione deve produrre il titolare di un certificato per richiederne la revoca?

Se il titolare richiede la revoca per telefono, l'help-desk provvede immediatamente alla sospensione cautelativa. Per la revoca definitiva, il titolare deve inviare richiesta scritta di revoca con le seguenti informazioni:

- esplicita dichiarazione della volontà di revocare il certificato;
- motivazione della richiesta di revoca e la decorrenza richiesta per tale revoca;
- codice di registrazione fornito al titolare al momento della richiesta di registrazione relativa al certificato da revocare;
- codice segreto di revoca fornito per ogni certificato insieme al codice di attivazione del dispositivo di firma;
- i seguenti dati anagrafici del richiedente:

- nome e cognome;
- data e luogo di nascita;
- indirizzo di residenza (costituito da via, numero civico, CAP, comune di residenza);
- codice fiscale.

Il fax dovrà inoltre contenere:

- fotocopia del medesimo documento di riconoscimento fornito al momento della richiesta di registrazione, ovvero del nuovo documento in caso di rinnovo;
- nel caso di richiesta di revoca motivata da smarrimento o furto del dispositivo di firma, la fotocopia della denuncia dell'avvenuto smarrimento o furto.

4.5.2 FAQ Normative

Dove è possibile trovare la normativa di riferimento della Firma Elettronica Qualificata?

La normativa è interamente presente e scaricabile dall'apposita sezione del sito internet dell'Agenzia per l'Italia Digitale (AgID): http://www.digitpa.gov.it.

Per la Firma Elettronica Qualificata è possibile utilizzare un qualsiasi certificato digitale scaricabile da internet?

Per la Firma Elettronica Qualificata occorre utilizzare un certificato ottenibile solo dai certificatori accreditati presenti nell'elenco pubblico tenuto dall'AgID e fornito assieme a un dispositivo sicuro di firma (smart card).

E' possibile firmare tutti i formati (esempio .doc, .xls, …) di documenti elettronici?

In linea di principio qualunque documento elettronico può essere firmato digitalmente, diventando un vero e proprio documento informatico provvisto di un valore probatorio. Tuttavia, se si tiene conto che un documento informatico deve equivalere ad un documento cartaceo sottoscritto, occorre organizzare la propria applicazione in modo tale che il documento soddisfi alcuni requisiti:

- Il documento deve essere autoconsistente, ossia deve essere leggibile ed utilizzabile senza dipendenze da altri oggetti esterni al documento. Quindi vanno evitati documenti come le pagine HTML arricchite da link o da immagini; vanno assolutamente evitati documenti costituiti da sequenze di campi ottenuti dalla compilazione di form, privi di significato fuori dal form.
- Il documento deve essere riproducibile senza ambiguità: anche se trasferito da un sistema ad un altro non deve essere possibile rappresentare lo stesso documento in modi diversi. Quindi è molto opportuno ricorrere a formati basati su standard internazionali consolidati, possibilmente per i quali esistano diverse applicazioni di gestione da diversi produttori su diverse piattaforme (per esempio il PDF/A), tanto più se si prevede una lunga durata di validità del documento stesso.
- Il documento non deve contenere macro o elementi variabili che possano modificarne la rappresentazione in tempi successivi. Questo è un punto molto importante, perché la presenza di elementi di questo tipo potrebbe annullare il valore probatorio del documento stesso.

Qual è l'ente preposto al controllo delle attività esercitate dagli iscritti nell'elenco dei Certificatori?

L'Agenzia per l'Italia Digitale – AgID (ex DigitPA, ex CNIPA).

Quali sono i riferimenti normativi che disciplinano l'attività di vigilanza e di controllo svolta nei confronti dei Certificatori qualificati e accreditati?

L'attività di vigilanza e di controllo nei confronti certificatori qualificati e accreditati viene svolta dall'AgID con le modalità indicate nella Circolare CNIPA 15 febbraio 2007, n.52, G.U. 23 febbraio 2007, n. 45).

5 SLA, indicatori e misure di qualità

In questo paragrafo sono definiti gli indicatori atti a descrivere i livelli di qualità relativi al servizio Firma Sicura.

Gli SLA (*Service Level Agreement*) riportati nel seguito sono validi per il servizio erogato da TI Trust Technologies tramite la piattaforma situata presso il Centro Servizi di Pomezia (RM).

Gli SLA vengono calcolati sulla base delle segnalazioni degli utenti tracciate su trouble ticket aperti dai tecnici dell'Help Desk. In particolare, ogni segnalazione di guasto che perviene al numero verde gestito dall'Help Desk dà luogo all'apertura di un ticket la cui registrazione consente di effettuare un monitoraggio periodico per la verifica del rispetto degli SLA.

Servizio	SLA
Disponibilità del Servizio Firma Sicura	99,5% su base 4 mesi
Disponibilità Certificate Revocation List (CRL)	99,8% su base 4 mesi
Supporto di Help Desk telefonico	H24 7x7

6 Definizioni e acronimi

6.1 Definizioni

Secondo la normativa vigente e ai fini dell'interpretazione del presente documento, i termini e le espressioni sotto elencate avranno il significato descritto nella definizione riportata.

Le definizioni adottate dalla normativa di riferimento non sono riportate e si rimanda ai testi in vigore per la loro consultazione.

I termini e le espressioni non definiti avranno il significato loro attribuito all'interno del paragrafo o sezione che li contiene.

Si definisce:

Certificatore (Certification Authority, CA, Autorità di Certificazione): prestatore di servizi di certificazione, la società TI Trust Technologies. Per Certificatore, si intende il soggetto che presta servizi di certificazione delle firme elettroniche o che fornisce altri servizi connessi con queste ultime.

Certificazione: Il risultato della procedura informatica applicata alla chiave pubblica e rilevabile dai sistemi di validazione, mediante la quale si garantisce la corrispondenza biunivoca tra chiave pubblica e soggetto titolare cui essa appartiene, si attesta il periodo di validità della predetta chiave e il termine di scadenza del relativo certificato.

Chiavi asimmetriche: La coppia di chiavi crittografiche una privata e una pubblica, correlate tra loro, e utilizzate nell'ambito dei sistemi di validazione di documenti informatici.

Chiavi di certificazione: Chiavi asimmetriche utilizzate esclusivamente per apporre la firma su certificati relativi a chiavi di sottoscrizione, di marcatura temporale e di autenticazione per Carta Nazionale dei Servizi (CNS) emessi dal Certificatore, sulle liste dei certificati sospesi e revocati (CRL) e su nuovi certificati relativi a chiavi di certificazione generate in sostituzione di chiavi scadute.

Chiavi di marcatura temporale: Chiavi asimmetriche utilizzate dal Certificatore per apporre la firma alle marche temporali.

Chiavi di sottoscrizione: Chiavi asimmetriche associate a persone fisiche, da utilizzare per l'apposizione di firme digitali a documenti e ad evidenze informatiche.

Cifratura: La trascrizione di un'evidenza informatica secondo un codice riservato che la renda inintelligibile ai terzi. Le operazioni di cifratura e decifrazione si effettuano applicando algoritmi standard che prevedono l'utilizzo di chiavi segrete.

CWA: European Commitee for Standardization Workshop Agreement; il comitato che, in sede di comunità europea, si occupa di standardizzazione.

Dati identificativi del Titolare: il nome, il cognome, il sesso, la data ed il luogo di nascita, il luogo di residenza, il codice fiscale (per quanto riguarda la Carta Nazionale dei Servizi, il luogo di residenza è quello al momento del rilascio della carta stessa).

Dispositivo sicuro di Firma: Apparato strumentale usato per la creazione della firma elettronica, rispondente ai requisiti fissati dalla normativa vigente in materia.

Elenco pubblico dei Certificatori Accreditati: L'elenco pubblico tenuto dall'Agenzia per l'Italia Digitale (AgID, ex DigitPA).

Estensione del Certificato: Lo standard X.509 versione v3, che definisce i criteri di compilazione dei certificati digitali, include la possibilità di inserire nel certificato dati aggiuntivi definiti dal Certificatore (le estensioni del certificato) in aggiunta alle informazioni standard (numero di serie, valore della chiave pubblica, periodo di validità, ecc.). Sono campi utilizzati secondo quanto prescritto dalla normativa.

Evidenza informatica: Una sequenza di simboli binari che può essere elaborata da una procedura informatica.

Firma Elettronica: l'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di identificazione informatica.

Firma Elettronica Qualificata: La firma elettronica ottenuta attraverso una procedura informatica che garantisce la connessione univoca al firmatario, creata con mezzi sui quali il firmatario può conservare un controllo esclusivo e collegata ai dati ai quali si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati, che sia basata su un certificato qualificato e realizzata mediante un dispositivo sicuro per la creazione della firma.

Firma Digitale: Un particolare tipo di Firma Elettronica Qualificata basata su un sistema di chiavi crittografiche, una pubblica e una privata, correlate fra loro, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici.

Firma di un documento o di un'evidenza informatica: Il processo informatico attraverso cui l'impronta di un documento o di un'evidenza informatica è cifrata con la chiave privata del firmatario, secondo modalità che consentano al destinatario di verificare la provenienza e l'integrità del documento tramite la corrispondente chiave pubblica ed il relativo certificato.

Firma Sicura Key: Dispositivo che integra una Smart Card in formato SIM, un lettore di Smart Card e una memoria flash che contiene al suo interno tutte le applicazioni per la gestione di documenti firmati digitalmente.

Funzione di hash: Una funzione matematica che, da una generica sequenza di simboli binari di partenza, genera una sequenza di simboli binari derivata (detta impronta o hash) di lunghezza fissa. La sequenza derivata è generata in modo tale che non sia possibile risalire alla sequenza di partenza e che, a fronte di sequenze di partenza diverse, non possano essere generate sequenze derivate identiche.

Impronta di un documento o di un'evidenza informatica: Sequenza di simboli binari, di lunghezza predefinita, generata mediante l'applicazione di un'opportuna funzione di hash al documento.

Lista dei Certificati Revocati o Lista di Revoca - (Certificate Revocation o CRL): La lista firmata digitalmente, tenuta e aggiornata dal Certificatore, dei certificati che hanno perduto temporaneamente (sospesi) o definitivamente (revocati) la propria validità, in anticipo rispetto alla scadenza prevista. La revoca e la sospensione, che possono essere richieste dai Titolari dei certificati, dal Certificatore o da un terzo interessato, determinano l'inserimento del certificato nella lista dei certificati revocati. Al termine della sospensione i certificati vengono rimossi dalla CRL/CSL. La lista è resa pubblica dal Certificatore.

Marca temporale: Un'evidenza informatica che consente la validazione temporale di un documento.

Manuale Operativo: Il documento pubblico che definisce le modalità operative del servizio di certificazione.

Registrazione di un utente, un sottoscrittore, un titolare: La procedura che precede il rilascio di un certificato da parte del Certificatore e che prevede l'acquisizione dei dati identificativi del Titolare.

Revoca di un Certificato: L'operazione mediante la quale il Certificatore annulla in maniera irreversibile, su iniziativa propria o del titolare o di terze parti interessate, la validità del certificato da un dato momento in poi. I certificati revocati sono inseriti definitivamente nella CRL.

Smart Card: Dispositivo elettronico costituito da un microchip inserito in una tessera di plastica delle dimensioni di una carta di credito. Il microchip è programmabile, può contenere dati e applicativi e interagire con altre apparecchiature elettroniche e computer tramite un apposito lettore.

Sospensione di un Certificato: L'operazione con cui l'Ente Certificatore sospende la validità del certificato per un determinato periodo di tempo. I certificati sospesi sono inseriti temporaneamente nella CRL.

Terzo interessato: Persona fisica o giuridica che (ove previsto) acconsente alla emissione di uno o più certificati digitali intestati a soggetto che derivi i propri poteri dalla suddetta persona fisica o giuridica.

Titolare: è la persona fisica cui é attribuita la Firma Elettronica Qualificata e che ha accesso al dispositivo di firma. Detiene una chiave privata per sottoscrizione ed è intestataria del certificato che attesta il valore della chiave pubblica ad essa relativa. Il titolare può utilizzare la chiave privata e il certificato per apporre firme digitali come privato, o in base al proprio ruolo all'interno di un'organizzazione pubblica o privata, ovvero in base a poteri di rappresentanza o titoli e abilitazioni professionali.

6.2 Acronimi e termini tecnici

AgID – Agenzia per l'Italia Digitale: L'Agenzia per l'Italia Digitale è l'ente che ha sostituito il DigitPA (già CNIPA, Centro Nazionale per l'Informatica nella Pubblica Amministrazione) nell'ambito dell'attuazione delle politiche governative in tema di Innovazione e Tecnologie.

AIPA - *Autorità per l'Informatica nella Pubblica Amministrazione*: Autorità pubblica indipendente, istituita dal decreto legislativo n. 39 del 12 febbraio 1993 "Norme in materia di sistemi informativi automatizzati delle amministrazioni pubbliche" (come modificato dall'art. 42 della legge 31 dicembre 1996, n.675). L'AIPA ha cambiato denominazione in CNIPA con l'articolo 176 del DL 196/003.

CNIPA – *Centro Nazionale per l'Informatica nella Pubblica Amministrazione*: Creato con l'articolo 176 del DL 196/03, il CNIPA ha incorporato le strutture e le funzioni dell'AIPA e del Centro Tecnico della RUPA.

DigitPA (ora 'AgID') – *Ente nazionale per la digitalizzazione della Pubblica Amministrazione*: ex-CNIPA, Ente pubblico non economico che svolge funzioni di natura progettuale, tecnica e operativa, con la missione di contribuire alla creazione di valore per cittadini e imprese da parte della pubblica amministrazione, attraverso la realizzazione dell'amministrazione digitale. Opera secondo le direttive, per l'attuazione delle politiche e sotto la vigilanza del Presidente del Consiglio dei Ministri o del Ministro delegato, con autonomia tecnica e funzionale, amministrativa, contabile, finanziaria e patrimoniale.

HTTP *(Hypertext Transfer Protocol):* Protocollo di trasmissione, che permette lo scambio di file (testi, immagini grafiche, suoni, video e altri documenti multimediali) su World Wide Web.

HTTPS *(Secure Hypertext Transfer Protocol):* Protocollo di trasmissione, sviluppato originalmente da Netscape Communications Corporation, per la cifratura e decifratura dei dati trasmessi durante la consultazione di siti e pagine web su internet. Corrisponde ad un'estensione del protocollo Internet standard HTTP (Hypertext Transfer Protocol), attraverso il protocollo SSL.

INTERNET*:* Un sistema globale di reti informatiche nel quale gli utenti di singoli computer possono ottenere informazioni da luoghi diversi. La sua grande diffusione è stata determinata principalmente dall'introduzione dei protocolli di trasmissione di documenti con riferimenti ipertestuali (HTTP) e dallo sviluppo del World Wide Web (WWW).

ISO - *International Standards Organization:* Organizzazione internazionale per la standardizzazione, costituita da organismi nazionali provenienti da più di 75 paesi. Ha stabilito numerosi standard nell'area dei sistemi informativi.

LDAP – *Lightweight Directory Access Protocol:* Protocollo utilizzato per la gestione degli accessi al registro dei certificati e l'effettuazione di operazioni di prelievo di certificati e liste di revoca e sospensione.

PIN - *Personal Identification Number:* Codice di sicurezza riservato che permette l'attivazione delle funzioni del dispositivo di firma.

POP – *Point of Presence:* Punto di accesso alla rete internet.

PKCS - *Public Key Cryptography Standard:* Standard tecnici per applicazioni crittografiche, realizzati dalla RSA Data Security Inc.

URL - *Uniform Resource Locator:* Sistema standard di nomenclatura specificante un sito, dominio o altro oggetto (file, gruppo di discussione, ecc.) su Internet. La prima parte dell'URL (http:, ftp:, file:, telnet:, news:) specifica le modalità di accesso all'oggetto.

WWW – *World Wide Web:* L'insieme delle risorse e degli utenti su Internet che utilizzano il protocollo HTTP.

X509*:* Specifica ITU-T che definisce la struttura e la terminologia da utilizzare per la compilazione dei certificati e delle liste di revoca/sospensione ad essi associate.