Firma Elettronica Qualificata

Descrizione del servizio

DOCUMENTO DESCRITTIVO

VERSIONI DEL DOCUMENTO		
Revisione	Descrizione delle modifiche	Emissione
00	Prima emissione (ricodifica del doc. CERTQUAL.IT.SODS092596.03 - Firma Digitale Qualificata Descrizione del servizio - USO INTERNO)	06/10/2023
01	.	

Indice degli argomenti

Scopo del documento

Questo documento descrive le soluzioni di **Firma Elettronica Qualificata** erogate da Telecom Italia Trust Technologies S.r.l. (in breve TI Trust Technologies o QTSP - *Qualified Trust Service Provider*) e le procedure per la sua gestione. È liberamente disponibile per la consultazione ed il download sul sito internet: https://www.trusttechnologies.it.

1 La Firma Elettronica Qualificata

La Firma Elettronica Qualificata (FEQ) - o digitale - è il risultato di una procedura informatica, detta validazione, che garantisce:

- 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**.

La **Firma Elettronica Qualificata** è un particolare tipo di Firma Elettronica Avanzata[1] basata su un certificato qualificato emesso da un Prestatore di servizi fiduciari (QSTP – *Qualified Trust Service Provider*)[2] e basata sull'utilizzo di un dispositivo sicuro per la creazione della firma.
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 essere identificate, al fine di completare la richiesta di Firma Elettronica Qualificata:

- le Persone Fisiche;
- le Persone Giuridiche (prevede l'identificazione della persona fisica che ne abbia la legale rappresentanza o procura)
- le Persone Giuridiche per il rilascio del Sigillo Elettronico[3].

[1] La Firma Elettronica Avanzata 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] I prestatori di servizi fiduciari qualificati (QSTP) sono soggetti che rilasciano certificati qualificati a norma del regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio, del 23 luglio 2014 (eIDAS). Tali soggetti, in Italia, sono i certificatori qualificati per la fornitura di servizi fiduciari qualificati ai sensi dell'articolo 29 del CAD. L'iter previsto dal citato articolo 29 del CAD prevede che il prestatore del servizio presenti all'Agenzia apposita richiesta per ottenere il riconoscimento di prestatore del servizio fiduciario qualificato di interesse, allegando un report della valutazione di conformità con il Regolamento rilasciato da un organismo di valutazione autorizzato dal preposto organismo nazionale, in Italia ACCREDIA. Dal 28 giugno 2016, data in cui ACCREDIA ha autorizzato i primi due organismi di valutazione, i prestatori di servizi hanno potuto presentare apposita istanza, ottenendo il riconoscimento di prestatori di servizi fiduciari qualificati. AgID pubblica l'elenco dei prestatori di servizi fiduciari stabiliti in Italia, unitamente alle informazioni sui servizi da loro prestati.

[3] Il sigillo elettronico qualificato è stato introdotto nel nostro ordinamento con l'emanazione del già citato Regolamento eIDAS. Sostanzialmente è equivalente a una firma elettronica qualificata, con la differenza che non afferisce a una persona fisica, bensì a una persona giuridica. In altri termini, mentre da una firma siamo in grado di individuare con certezza un soggetto attraverso il suo nome, cognome, codice fiscale ecc., da un sigillo possiamo risalire con certezza ad una persona giuridica attraverso la sua denominazione, partita IVA o codice fiscale, ma non abbiamo alcun riferimento alla persona fisica che ha materialmente utilizzato le credenziali per generare tale sigillo.

che abbiano seguito una delle modalità di identificazione ammesse e previste dal CPS (*certification practice statement*) rilasciato da Trust Technologies e pubblicato sul sito internet: https://www.trusttechnologies.it a cui si rimanda per approfondimenti.

1.1 Effetti giuridici della Firma Elettronica Qualificata

Gli effetti giuridici di una firma elettronica sono riconducibili alla loro capacità di soddisfare il requisito della forma scritta alla loro efficacia giuridica, all'onere della prova. Quest'ultimo, si riferisce all'individuazione del soggetto che, in caso di contestazione, deve fornire prove atte a dimostrare la validità o invalidità della firma oggetto di contestazione.

I documenti sottoscritti con firma elettronica qualificata (cd. firma digitale**), soddisfano il requisito della forma scritta e hanno l'efficacia prevista dall'articolo 2702 del Codice Civile**; inoltre, l'utilizzo del dispositivo di firma elettronica qualificata o digitale si presume riconducibile al titolare della firma elettronica, salvo che questi dia prova contraria.

Pertanto, al fine del disconoscimento, è l'apparente sottoscrittore (il soggetto cui la firma afferisce) che ha l'onere di dimostrare che tale firma digitale non sia stata generata da lui. Visto che il titolare della firma elettronica qualificata deve assicurare la custodia del dispositivo di firma ed utilizzare personalmente il dispositivo di firma, considerato che:

- i dispositivi utilizzati (chiamati dispositivi sicuri per la generazione della firma, ovvero QSCD) sono utilizzabili esclusivamente se si conoscono i codici segreti necessari;
- i codici segreti sono consegnati al titolare della firma dal certificatore in modalità sicura.

Il titolare della firma che intende disconoscerla ha solo due alternative: dichiarare di non aver mai richiesto la firma digitale al certificatore accreditato (che conserva elementi utili a provare di aver rilasciato la firma al soggetto) o dimostrare che è stato vittima di furto o sottrazione temporanea del dispositivo e dei relativi codici per il suo utilizzo.

1.2 Quadro Normativo di riferimento

La storia italiana del documento informatico e della firma digitale 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 digitale.

Il processo legislativo ha anche fornito delle indicazioni sulle tecnologie da impiegare per ottenere delle firme digitali che possono ritenersi equivalenti a quelle autografe.

La firma digitale diventa lo strumento abilitante per l'intero sistema della "de-materializzazione" della documentazione. Può essere pienamente utilizzata come strumento che garantisce autenticità, paternità e integrità, non solo per la sottoscrizione del documento informatico, ma anche nella conservazione a norma, nella fatturazione elettronica, nello scambio di documenti informatici in procedimenti amministrativi digitalizzati.

1.2.1 Normative

Le norme ad oggi in vigore, su cui si fonda la regolamentazione normativa della Firma Elettronica Qualificata - o Digitale, sono elencate nella tabella sottostante che riporta i link ai contenuti rilasciati dall'Agenzia per l'Italia Digitale.

Tipologia	URL
Leggi, Decreti e Direttive	• DPCM 5 febbraio 2015 - dispositivi certificati per apposizione di firme elettroniche • DPCM 22 febbraio 2013 - Nuove regole tecniche • DPCM 19 luglio 2012 - Decreto sui dispositivi automatici di firma - HSM • DPCM 10 febbraio 2010 (Autocertificazione dispositivi automatici di firma) • DPCM 10 febbraio 2010 - Modulo di autocertificazione • DPCM 30 marzo 2009 (Regole tecniche firma digitale) • Direttiva 1999/93/CE (Quadro comunitario per le firme elettroniche) • Regolamento n. 910/2014 (eIDAS).
Circolari e deliberazioni	• Linee guida CAD art. 35, comma 5 • Determinazione AgID n. 63/2014 - Firma digitale verificata • Deliberazione CNIPA n. 45/2009 modificata dalla Determ. DigitPA n. 69/2010 • Determinazione DigitPA n. 69/2010 - Modifiche alla Deliberazione CNIPA n. 45/2009 • Deliberazione CNIPA n. 45/2009 - Regole riconoscimento e verifica doc. informatico • Limiti d'uso garantiti agli utenti • Estensione IssuingDistributionPoint nelle Liste di Revoca • Modifica alla Deliberazione 45/2009 • Determinazione n. 185/2017 - Modalità per la domanda di qualificazione per i servizi eIDAS - sostituisce la Circolare n. 48/2005 • Determinazione n. 185/2017 - Modalità per la domanda di qualificazione - Allegato contenuto nella Determinazione • Determinazione n. 189/2017 - Modifiche alla Deliberazione n. 45/2009 • Avviso emanazione Determina 185/2017 • modello richiesta qualificazione v1.3 • Determinazione n. 121/2019 - Linee Guida "Regole Tecniche e Raccomandazioni afferenti la generazione di certificati elettronici qualificati, firme e sigilli elettronici qualificati e validazioni temporali elettroniche qualificate" • Determinazione n. 147/2019: Rettifica per errore materiale della determinazione n.121/2019 • Determinazione n. 147/2019 - Allegato contenuto nella Determinazione

Al link https://www.agid.gov.it/it/piattaforme/firma-elettronica-qualificata è possibile prendere visione degli ultimi novità e della documentazione sempre aggiornata.

2 Il servizio *Firma Sicura*™

Firma Sicura è il servizio di Firma Elettronica Qualificata che TI Trust Technologies offre in qualità di Prestatore di Servizi Fiduciari (QSTP) attivo in Italia, 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 (CPS o Manuale operativo) pubblicate sul sito https://www.agid.gov.it/piattaforme/firma-elettronica-qualificata/prestatori-di-servizi-fiduciari-attivi-in-italia.

Gli utenti vengono dotati di Firma Elettronica Qualificata mediante un processo di 'registrazione' a cura di TI

Trust Technologies, che ha la responsabilità di identificare il titolare di un certificato digitale e di procedere alla corretta registrazione dei suoi dati.

2.1 La suite *Firma Sicura*™

Firma Sicura è la suite di soluzioni che consente di conferire al documento informativo piena **validità legale.**

Le soluzioni proposte da Trust Technologies prevedono l'utilizzo dei tradizionali strumenti hardware e software, affiancati da tool applicativi e App mobile che consentono un utilizzo più agevole del servizio:

- Kit Firma Sicura (Token USB e Smart-card);
- Firma Sicura Remota:
  - SecureCall
  - OTP via SMS
  - via App mobile
  - Biometrica
  - Massiva.

2.1.1 Kit Firma Sicura (Token USB e Smart-card)

Il kit Firmasicura è lo strumento per l'apposizione della Firma Elettronica Qualificata con Token usb o Smart-card.

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 da inserire in card-reader USB (entrambe compresi nel kit fornito da TI Trust Technologies).

La soluzione comprende:

- Card reader per Smart-card
- Smart-card con a bordo il certificato di firma qualificata;
- Software di firma e verifica gratuito scaricabile dal sito di Trust Technologies (https://www.trusttechnologies.it/download/software);
- Busta virtuale o fisica (antieffrazione) con i codici PIN e PUK riservati al titolare del certificato di firma.

2) **Firma Sicura Key (Token USB)**, ovvero dispositivi, dotati anche mi memoria storage, che contengono il certificato di firma attraverso una mini-SIM alloggiata all'interno. Firma Sicura Key è facile da usare, portabile ed autoconsistente, ovvero è in grado di funzionare senza l'installazione di alcun driver e/o applicazione su PC ospite.

La soluzione comprende:

- SIM con a bordo il certificato di firma qualificata;
- Token USB con 2 Gb di storage
- Software di firma installato all'interno del Token;
- Busta virtuale o fisica (antieffrazione) con i codici PIN e PUK riservati al titolare del certificato di firma.

2.1.2 Firma Sicura Remota

La **Firma Remota** è una particolare procedura di Firma Elettronica Qualificata, o di Firma Digitale[4], generata su

[4] un particolare tipo di Firma Elettronica Avanzata basata su un certificato qualificato e su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente,

HSM, che consente di garantire il controllo esclusivo delle chiavi private da parte dei titolari delle stesse.

Il sistema remoto garantisce al titolare della firma che l'operazione sia effettuata in modalità sicura e con un'autenticazione forte. Il dispositivo (prevalentemente mobile) dell'utilizzatore occorre per effettuare le operazioni seguenti:

- **autenticazione** forte dell'utente (strong authentication);
- **autorizzazione diretta della firma** da parte dell'utente.

Un apposito **HSM** (hardware security module) custodisce in maniera sicura i certificati digitali e le chiavi private dei clienti.

Agli utenti viene fornito un certificato di firma digitale mediante un preventivo processo di registrazione.

Tra le informazioni acquisite in fase di attivazione del servizio, è compresa **l'associazione tra utente e numero di telefono cellulare.**

Durante la registrazione viene comunicato al cliente il suo PIN personale ed un codice segreto per la sospensione cautelativa del proprio certificato in caso di emergenza.

Il servizio di Firma Sicura Remota consente di soddisfare i seguenti requisiti:

- **Identificazione certa ed autenticazione sicura del titolare remoto**: l'autenticazione avviene tramite telefonata ad un sistema che riconosce il CLI (caller ID) da cui proviene la chiamata.
- **Associazione univoca dell'operazione di firma con uno specifico documento:** la chiamata allo specifico numero di Rete Intelligente e la digitazione del codice OTP fornito dal sistema di autenticazione consentono di associare univocamente e temporaneamente la chiamata all'operazione di firma di "quel" documento.
- **Controllo "esclusivo" dell'operazione di firma da parte del titolare:** l'associazione dei passi precedenti alla protezione mediante PIN personale permette di apporre la firma digitale allo specifico documento in totale sicurezza.

2.1.2.1 MOST/SecureCall

MOST/SecureCall è la modalità di Firma Remota che permette di determinare in maniera sicura, e quindi garantire, **il numero dal quale si sta effettuando una chiamata** (Caller ID) per l'operazione di apposizione della Firma Elettronica Qualificata (esempio in *Figura 1*).

Figura 1

di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici.

il processo di firma si compone di due fasi:

FASE1. Strong authentication (componente MOST/SecureCall).
La fase di strong authentication avviene con una chiamata ad un numero verde, durante la quale l'utente digita un codice OTP di sessione. In questo caso non è richiesto nessun token o dispositivo generatore di chiavi addizionale, in quanto l'utente può usare direttamente il proprio cellulare senza nessuna applicazione a bordo.

FASE 2. Firma del documento.

1) L'utente visualizza e naviga il documento da firmare dal suo PC/Tablet;
2) L'utente seleziona i punti firma che vuole sottoscrivere all'interno del documento;
3) Viene visualizzato sul desktop del PC (nello scenario da sportello) o del tablet (nello scenario da mobile) un numero e un codice OTP;
4) L'utente chiama il numero che appare sullo schermo (oppure scannerizza il QRCode);
5) MOST/SecureCall Server risponde (tramite IVR) alla chiamata e chiede all'utente tramite messaggio vocale di digitare l'OTP.
6) Per lo sblocco del certificato qualificato (custodito negli HSM di TI Trust Technologies) MOST/SecureCall verifica che:
   a) il numero chiamante corrisponde al numero associato al profilo utente del firmatario;
   b) il codice OTP digitato corrisponda a quello associato alla specifica operazione.

7) Una volta effettuata la verifica positiva il documento viene firmato.

2.1.2.2 OTP via SMS

La variante Firma con SMS OTP prevede anch'essa una fase di strong authentication che precede la fase di firma. In questo caso però invece che effettuare una chiamata ad un numero verde, **l'utente riceve un sms contenente un codice OTP** (esempio *Figura 2*).

La fase di strong authentication via SMS viene utilizzata per lo "sblocco" del certificato.

Figura 2

1) L'utente visualizza e naviga il documento da firmare dal suo PC/Tablet;
2) L'utente seleziona i punti firma che vuole sottoscrivere all'interno del documento;
3) L'utente riceve sul proprio telefono cellulare un SMS contenente un codice OTP di sessione che inserisce nell'apposito box sul desktop del pc (nello scenario da sportello) o del tablet (nello scenario da mobile);
4) MOST/SecureCall verifica che il codice OTP digitato corrisponda a quello associato alla specifica operazione.
5) Una volta effettuata la verifica, il documento viene firmato.

2.1.2.3 Via App mobile

Attraverso la App "Trust Signer" (disponibile per iOS e Android) il titolare di firma dispone di una applicazione mobile di firma remota e autorizzazione per usufruire della firma digitale qualificata in mobilità, con estrema semplicità e flessibilità di utilizzo, con elevati standard di sicurezza e con un'esperienza d'uso personalizzata per l'offerta commerciale verso Trust Technologies.

Al primo download è necessaria una fase di enrollment, basato sul numero di telefono che è stato utilizzato per la registrazione del certificato di firma remota.

Segue ricezione dell'SMS di conferma per completare l'associazione certificato di firma/smartphone.

In seguito alla "registrazione" della App, l'operazione di firma digitale si completa attraverso la ricezione di notifiche push (servizio smartOTP) a ogni operazione di firma remota.

La App è anche strumento di autorizzazione della firma digitale nelle situazioni in cui il servizio di firma elettronica qualificata, e i servizi smartOTP, sono integrati con portali di terze parti.

2.1.3 Biometrico

Al momento della registrazione, al Titolare viene associato un insieme di **informazioni caratteristiche della sua firma autografa**, rilevate da un apposito dispositivo di tipo grafometrico e consegnata una busta contenente i codici segreti per l'utilizzo del servizio.

Nella fase di autenticazione forte (finalizzata all'operazione di firma), il Titolare dovrà apporre su un dispositivo grafometrico la propria firma autografa per consentire alla CA TI Trust Technologies di verificarne la corrispondenza alle informazioni rilevate per essa al momento della registrazione.

Per l'autenticazione forte Biometrica, è prevista la possibilità di non rilasciare ai titolari del certificato di firma i codici segreti per l'utilizzo del servizio. In tal caso:

- nell'operazione di firma, il titolare appone la propria firma autografa esclusivamente su un dispositivo grafometrico installato presso una postazione presidiata da un addetto dell'Organizzazione del cliente o della CA di TI Trust Technologies che accerta direttamente l'identità del titolare e, dunque, non viene effettuata la verifica del codice PIN;
- l'utilizzo della firma del titolare viene limitato ("firma per scopo"). A tal fine, nei certificati sarà presente un limite d'uso.

Le tavolette grafometriche saranno istallate sulle attuali postazioni di lavoro tramite una semplice porta USB.

La soluzione si presta prevalentemente in contesti bancari (filiali) e in tutte le situazioni nelle quali è richiesta la presenza fisica 'a sportello' del sottoscrittore.

2.1.4 Massiva

La soluzione di Firma Sicura Remota **massiva** è variante della firma remota utilizzabile in contesti automatici per la firma di grossi volumi di documenti.

È un servizio erogato in modalità applicativa, basato sull'emissione e la gestione di Certificati di firma elettronica qualificata per chiavi di sottoscrizione.
Le chiavi sono custodite su HSM installati presso il CED del certificatore e sono utilizzabili per la firma in modalità massiva dei documenti ai sensi della normativa vigente in materia.

È prevista la fornitura di un Certificato Qualificato per utente e, se richiesto, l'erogazione di un servizio di marcatura temporale di tipo applicativo da utilizzarsi nello stesso ambito di servizio.

2.2 Servizio di identificazione e formazione

Preliminarmente all'emissione di un certificato di Firma Elettronica Qualificata è necessario che il Prestatore di Servizi Fiduciari Qualificati (QTSP) **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 Prestatore di Servizi Fiduciari Qualificati (QTSP) stesso o da personale da esso formato e delegato.

Le principali modalità che TI Trust Technologies mette in campo per l'identificazione del richiedente un certificato di Firma Elettronica Qualificata sono:

- *de visu*, ossia di persona tramite esibizione a vista di un valido documento d'identità;
- mediante *utilizzo della firma elettronica qualificata* emessa da altro QTSP. TI Trust Technologies si basa sul riconoscimento già effettuato da un altro Qualified Trust Service Provider che ha emesso il certificato qualificato utilizzato dal richiedente per firmare digitalmente la richiesta in formato elettronico;
- mediante *Videoidentificazione da remoto*, ovvero nel corso di una sessione audio video registrata automaticamente, alla quale il richiedente partecipa assieme ad un operatore incaricato designato da TI Trust Technologies;
- con identità digitale SPID, attraverso un processo di autenticazione SPID con credenziali di livello 2 o 3;
- altre modalità, eseguite da soggetti destinatari degli obblighi di Identificazione e Adeguata Verifica, ai sensi delle normative vigenti, di finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo, e delle successive ulteriori normative comunitarie di esecuzione.

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***, su tutto il territorio nazionale.

Per ulteriori dettagli sul servizio di identificazione e formazione è disponibile il CPS del QTSP pubblicato nell'apposita sezione del sito di TI Trust Technologies:

https://www.trusttechnologies.it/download/documentazione .

2.3 Obiettivi del servizio e vantaggi per gli utilizzatori

Dalle caratteristiche proprie della firma digitale (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;
- **smaterializzazione** 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 3 "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 QTSP 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.

2.4 Supporto tecnico

I titolari del servizio Firma Sicura 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.