

Linee guida sulla qualità dei beni e dei servizi ICT per la definizione ed il governo dei contratti della Pubblica Amministrazione

Manuale operativo

# Dizionario delle Forniture ICT

Classe di Fornitura

# Certificazione della Firma digitale CFD

---

Numero d'Oggetto/Part Number	Ed./Issue	Data/Date	Com. Mod./Ch. Notice	2.3.1 CFD CERTIFICAZIONE DELLA FIRMA DIGITALE
MANUALE 4	2.0	19.05.2008	---	

## INDICE

1	GENERALITÀ SUL DOCUMENTO.....	3
2	DESCRIZIONE DELLA CLASSE DI FORNITURA.....	4
3	MODALITÀ DI DEFINIZIONE DELLA FORNITURA.....	4
3.1	OBIETTIVI.....	5
3.2	UTENZA.....	6
3.3	DIMENSIONI.....	6
3.4	VINCOLI E REQUISITI.....	7
3.5	STANDARD E NORME.....	7
4	MODALITÀ DI STIMA DEI COSTI ANCHE IN FUNZIONE DELLA QUALITÀ RICHIESTA.....	8
5	DESCRIZIONE DELLE ATTIVITÀ E DEI PRODOTTI.....	8
5.1	GESTIONE OPERATIVA.....	9
5.2	DESCRIZIONE DELLE CLASSI DI FORNITURA ASSOCIABILI.....	10
6	DESCRIZIONE DEI PROFILI PROFESSIONALI COINVOLTI.....	12
7	INDICATORI/MISURE DI QUALITÀ.....	17
8	GLOSSARIO.....	22

---

Numero d'Oggetto/Part Number	Ed./Issue	Data/Date	Com. Mod./Ch. Notice	
MANUALE 4	2.0	19.05.2008	---	2.3.1 CFD CERTIFICAZIONE DELLA FIRMA DIGITALE

## 1 GENERALITÀ SUL DOCUMENTO

Questo documento descrive uno dei lemmi del Manuale operativo “Dizionario delle forniture ICT” delle Linee guida sulla qualità dei beni e dei servizi ICT per la definizione ed il governo dei contratti della Pubblica Amministrazione. Ogni lemma del Dizionario rappresenta una classe di fornitura ICT elementare. Il Dizionario contiene tutte le classi di forniture che si sono ritenute necessarie per rappresentare compiutamente i contratti ICT delle pubbliche amministrazioni. Ogni lemma del Dizionario è autoconsistente e indipendente; esso prevede:

- **la descrizione della classe di fornitura ICT elementare**, che ha lo scopo di definirne univocamente l’ambito di applicazione;
- **l’esplicitazione di “regole” per l’uso della classe di fornitura**, utile a proporre al lettore suggerimenti sull’uso del lemma per la stesura dell’oggetto contrattuale;
- **la descrizione delle attività** relative alla classe di fornitura e dei relativi prodotti, utile al lettore come traccia riutilizzabile per scrivere contratti e capitolati tecnici;
- **una tabella che riassume attività, prodotti e indicatori di qualità**, utile al lettore come quadro sinottico che riassume il legame tra attività e relativi prodotti da queste realizzati ed identifica, in relazione ad entrambi, gli indicatori di qualità adottati per la classe di fornitura;
- **una scheda per ogni indicatore di qualità** (presente nella tabella di cui sopra), utile al lettore come traccia riutilizzabile, per scrivere contratti e capitolati tecnici;
- **un glossario** (ove necessario) specifico per la classe di fornitura.

Nell’ambito della complessa attività di scrittura di contratti e capitolati tecnici, i lemmi possono essere intesi come “ricette contrattuali” di immediato utilizzo mediante processi di copia e incolla, per rappresentare le esigenze dell’Amministrazione.

Nell’ottica del riuso, particolare attenzione dovrà essere prestata alle imprescindibili e necessarie attività di specificazione e taratura delle classi di fornitura ICT elementari utilizzate e, successivamente, all’integrazione delle diverse classi di fornitura scelte in un unico e coerente contratto ICT.

La versione digitale di ogni lemma è singolarmente scaricabile dal sito CNIPA in formato editabile (.doc) che ne permette il riutilizzo anche parziale.

Per maggiori informazioni sull’utilizzo integrato delle classi di fornitura e dei processi trasversali si rimanda agli esempi contenuti nel Manuale applicativo “Esempi di applicazione”.

---

Numero d'Oggetto/Part Number	Ed./Issue	Data/Date	Com. Mod./Ch. Notice	2.3.1 CFD CERTIFICAZIONE DELLA FIRMA DIGITALE
MANUALE 4	2.0	19.05.2008	---	

## 2 DESCRIZIONE DELLA CLASSE DI FORNITURA

Per firma digitale qualificata si intende un servizio finalizzato ad assicurare la paternità, integrità e riservatezza ai documenti elettronici prodotti, mediante la fornitura di specifici dispositivi hardware e software.

La firma digitale è basata su un procedimento di “crittografia asimmetrica”, che fa uso di una coppia di chiavi a 1024 bit: una privata, utilizzata per firmare (che dovrà essere tenuta segreta e conservata in maniera sicura dal titolare), e una pubblica, utilizzata per le operazioni di verifica della firma. La corrispondenza tra le chiavi di firma e il sottoscrittore è garantita da una terza parte fidata, l’Ente Certificatore, riconosciuto da CNIPA.

Ogni titolare del servizio, infatti, dispone di un dispositivo sicuro di firma (smart card, token USB o altro dispositivo idoneo) nel quale è stata generata una coppia di chiavi assieme ad un certificato di firma che consente l’associazione della persona con la sua chiave pubblica. Tale associazione avviene solo dopo l’identificazione e registrazione certa del richiedente da parte dell’Ente Certificatore che ha anche il compito di gestire l’intero ciclo di vita del certificato, compresa la sospensione temporanea della sua validità o la sua revoca definitiva.

## 3 MODALITÀ DI DEFINIZIONE DELLA FORNITURA

Nei casi in cui l’Amministrazione intenda acquistare il servizio di Certificazione della Firma Digitale (CFD) può rivolgersi ad un Certificatore Accreditato, che assicura l’erogazione del servizio previsto e la fornitura dei prodotti necessari alla sua fruizione. Si tratta di forniture che fanno riferimento al servizio come definito dal Certificatore all’interno del **Manuale Operativo**, depositato e pubblicato presso il CNIPA.

Nel suddetto Manuale sono riportate le procedure applicate dal Certificatore Accreditato nello svolgimento della propria attività, stabilendo obblighi e responsabilità del Certificatore, del titolare e di quanti accedono alle evidenze pubbliche per eseguire la verifica delle firme.

L’Ente Certificatore ha anche l’onere di rendere noto l’insieme di regole cui si attiene nella sua attività di certificazione delle chiavi pubbliche per consentire l’applicabilità di un certificato ad una particolare comunità e/o la classe di applicazioni con requisiti di sicurezza comuni.

Il **deliverable** al Titolare del Certificato è costituito dal dispositivo sicuro di firma contenente il Certificato di Firma Digitale, unitamente a tutti i prodotti e servizi accessori, descritti di seguito:

- Emissione e gestione del certificato di Firma Digitale, come definito dalla vigente normativa sulla documentazione amministrativa (TUDA dpr 445/2000 e successive modifiche) e gestito secondo le norme di qualità (UNI EN ISO 9002);
- Generazione di una coppia di chiavi almeno a 1024 bit, secondo procedimento di crittografia asimmetrica;
- Fornitura del dispositivo sicuro di firma;

---

Numero d’Oggetto/Part Number	Ed./Issue	Data/Date	Com. Mod./Ch. Notice	2.3.1 CFD CERTIFICAZIONE DELLA FIRMA DIGITALE
MANUALE 4	2.0	19.05.2008	---	

- Fornitura del lettore di smart card (ove necessario);
- Fornitura del client software per la firma, la verifica delle firme ed eventualmente per la cifratura dei documenti (dispositivo di verifica della firma);
- Fornitura della manualistica di supporto;
- Servizio locale di Registrazione dei Titolari.

A completamento del servizio di Certificazione, possono essere richiesti altri servizi riferiti ad altre classi di fornitura, di seguito individuate:

- **1.3.1 – Assistenza in remoto e in locale:** Help Desk di primo livello per l'assistenza all'utente in fase di installazione dei dispositivi HW e SW e l'inoltro delle richieste di sospensione, riabilitazione e revoca del certificato; Help Desk di secondo livello per la risoluzione di problematiche inerenti il non corretto funzionamento dei sistemi del Certificatore.
- **1.3.2 – Formazione e addestramento:** per fornire all'Amministrazione informazioni specifiche sulla normativa vigente e le funzioni d'uso inerenti la firma digitale ed il corretto uso dei dispositivi di firma, nonché illustrare ad un Incaricato scelto dall'Amministrazione il funzionamento del servizio locale di Registrazione dei Titolari.
- **5.1.1 – Fornitura prodotti HW e SW:** per l'erogazione del servizio di firma in modalità hosting, housing e on site, e. per lo sviluppo di servizi applicativi che prevedono al loro interno funzionalità di firma digitale.

### 3.1 OBIETTIVI

In virtù dei requisiti richiesti per l'emissione e la gestione del **servizio di firma digitale**, un documento informatico sottoscritto con firma digitale garantisce il soddisfacimento delle esigenze di integrità e non ripudio del documento stesso. Questo, inoltre, è equiparato ad un documento cartaceo con firma autografa, purché siano soddisfatti i seguenti requisiti:

- sia sottoscritto con firma digitale o con un altro tipo di firma elettronica avanzata;
- la firma sia basata su di un certificato qualificato (e quindi emesso da un Certificatore Accreditato presso il CNIPA);
- la firma sia generata mediante un dispositivo sicuro per la creazione di una firma.

Secondo quanto stabilisce la normativa corrente, se tutti i requisiti sono contemporaneamente soddisfatti, il documento informatico firmato digitalmente fa piena prova, fino a querela di falso, della provenienza delle dichiarazioni da chi l'ha sottoscritto. All'uopo, si ricorda che la normativa vigente prescrive che:

- in tutti i documenti informatici delle pubbliche amministrazioni la firma autografa o la firma, comunque prevista, è sostituita dalla firma digitale;
- l'uso della firma digitale integra e sostituisce ad ogni fine di legge l'apposizione di sigilli, punzoni, timbri, contrassegni e marchi comunque previsti.

Numero d'Oggetto/Part Number	Ed./Issue	Data/Date	Com. Mod./Ch. Notice	2.3.1 CFD CERTIFICAZIONE DELLA FIRMA DIGITALE
MANUALE 4	2.0	19.05.2008	---	

### 3.2 UTENZA

Per meglio distinguere il diverso profilo degli utenti del servizio CFD è necessario identificare tutti gli attori principali di questa classe di fornitura:

- **Gestore del servizio / Terza Parte Fidata:** L'Ente Certificatore che garantisce, mediante l'emissione del certificato digitale, l'associazione tra la persona (l'Utente Titolare) e la sua chiave pubblica, generati all'interno del dispositivo sicuro di firma;
- **Cliente:** L'Amministrazione che sigla il contratto di fornitura con l'Ente Certificatore per i suoi dipendenti (Utenti Titolari) verso cui erogare il servizio di Certificazione;
- **Utenti Titolari,** dipendenti dell'Amministrazione che possono utilizzare il certificato di firma digitale per firmare documenti informatici che assumono così la rilevanza giuridica dettata dalla normativa in materia;
- **Incaricati,** dipendenti dell'Amministrazione che sono incaricati dal Certificatore e dall'Amministrazione di effettuare le operazioni di identificazione e di censimento degli utenti titolari appartenenti all'ente richiedente. Tali utenti fungono da punto di riferimento interno all'Amministrazione per i rapporti tra il certificatore e gli utenti titolari (tale funzione viene di solito indicata come RA locale - Registration Authority) e provvedono anche alla consegna dei kit ai rispettivi titolari.

Ove il Certificatore metta a disposizione un applicativo web per automatizzare le operazioni di registrazione degli Utenti Titolari, gli utenti amministratori devono essere muniti di idonei strumenti di accesso (smart card con certificato di autenticazione o identificativo personale e password), mentre è rimesso alle scelte dell'Amministrazione che dispongano anche del certificato di firma qualificata.

### 3.3 DIMENSIONI

I Certificatori che offrono servizi di firma qualificata sono accreditati presso il CNIPA e devono pubblicare nel Manuale Operativo tutte le informazioni relative alle modalità con cui il servizio viene erogato. Tale servizio, per ciascun Certificatore, corrisponde quindi ad una proposta definita e standardizzata che ha come corrispettivo un prezzo predeterminato. Spesso, le richieste delle Pubbliche Amministrazioni possono presentare esigenze particolari che giustificano la modifica di tali servizi di riferimento e, conseguentemente, del loro prezzo. Lasciando da parte fattispecie molto complesse che rientrano nel campo della progettazione di sistemi informatici e nell'erogazione di servizi integrati, si possono indicare alcuni elementi che possono influenzare costi, rischi e qualità del servizio di Certificazione digitale:

- **Periodo di validità del certificato digitale.** L'esistenza del certificato di firma qualificata presuppone un'attività di gestione curata dal Certificatore, il quale deve assicurare che un insieme di informazioni e di operazioni riguardanti il certificato risultino sempre disponibili in linea. L'onere derivante da questa gestione corrisponde al costo del servizio ed è quindi variabile in funzione della durata per cui deve essere assicurata la gestione stessa;
- **Caratteristiche del dispositivo sicuro di firma.** La **capacità in KB** del dispositivo determina un limite fisico al suo utilizzo: sebbene sia possibile utilizzare dispositivi in grado di scrivere e riscrivere sulla propria memoria, le chiavi o i certificati, in molti casi non possono essere cancellati, accumulandosi fino ad impedire l'impiego del dispositivo

Numero d'Oggetto/Part Number	Ed./Issue	Data/Date	Com. Mod./Ch. Notice	2.3.1 CFD CERTIFICAZIONE DELLA FIRMA DIGITALE
MANUALE 4	2.0	19.05.2008	---	

per la remissione del certificato di firma qualificata.  
 Vi è poi la possibilità che il dispositivo si **usuri**, impedendo il normale funzionamento. In questi casi, sarà necessario revocare i certificati in uso ed emetterne dei nuovi, unitamente alla consegna di un nuovo dispositivo di firma;

- **Modalità di registrazione.** Tipicamente il Certificatore definisce e pubblica nel proprio Manuale Operativo le procedure per la richiesta e l'emissione dei certificati di firma qualificata. La modifica di tali procedure da parte dell'Amministrazione, sempre compatibilmente con le disposizioni vigenti, può avere impatto sui costi del servizio;
- **Disponibilità del servizio.** Anche in questo caso il Certificatore definisce e pubblica nel proprio Manuale Operativo i tempi ed i modi in cui il servizio che fornisce è disponibile, e questo costituisce un riferimento per il prezzo praticato. Ove l'Amministrazione richiedesse modifica a tali tempi e modi, sempre compatibilmente con le disposizioni vigenti, si possono verificare impatti sui costi del servizio.

### 3.4 VINCOLI E REQUISITI

I Certificatori che emettono i certificati di Firma Digitale devono possedere i seguenti requisiti essenziali:

- Iscrizione nel registro pubblico firmato dal CNIPA ([www.cnipa.it](http://www.cnipa.it));
- Garantire l'accertamento dell'identità del titolare con documenti ufficiali;
- Utilizzare specifiche procedure, rese note mediante la pubblicazione di un apposito Manuale Operativo. Tali procedure devono essere tali da dimostrare l'aderenza del Certificatore a tutti i requisiti previsti dalla normativa vigente;
- Garantire la conservazione della documentazione relativa all'identificazione per dieci anni dalla scadenza dei certificati.

### 3.5 STANDARD E NORME

L'oggetto della fornitura deve essere conforme a quanto stabilito dai riferimenti normativi e regolamentari. Di seguito si indicano i principali:

- Fonti nazionali:
  - DPR 28/12/2000, n. 445 - Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa, con tutte le sue successive modifiche ed integrazioni;
  - DPCM 13/01/2004 - Regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici;
  - D. Leg.vo 23/01/2002, n. 10, di recepimento della Direttiva 1999/93/CE sulla firma elettronica;
  - CIRCOLARE n. AIPA/CR/27, 16/02/2001 – Relativa all'Art. 17 del DPR 10/11/1997, n. 513: utilizzo della firma digitale nelle Pubbliche Amministrazioni.

- Fonti UE:

Numero d'Oggetto/Part Number	Ed./Issue	Data/Date	Com. Mod./Ch. Notice	2.3.1 CFD CERTIFICAZIONE DELLA FIRMA DIGITALE
MANUALE 4	2.0	19.05.2008	---	

Direttiva 1999/93/CE sulla firma elettronica.

Standard: gli standard di riferimento sono quelli internazionalmente riconosciuti (X509, PKCS, RTF) e quelli specificamente individuati dalla Commissione europea secondo la procedura di cui all’art. 9 della Direttiva sopra citata.

In particolare, per quanto concerne i dispositivi di firma si indica il “CWA 14169 (March 2002): secure signature-creation devices”

**4 MODALITÀ DI STIMA DEI COSTI ANCHE IN FUNZIONE DELLA QUALITÀ RICHIESTA**

Gli aspetti economici da considerare per la determinazione del costo di un servizio CFD sono principalmente dipendenti da:

- costo della tecnologia da acquistare: la piattaforma tecnologica ed i programmi applicativi;
- costo del personale;
- costi fissi di struttura;
- costi diretti o variabili generati in base ai diversi sistemi di accounting previsti dal Service Provider (offerte flat o a consuntivo, in base al numero di utenze attivate e certificati utilizzati, ecc.).

Generalmente, l’Ente Certificatore eroga verso gli utenti del servizio offerte a pacchetto che comprendono oltre al certificato digitale, il dispositivo sicuro di firma, il lettore (nel caso di impiego di Smart Card come dispositivo), il client sw per la firma dei documenti elettronici e la fornitura di manualistica di supporto. Tali kit di offerta sono resi noti dal Certificatore con le modalità indicate nel Manuale Operativo.

In considerazione del fatto che il servizio di Certificazione può essere sviluppato mediante l’integrazione di altre classi di fornitura come indicato in precedenza, si rimanda alle suddette classi per la determinazione del prezzo di un servizio di Certificazione evoluto.

**5 DESCRIZIONE DELLE ATTIVITÀ E DEI PRODOTTI**

Le attività ed i prodotti relativi ai processi organizzativi e di supporto (processi trasversali), e cioè per esempio quelli relativi a gestione, documentazione, gestione della configurazione e assicurazione della qualità non sono descritti nel seguito e per la loro descrizione si rimanda alle classi specifiche.

Nel caso in cui attività o prodotti relativi a questi processi abbiano particolare rilevanza o criticità per la classe, essi sono comunque richiamati, evidenziando gli aspetti rilevanti o critici, rimandando per le caratteristiche generali alla classe del processo.

Il profilo professionale EUCIP responsabile delle attività della classe di fornitura è il Consulente per la Sicurezza (per maggiori dettagli si rimanda al successivo paragrafo 6).

Numero d’Oggetto/Part Number	Ed./Issue	Data/Date	Com. Mod./Ch. Notice	2.3.1 CFD CERTIFICAZIONE DELLA FIRMA DIGITALE
MANUALE 4	<b>2.0</b>	<b>19.05.2008</b>	---	

La seguente tabella riassume i prodotti in ingresso ed uscita, distinti in tre casi tipici dell'attività di Gestione Operativa. Il profilo professionale EUCIP responsabile dell'attività nel suo complesso è il Consulente per la Sicurezza (per ulteriori dettagli si rimanda al successivo capitolo 6)

Attività	Input	Output	Profilo Professionale Responsabile
Gestione operativa	<u>Richiesta di Attivazione/Rinnovo del Servizio</u>	<u>Emissione/Rinnovo del Certificato</u> <u>Generazione delle chiavi asimmetriche</u> <u>Dispositivo sicuro di firma</u> <u>Lettores di Smart card (eventuale)</u> <u>SW Client per la firma e verifica delle firme</u> <u>Servizio Locale di Registrazione dei Titolari</u>	<u>Consulente per la Sicurezza</u>
	<u>Richiesta di Sospensione del Servizio</u>	<u>Sospensione del Certificato</u> <u>Emissione della Lista dei Certificati Sospesi (CSL)</u>	
	<u>Richiesta di Revoca del Servizio</u>	<u>Revoca del Certificato</u> <u>Emissione della Lista dei Certificati Revocati (CRL)</u>	

### 5.1 GESTIONE OPERATIVA

La gestione di un Certificato Digitale, da parte di un Ente Certificatore, comporta un insieme di attività necessarie a garantire la conformità alle procedure operative predeterminate insieme con il cliente.

Tali procedure devono rispettare le indicazioni generali imposte dalla normativa in materia e risultano uguali per tutti i Prestatori di Servizi di Certificazione a conformi alla norma.

In generale, prescindendo dalla tipologia dei certificati e dalle procedure di dettaglio, le attività di gestione sono:

- richiesta ed emissione;
- revoca, sospensione, riattivazione e rinnovo.

Altre attività a supporto delle precedenti sono:

- produzione e fornitura di report sui servizi;
- operazioni per la verifica dello stato del certificato, ovvero:
  - download della lista dei certificati revocati CRL (Certificate Revocation List);
  - emissione periodica o a richiesta della CRL.

Si ricorda che il deliverable al Titolare del Certificato è costituito dal **dispositivo sicuro** di firma contenente il **Certificato di Firma Digitale** e le chiavi asimmetriche per la firma dei documenti elettronici, unitamente a tutti i prodotti accessori come la licenza d'uso dell'**applicativo software** per la firma e la verifica delle firme, l'eventuale **lettore** di Smart Card, nonché i codici di accesso per l'utilizzo del Certificato e la manualistica di supporto forniti ai Titolari attraverso il **Servizio Locale di Registrazione** dei Titolari.

Numero d'Oggetto/Part Number	Ed./Issue	Data/Date	Com. Mod./Ch. Notice	2.3.1 CFD CERTIFICAZIONE DELLA FIRMA DIGITALE
MANUALE 4	2.0	19.05.2008	---	

**Revoca, sospensione, riattivazione e rinnovo del Certificato di Firma**

Il Titolare o un Terzo Interessato può richiedere in qualsiasi momento la revoca o la sospensione del certificato, attraverso le diverse modalità previste dal Certificatore nel Manuale Operativo (come l'invio della richiesta via fax, tramite web o raccomandata A/R) che consentano al Certificatore di poter identificare con certezza la paternità della richiesta e la coerenza della motivazione fornita nella richiesta.

Il certificato revocato è iscritto in una lista apposita (Lista di Revoca dei Certificati - CRL).

Così come per la revoca, anche la procedura di sospensione di un certificato determina l'immediata cessazione della sua validità, indipendentemente dalla data di scadenza del certificato medesimo, sino al momento della sua eventuale riabilitazione. La sospensione non inficia la validità del certificato nel lasso di tempo precedente il momento della sospensione stessa. Con la sospensione, il certificato viene inserito in un'apposita lista (Lista di Sospensione dei Certificati - CSL).

Il certificato sospeso può essere riabilitato quando si verifichino le relative condizioni, specificate nelle procedure concordate con l'Amministrazione.

Di norma, il rinnovo consiste in una nuova emissione effettuata dall'Ente Certificatore, in prossimità della data di scadenza del vecchio certificato del titolare.

**5.2 DESCRIZIONE DELLE CLASSI DI FORNITURA ASSOCIABILI**

Attraverso l'associazione con altre classi di fornitura, il servizio di "base" di Certificazione della Firma Digitale può essere sviluppato per meglio adattarsi alle esigenze dell'Amministrazione, secondo le indicazioni fornite di seguito.

**Servizio di assistenza telefonica**

Il servizio di assistenza telefonica deve garantire almeno le seguenti prestazioni:

- acquisizione delle richieste di sospensione con copertura H24;
- acquisizione delle richieste di assistenza dal lunedì al venerdì, dalle 8,00 alle 17,00, esclusi i giorni festivi;
- conduzione tramite personale tecnico specializzato.

**Servizio di assistenza telefonica e supporto tecnico di 2° livello**

Il livello minimo di assistenza e supporto tecnico specialistico (2° livello) deve essere fornito su chiamata telefonica, ai seguenti destinatari del servizio:

- il personale che svolgerà funzioni di RA Territoriale;
- il personale tecnico della organizzazione dell'Amministrazione.

**Fornitura di prodotti HW e SW**

Il servizio di CFD, oltre che nelle modalità fin qui delineate, può essere acquisito dall'Amministrazione secondo le differenti modalità descritte qui di seguito che richiamano la

Numero d'Oggetto/Part Number	Ed./Issue	Data/Date	Com. Mod./Ch. Notice	2.3.1 CFD CERTIFICAZIONE DELLA FIRMA DIGITALE
MANUALE 4	2.0	19.05.2008	---	

suddetta classe di fornitura. Nell'elenco viene indicato anche se è necessaria la qualifica dell'Amministrazione come Certificatore Accreditato dal CNIPA.

- **soluzione in hosting:** il Certificatore, utilizzando le proprie infrastrutture e le proprie piattaforme di erogazione, eroga servizi personalizzati per conto dell'Amministrazione; non necessariamente fornisce anche i prodotti hardware e software per la fruizione dei servizi.

Queste modalità sono adatte a forniture con bacini di utenza numerosi (ordine di grandezza delle **migliaia e oltre**) per le quali l'Amministrazione esprima esigenze di maggiore personalizzazione (come ad esempio una diversa modalità per l'attivazione dei Titolari tramite web, l'integrazione della firma digitale in applicazioni client / server dell'Amministrazione, un più elevato livello di assistenza sistemistica, la richiesta di architetture dislocate diversamente sul territorio per l'erogazione del servizio).

Nella modalità di fornitura in hosting si possono dare 4 casi distinti:

1. **Soluzione condivisa: fornitore come Certificatore Accreditato**

L'Amministrazione dispone di un ambiente SW dedicato, ma gestito su server e motori di firma condivisi.

Le smart card sono emesse dal Certificatore.

La fornitura prevede anche una licenza di CA (Certification Authority), l'installazione e la personalizzazione dell'ambiente SW dedicato.

2. **Soluzione condivisa: l'Amministrazione come Certificatore Accreditato**

L'Amministrazione dispone di un ambiente SW e HW dedicato ed emette in autonomia le smart card.

La fornitura prevede una licenza di Certification Authority, l'installazione e la personalizzazione dell'ambiente SW dedicato, hardware e software per la produzione delle buste oscurate e periferiche di personalizzazione delle Smart Card.

3. **Soluzione dedicata: fornitore come Certificatore Accreditato**

L'Amministrazione dispone di un ambiente SW e HW dedicato.

Le smart card sono emesse dal Certificatore.

La fornitura prevede una licenza di CA, un cluster, una coppia di web server, una coppia di Directory server, licenze di backup e monitoraggio, due motori di firma, installazione e personalizzazione dell'ambiente SW dedicato.

4. **Soluzione dedicata: l'Amministrazione come Certificatore Accreditato**

L'Amministrazione dispone di un ambiente SW e HW dedicato ed emette in autonomia le smart card.

La fornitura prevede una licenza di CA, un cluster, una coppia di web server, una coppia di Directory server, licenze di backup e monitoraggio, due motori di firma, installazione e personalizzazione dell'ambiente SW dedicato, hardware e software per la produzione delle buste oscurate e periferiche di personalizzazione delle Smart Card.

- **Soluzione in housing:** il Certificatore ospita e gestisce presso proprie infrastrutture gli apparati dell'Amministrazione necessari all'erogazione del servizio di Certificazione Digitale.

Il fornitore può agire anche come consulente nella fase di progettazione.

Numero d'Oggetto/Part Number	Ed./Issue	Data/Date	Com. Mod./Ch. Notice	2.3.1 CFD CERTIFICAZIONE DELLA FIRMA DIGITALE
MANUALE 4	2.0	19.05.2008	---	

Tale modalità è particolarmente adatta in caso di bacini di utenza molto numerosi (ordine di grandezza delle **decine di migliaia e oltre**) e per Amministrazioni che esprimono elevati livelli di personalizzazione della propria soluzione (come ad esempio un più elevato livello di assistenza sistemistica ed una maggiore riservatezza dei dati e delle applicazioni client / server dell'Amministrazione).

- **Soluzione on site presso l'Amministrazione, gestita dal Certificatore:**  
Il Certificatore progetta, realizza e gestisce la soluzione presso le sue infrastrutture, in base ai requisiti dell'Amministrazione.  
Tale modalità è adatta per le Amministrazioni che devono servire bacini di utenza molto numerosi (ordine di grandezza delle **decine di migliaia e oltre**) e che esprimono esigenze complesse con elevati livelli di personalizzazione, fra cui l'esigenza di qualificarsi come Certificatori Accreditati, presso il CNIPA, oppure la possibilità di poter reingegnerizzare completamente il processo di attivazione dei Titolari, disporre di una maggiore riservatezza dei dati e delle proprie applicazioni client / server.
- **Fornitura chiavi in mano presso l'Amministrazione, gestita dalla stessa:**  
Il Certificatore provvede a fornire all'Amministrazione le apparecchiature richieste, nella configurazione concordata. Non sono previste attività di erogazione, mentre si possono prevedere attività di consulenza in fase di progettazione e le usuali attività di manutenzione.  
Tale modalità è adatta per le Amministrazioni che devono servire bacini di **utenza molto numerosi** e che esprimono specifiche e stringenti esigenze di controllo di processo, tali da non poter essere soddisfatte dalle precedenti modalità.  
L'Amministrazione deve qualificarsi come Certificatore Accreditato presso il CNIPA.

#### **Formazione del personale addetto**

Devono essere previsti strumenti di formazione orientati sia agli utenti titolari sia agli utenti amministratori, per consentire loro di trarre i massimi benefici dal servizio.

L'obiettivo primario del piano di formazione è di fornire le competenze operative necessarie per poter sfruttare al meglio le potenzialità offerte dai servizi realizzati, ed in particolare:

- Comprendere gli obiettivi e le potenzialità del servizio messo a disposizione;
- Utilizzare al meglio le funzionalità ed i servizio messi a loro disposizione;
- Comprendere il significato dei dati che il sistema tratta e come le informazioni provenienti dal sistema possono essere utili nelle loro attività operative.

## **6 DESCRIZIONE DEI PROFILI PROFESSIONALI COINVOLTI**

Il fornitore del servizio, ossia l'Ente Certificatore che emette il certificato di firma digitale, provvederà all'erogazione del servizio avvalendosi di una struttura organizzativa e di competenze professionali coerenti con quanto riportato nello specifico Manuale Operativo depositato e pubblicato presso il CNIPA.

Numero d'Oggetto/Part Number	Ed./Issue	Data/Date	Com. Mod./Ch. Notice	2.3.1 CFD CERTIFICAZIONE DELLA FIRMA DIGITALE
MANUALE 4	2.0	19.05.2008	---	

In questo paragrafo sono descritti i profili professionali, di natura generale, tipicamente coinvolti nello svolgimento delle attività della classe di fornitura e riferiti al framework di competenze EUCIP.

Nella tabella seguente (Matrice di Responsabilità Attività – Profilo Professionale) sono riportati per ciascuna attività i profili professionali EUCIP tipicamente coinvolti nello svolgimento dell'attività stessa e nel rilascio dei relativi prodotti, qualificati in termini di:

- responsabile (**R**), è il profilo professionale che esegue l'attività, coordina gli eventuali contributi di altri profili professionali ed è responsabile primario della qualità dei prodotti dell'attività;
- contributore (**C**), è il profilo professionale che contribuisce con competenze specialistiche (se richieste dal particolare sviluppo) allo svolgimento di elementi dell'attività e può gestire in autonomia, in accordo con il responsabile, specifiche sotto-attività; i contributori sono suddivisi in due categorie:
  - contributore tipico (**Ct**), il suo contributo all'attività è richiesto nella quasi totalità delle istanze di fornitura, una sua eventuale assenza dovrebbe essere considerata un'eccezione e le relative motivazioni dovrebbero essere esplicitate (peculiarità tecniche od organizzative dell'istanza di fornitura)
  - contributore specifico (**Cs**), il suo contributo all'attività è legato alle specificità dell'istanza di fornitura, la sua presenza, anche se frequente, non può essere considerata tipica.

Il profilo professionale che ha maggiori competenze in materia di organizzazione, processi e tecnologie per la sicurezza IT e che è identificato come responsabile delle attività della fornitura è il Consulente per la Sicurezza.

In termini generali, il Consulente per la sicurezza è in grado di assicurare, sia in fase di progettazione di un sistema di sicurezza che di sua gestione operativa, l'efficace integrazione di politiche, procedure e strumenti necessari al conseguimento degli obiettivi aziendali di sicurezza e controllo dei rischi.

Nel contesto della classe di fornitura CFD, il Consulente per la sicurezza è in grado di valutare le esigenze dell'Amministrazione in tema di firma digitale, di coordinare l'organizzazione del fornitore per l'erogazione del servizio, di assicurare il rispetto della normativa e l'utilizzo delle opportune tecnologie.

Contribuiranno all'erogazione del servizio, per la gestione dell'infrastruttura informatica di soluzioni in hosting o in housing se previste (o per la gestione dell'infrastruttura presumibilmente utilizzata dall'Ente Certificatore), i seguenti profili professionali (descritti più avanti): Responsabile di basi di dati, Responsabile di rete, Responsabile della configurazione e del centro dati, Sistemista multiplatforma, Supervisore di un centro di assistenza.

Tutti i profili menzionati sono qualificati come contributori specifici (Cs) in quanto, come indicato nei capitoli precedenti, i servizi di gestione dell'infrastruttura sono opzionali e le modalità organizzative di erogazione del servizio da parte dell'Ente Certificatore possono essere diversificate.

Nel caso la fornitura comprenda anche l'assistenza telefonica e la formazione saranno coinvolti come responsabili delle specifiche attività i profili di Supervisore di un centro di assistenza e Formatore IT (per maggiori dettagli si rimanda alle relative classi di fornitura).

Nel caso di impiego di Registration Authority locale per l'identificazione degli utenti e la distribuzione dei dispositivi di firma (attività usualmente svolta da dipendenti dell'Amministrazione, paragrafo 3.2) potrebbe essere utile prevedere il coinvolgimento per tali

attività del profilo di Amministratore di sistemi informatici che tipicamente gestisce l'infrastruttura IT di una unità locale, supporta gli utenti ed ha specifiche competenze in materia di sicurezza. Le competenze del profilo possono risultare sovradimensionate rispetto alle incombenze (delegabili anche a personale esecutivo opportunamente addestrato), tuttavia l'Amministratore di sistemi informatici potrebbe svolgere, se richieste, una serie di funzioni complementari (di facilitazione al cambiamento e supporto operativo) fondamentali per l'avvio efficace del servizio.

Nella tabella “Matrice di Responsabilità Attività – Profilo Professionale” è anche indicata per ciascun profilo professionale, responsabile (R) o contributore tipico (Ct), un'ipotesi di massima del suo impegno (quantità di lavoro, “effort”) nell'attività. Tale impegno è espresso come percentuale, fatto 100 l'impegno totale richiesto dall'attività, ma non tiene conto della presenza di contributori specifici (Cs). Per il servizio di certificazione della firma digitale, essendo tutti i contributori qualificati come Cs per i motivi in precedenza indicati, tutto l'effort è stimato in carico al profilo di Consulente per la Sicurezza.

TABELLA MATRICE DI RESPONSABILITA' ATTIVITA' – PROFILO PROFESSIONALE

	Attività
Profilo professionale	Gestione operativa
15 – Consulente per la Sicurezza	<b>R 100%</b>
16 – Responsabile di Basi di Dati	Cs
17 – Responsabile di Rete	Cs
18 - Responsabile della Configurazione e del Centro Dati	Cs
19 – Sistemista Multiplatforma	Cs
20 – Supervisore di un Centro di Assistenza	Cs
21 – Formatore IT	Cs
22 – Amministratore di Sistemi Informatici	Cs
% di effort - totale	100%

I profili professionali di riferimento sono quelli definiti dallo schema EUCIP (European Certification of Informatics Professionals) sviluppato dal CEPIS (Council of European Professional Informatics Societies) che, per ciascun profilo, indica le attività tipiche ed il dettaglio delle competenze possedute.

Le sintesi delle competenze dei profili professionali citati sono le seguenti (tra parentesi l'identificativo del profilo):

Numero d'Oggetto/Part Number	Ed./Issue	Data/Date	Com. Mod./Ch. Notice	2.3.1 CFD CERTIFICAZIONE DELLA FIRMA DIGITALE
MANUALE 4	2.0	19.05.2008	---	

**(15) Consulente per la Sicurezza (Security Adviser).** Un consulente per la sicurezza secondo lo standard EUCIP deve essere molto efficace nell'identificare i requisiti di sicurezza dei sistemi ICT e nel definire soluzioni affidabili e agevoli da gestire. Ad una competenza dell'ICT ampia e approfondita deve essere abbinata la capacità di interagire con altre funzioni ICT per favorire l'integrazione di tecnologie per la sicurezza all'interno dell'infrastruttura ICT.

**(16) Responsabili di Basi di Dati (Database Manager).** Un responsabile di basi di dati secondo lo standard EUCIP assume un ruolo centrale tanto nella progettazione di strutture di dati quanto nella gestione ordinaria dei DB; tra i requisiti figurano dunque una profonda competenza in tutti gli aspetti delle tecnologie dei DB, un approccio collaborativo ai contesti di progetto, esperienza nelle tecniche di modellazione dei dati, ma anche l'efficacia nel definire e applicare le procedure e nell'organizzare le operazioni ordinarie.

**(17) Responsabile di Rete (Network Manager).** Un responsabile di rete secondo lo standard EUCIP deve essere molto efficace nel gestire un sistema informativo di rete di media complessità e nel migliorarne le prestazioni. Deve inoltre saper interagire con i progettisti di reti e con eventuali fornitori esterni in merito a tutte le fasi del ciclo di vita di una rete.

**(18) Responsabile della Configurazione e del Centro Dati (Data Centre & Configuration Manager).** Un responsabile della configurazione e del centro dati secondo lo standard EUCIP deve avere un approccio strutturato alla progettazione, allestimento e manutenzione di un ambiente di lavoro supportato dall'IT, sia nel caso di un ambiente di sviluppo, sia nel caso di un sistema “in produzione” destinato agli utenti finali; è richiesta una particolare competenza sulle procedure di qualità e su strumenti e sistemi di gestione procedurale delle attività.

**(19) Sistemista Multiplatforma (X-Systems Engineer).** Un sistemista multiplatforma secondo lo standard EUCIP deve avere una particolare competenza su vari sistemi operativi e sui rispettivi metodi per affrontare i problemi, sull'ottimizzazione delle prestazioni, sulla programmazione a livello di sistema e sull'integrazione tra piattaforme diverse; l'attitudine alla diagnosi e alla risoluzione dei problemi è richiesta per dare supporto su sistemi proprietari o aperti e su configurazioni ibride.

**(20) Supervisore di un Centro di Assistenza (Help Desk Supervisor).** Un supervisore di un centro di assistenza secondo lo standard EUCIP deve essere efficace nel fornire supporto tecnico; ciò richiede competenza di una tecnologia specifica (legata al contesto, es. servizi in rete), ma anche dimestichezza con contratti SLA, consapevolezza delle priorità operative nell'attività del cliente e delle problematiche tipiche degli utenti, così come un atteggiamento positivo nel reagire ai problemi e nel rapportarsi con il cliente.

**(21) Formatore IT (IT Trainer).** Un formatore IT secondo lo standard EUCIP deve essere molto efficace nel comunicare concetti IT, nell'addestrare gli utenti e nel motivarli a utilizzare al meglio i sistemi IT; tra i requisiti figurano un'ampia cultura ICT, una specializzazione su una particolare tecnologia (legata al contesto, es. prodotti IT per la collaborazione),

Numero d'Oggetto/Part Number	Ed./Issue	Data/Date	Com. Mod./Ch. Notice	2.3.1 CFD CERTIFICAZIONE DELLA FIRMA DIGITALE
MANUALE 4	2.0	19.05.2008	---	

un'eccellente capacità di esposizione e la padronanza delle tecniche didattiche, comprensive della progettazione e preparazione di materiale efficace.

**(22) Amministratore di Sistemi Informatici (IT Administrator).** Un amministratore di sistemi informatici secondo lo standard EUCIP deve saper gestire efficacemente l'infrastruttura IT, tipicamente basata su LAN di PC, di una unità organizzativa di piccole dimensioni (piccola azienda o ufficio decentrato di una grande organizzazione). A competenze generali su hardware del PC, sistemi operativi, reti e sicurezza informatica abbina capacità di supporto degli utenti, gestione dei malfunzionamenti, amministrazione del sistema locale.

---

Numero d'Oggetto/Part Number	Ed./Issue	Data/Date	Com. Mod./Ch. Notice	2.3.1 CFD CERTIFICAZIONE DELLA FIRMA DIGITALE
MANUALE 4	2.0	19.05.2008	---	

**7 INDICATORI/MISURE DI QUALITÀ**

In questo paragrafo sono definiti gli indicatori atti a descrivere i livelli di qualità della fornitura. La tabella Attività / Prodotti / Indicatori associa ad ogni attività e/o prodotto della fornitura gli indicatori di pertinenza descritti nelle schede successive.

**Tabella 1. Attività / Prodotti / Indicatori**

Attività	Prodotto	Indicatore di qualità				Processo trasversale		
		Caratteristica	Sottocaratt.	acro IQ	Denominazione IQ	cod PT	acro PT	Denominazione PT
Gestione Operativa	Certificato Emesso	Efficienza	Efficienza temporale	TEC	Tempo di emissione del certificato			
Gestione Operativa	Certificato Rinnovato	Efficienza	Efficienza temporale	TER	Tempo di rinnovo del certificato			
Gestione Operativa	Certificato Sospeso	Efficienza	Efficienza temporale	TSC	Tempo di sospensione di un certificato			
Gestione Operativa	Certificato Revocato	Efficienza	Efficienza temporale	TRCE	Tempo di revoca di un certificato			

<b>Classe di fornitura</b>	CERTIFICAZIONE DELLA FIRMA DIGITALE
<b>Caratteristica /Sottocaratteristica</b>	Efficienza / efficienza temporale
<b>Indicatore/Misura</b>	Tempo di emissione del certificato – <b>TEC</b>
<b>Sistema di gestione delle misure</b>	Diario di Bordo
<b>Metodi e strumenti di misura</b>	Si misura per ciascun certificato, il tempo intercorrente tra la sua richiesta (accettata dal Certificatore) e le sua emissione. La finestra temporale da considerare è dal lunedì al venerdì, esclusi festivi, dalle 8.00 alle 17.00
<b>Unità di misura</b>	Percentuale.
<b>Dati elementari da rilevare</b>	<ul style="list-style-type: none"> <li>• Numero dei certificati emessi nel periodo di osservazione</li> <li>• Data di accettazione, ovvero data in cui il Certificatore accetta la richiesta del Titolare (il Certificatore può respingere la richiesta entro il limite temporale indicato nel Manuale Operativo. In caso di rifiuto, fornisce adeguata motivazione).</li> <li>• Data di emissione del certificato</li> </ul>
<b>Periodo di riferimento</b>	6 mesi
<b>Frequenza esecuzione misure</b>	Le misure vengono effettuate come minimo 4 volte l'anno
<b>Regole di campionamento</b>	Le misure sono effettuate sul complesso degli elementi prodotti. Si prendono pertanto in considerazione i certificati richiesti ed emessi nel periodo di riferimento
<b>Formula di calcolo</b>	<p>Dati necessari:</p> <ul style="list-style-type: none"> <li>• N.E.: numero di certificati emessi entro i tempi dichiarati (nel periodo di osservazione)</li> <li>• N.R.: numero totale di certificati richiesti ed approvati (nel periodo di osservazione)</li> </ul> $TEC = \frac{N.E.}{N.R.} \times 100$
<b>Regole di arrotondamento</b>	<p>TEC va arrotondato alla frazione di punto percentuale sulla base del primo decimale:</p> <ul style="list-style-type: none"> <li>• al punto % per difetto se la parte decimale è ≤ 0,5</li> <li>• al punto % per eccesso se la parte decimale è &gt; 0,5</li> </ul>
<b>Obiettivi, (valori soglia)</b>	<p>Valori soglia:</p> <ul style="list-style-type: none"> <li>• Tempo massimo di emissione / rinnovo = 20 giorni</li> <li>• <b>TEC ≥ 95%</b></li> </ul>
<b>Azioni contrattuali</b>	<ul style="list-style-type: none"> <li>▪ Dal 94% al 90%, per ogni punto % in meno si applica una penale di importo pari allo 0,5% del corrispettivo del servizio relativo al periodo di osservazione.</li> <li>▪ Dall'89% in giù, per ogni punto % in meno si applica una penale di importo pari all'1% del corrispettivo del servizio relativo al periodo di osservazione..</li> </ul>
<b>Eccezioni</b>	L'applicazione delle regole contrattuali inizia dopo un periodo di osservazione dall'avvio del servizio della durata di 3 mesi

<b>Classe di fornitura</b>	CERTIFICAZIONE DELLA FIRMA DIGITALE
<b>Caratteristica /Sottocaratteristica</b>	Efficienza / efficienza temporale
<b>Indicatore/Misura</b>	Tempo di rinnovo del certificato – <b>TER</b>
<b>Sistema di gestione delle misure</b>	Diario di Bordo
<b>Metodi e strumenti di misura</b>	Si misura per ciascun certificato, il tempo intercorrente tra la sua richiesta (accettata dal Certificatore) e le sua emissione. La finestra temporale da considerare è dal lunedì al venerdì, esclusi festivi, dalle 8.00 alle 17.00
<b>Unità di misura</b>	Percentuale.
<b>Dati elementari da rilevare</b>	<ul style="list-style-type: none"> <li>• Numero dei certificati rinnovati nel periodo di osservazione</li> <li>• Data di accettazione, ovvero data in cui il Certificatore accetta la richiesta del Titolare (il Certificatore può respingere la richiesta entro il limite temporale indicato nel Manuale Operativo. In caso di rifiuto, fornisce adeguata motivazione).</li> <li>• Data di emissione del certificato</li> </ul>
<b>Periodo di riferimento</b>	6 mesi
<b>Frequenza esecuzione misure</b>	Le misure vengono effettuate come minimo 4 volte l'anno
<b>Regole di campionamento</b>	Le misure sono effettuate sul complesso degli elementi prodotti. Si prendono pertanto in considerazione i certificati richiesti ed emessi nel periodo di riferimento
<b>Formula di calcolo</b>	<p>Dati necessari:</p> <ul style="list-style-type: none"> <li>• N.Rin.: numero di certificati rinnovati entro i tempi dichiarati (nel periodo di osservazione)</li> <li>• N.Ric.: numero totale di certificati richiesti ed approvati entro i tempi dichiarati (nel periodo di osservazione)</li> </ul> $TER = \frac{N.Rin.}{N.Ric.} \times 100$
<b>Regole di arrotondamento</b>	<p><b>TER</b> va arrotondato alla frazione di punto percentuale sulla base del primo decimale:</p> <ul style="list-style-type: none"> <li>• al punto % per difetto se la parte decimale è ≤ 0,5</li> <li>• al punto % per eccesso se la parte decimale è &gt; 0,5</li> </ul>
<b>Obiettivi, (valori soglia)</b>	<p>Valori soglia:</p> <ul style="list-style-type: none"> <li>• Tempo massimo di emissione/rinnovo = 15 giorni</li> <li>• <b>TER</b> ≥ 95%</li> </ul>
<b>Azioni contrattuali</b>	<ul style="list-style-type: none"> <li>▪ Dal 94% al 90%, per ogni punto % in meno si applica una penale di importo pari allo 0,5% del corrispettivo del servizio relativo al periodo di osservazione.</li> <li>▪ Dall'89% in giù, per ogni punto % in meno si applica una penale di importo pari all'1% del corrispettivo del servizio relativo al periodo di osservazione.</li> </ul>
<b>Eccezioni</b>	L'applicazione delle regole contrattuali inizia dopo un periodo di osservazione dall'avvio del servizio della durata di 3 mesi

<b>Classe di fornitura</b>	CERTIFICAZIONE DELLA FIRMA DIGITALE
<b>Caratteristica /Sottocaratteristica</b>	Efficienza / efficienza temporale
<b>Indicatore/Misura</b>	Tempo di revoca del certificato – <b>TRCE</b>
<b>Sistema di gestione delle misure</b>	Diario di Bordo
<b>Metodi e strumenti di misura</b>	Si misura per ciascun certificato, il tempo intercorrente tra la richiesta di revoca (accettata dal Certificatore) e le sua effettiva revoca La finestra temporale da considerare è dal lunedì al venerdì, esclusi festivi, dalle 8.00 alle 17.00
<b>Unità di misura</b>	Percentuale.
<b>Dati elementari da rilevare</b>	<ul style="list-style-type: none"> <li>• Numero dei certificati revocati nel periodo di osservazione</li> <li>• Data di accettazione, ovvero data in cui il Certificatore accetta la richiesta di revoca del Titolare (il Certificatore può respingere la richiesta entro il limite temporale indicato nel Manuale Operativo. In caso di rifiuto, fornisce adeguata motivazione).</li> <li>• Data di revoca del certificato (è indicata come data di emissione della CRL)</li> </ul>
<b>Periodo di riferimento</b>	6 mesi
<b>Frequenza esecuzione misure</b>	4 volte l'anno
<b>Regole di campionamento</b>	Si prendono in considerazione i certificati revocati nel periodo di riferimento
<b>Formula di calcolo</b>	<p>Dati necessari:</p> <ul style="list-style-type: none"> <li>• N.R.R.: numero di richieste di revoca pervenute (nel periodo di osservazione)</li> <li>• N.C.R.: numero totale di certificati revocati entro i tempi dichiarati (nel periodo di osservazione)</li> </ul> $TRCE = \frac{N.C.R.}{N.R.R.} \times 100$
<b>Regole di arrotondamento</b>	<p><b>TRCE</b> va arrotondato alla frazione di punto percentuale sulla base del primo decimale:</p> <ul style="list-style-type: none"> <li>• al punto % per difetto se la parte decimale è ≤ 0,5</li> <li>• al punto % per eccesso se la parte decimale è &gt; 0,5</li> </ul>
<b>Obiettivi, (valori soglia)</b>	<p>Valori soglia:</p> <ul style="list-style-type: none"> <li>• Tempo massimo di revoca = 48 ore</li> <li>• <b>TRCE</b> = 98%</li> </ul>
<b>Azioni contrattuali</b>	<p>:</p> <ul style="list-style-type: none"> <li>▪ <b>Dal 97% al 90%</b>, per ogni punto % in meno si applica una penale di importo pari allo 0,5% del corrispettivo del servizio relativo al periodo di osservazione.</li> <li>▪ <b>Dall'89% in giù</b>, per ogni punto % in meno si applica una penale di importo pari all'1% del corrispettivo del servizio relativo al periodo di osservazione.</li> </ul>
<b>Eccezioni</b>	L'applicazione delle <b>regole contrattuali</b> inizia dopo un <b>periodo di osservazione</b> dall'avvio del servizio della durata di 3 mesi

<b>Classe di fornitura</b>	CERTIFICAZIONE DELLA FIRMA DIGITALE
<b>Caratteristica /Sottocaratteristica</b>	Efficienza / efficienza temporale
<b>Indicatore/Misura</b>	Tempo di sospensione del certificato – <b>TSC</b>
<b>Sistema di gestione delle misure</b>	Diario di Bordo
<b>Metodi e strumenti di misura</b>	Si misura per ciascun certificato, il tempo intercorrente tra la richiesta di sospensione (accettata dal Certificatore) e le sua effettiva sospensione. Il servizio è operativo H24
<b>Unità di misura</b>	Percentuale.
<b>Dati elementari da rilevare</b>	<ul style="list-style-type: none"> <li>• Conteggio dei certificati sospesi nel periodo di osservazione</li> <li>• Data di accettazione, ovvero data in cui il Certificatore accetta la richiesta di sospensione del Titolare (il Certificatore può respingere la richiesta entro il limite temporale indicato nel Manuale Operativo. In caso di rifiuto, fornisce adeguata motivazione).</li> <li>• Data di sospensione del certificato (è indicata come data di emissione della CSL)</li> </ul>
<b>Periodo di riferimento</b>	6 mesi
<b>Frequenza esecuzione misure</b>	4 volte l'anno
<b>Regole di campionamento</b>	Si prendono in considerazione i certificati sospesi nel periodo di riferimento
<b>Formula di calcolo</b>	Dati necessari: <ul style="list-style-type: none"> <li>• N.R.S.: numero di richieste di sospensione pervenute (nel periodo di osservazione)</li> <li>• N.C.S.: numero totale di certificati sospesi entro i tempi dichiarati (nel periodo di osservazione)</li> </ul> $TSC = \frac{N.C.S.}{N.R.S.} \times 100$
<b>Regole di arrotondamento</b>	<b>TSC</b> va arrotondato alla frazione di punto percentuale sulla base del primo decimale: <ul style="list-style-type: none"> <li>• al punto % per difetto se la parte decimale è ≤ 0,5</li> <li>• al punto % per eccesso se la parte decimale è &gt; 0,5</li> </ul>
<b>Obiettivi, (valori soglia)</b>	Valori soglia: <ul style="list-style-type: none"> <li>• Tempo massimo di sospensione = 60 minuti</li> <li>• TSC ≥ 99%</li> </ul>
<b>Azioni contrattuali</b>	<ul style="list-style-type: none"> <li>▪ Dal 99% al 90%, per ogni punto % in meno si applica una penale di importo pari allo 0,5% del corrispettivo del servizio relativo al periodo di osservazione.</li> <li>▪ Dall'89% in giù, per ogni punto % in meno si applica una penale di importo pari all'1% del corrispettivo del servizio relativo al periodo di osservazione.</li> </ul>
<b>Eccezioni</b>	L'applicazione delle regole contrattuali inizia dopo un periodo di osservazione dall'avvio del servizio della durata di 3 mesi

## 8 GLOSSARIO

**CERTIFICATI ELETTRONICI:** attestati elettronici che collegano i dati utilizzati per verificare le firme elettroniche ai titolari e confermano l'identità dei titolari stessi;

**CERTIFICATI QUALIFICATI:** certificati elettronici conformi ai requisiti di cui all'allegato I della direttiva n. 1999/93/CE, rilasciati da certificatori che rispondono ai requisiti di cui all'allegato II della medesima direttiva;

**CERTIFICATORE:** soggetto che presta servizi di certificazione delle firme elettroniche o che fornisce altri servizi connessi con queste ultime;

**CERTIFICATORE QUALIFICATO:** certificatore che rilascia al pubblico certificati elettronici conformi ai requisiti indicati nella normativa sulla documentazione amministrativa e nelle relative regole tecniche;

**CERTIFICATORE ACCREDITATO:** certificatore accreditato in Italia ovvero in altri Stati membri dell'Unione europea ai sensi della normativa comunitaria e della normativa sulla documentazione amministrativa;

**CHIAVI ASIMMETRICHE:** coppia di chiavi crittografiche, una privata ed una pubblica, correlate tra loro, utilizzate nell'ambito dei sistemi di validazione di documenti informatici;

**CHIAVE PRIVATA:** elemento della coppia di chiavi asimmetriche, destinato ad essere conosciuto soltanto dal soggetto titolare, mediante il quale si appone la firma digitale sul documento informatico;

**CHIAVE PUBBLICA:** elemento della coppia di chiavi asimmetriche destinato ad essere reso pubblico, con il quale si verifica la firma digitale apposta sul documento informatico dal titolare delle chiavi asimmetriche;

**DOCUMENTO DI RICONOSCIMENTO:** ogni documento munito di fotografia del titolare e rilasciato, su supporto cartaceo, magnetico o informatico, da una pubblica Amministrazione italiana o di altri Stati, che consenta l'identificazione personale del titolare;

**DOCUMENTO D'IDENTITÀ:** carta d'identità ed ogni altro documento munito di fotografia del titolare e rilasciato, su supporto cartaceo, magnetico o informatico, da una pubblica Amministrazione competente dello Stato italiano o di altri Stati, con la finalità prevalente di dimostrare l'identità personale del suo titolare;

**DOCUMENTO INFORMATICO:** rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti;

**FIRMA DIGITALE:** é un particolare tipo di firma elettronica qualificata basata su un sistema di chiavi asimmetriche a coppia, una pubblica e una privata, 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 ELETTRONICA:** insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di autenticazione informatica;

**FIRMA ELETTRONICA AVANZATA:** firma elettronica ottenuta attraverso una procedura informatica che garantisce la connessione univoca al firmatario e la sua univoca identificazione, 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;

**FIRMA ELETTRONICA QUALIFICATA:** firma elettronica avanzata che sia basata su un certificato qualificato e creata mediante un dispositivo sicuro per la creazione della firma;

Numero d'Oggetto/Part Number	Ed./Issue	Data/Date	Com. Mod./Ch. Notice	2.3.1 CFD CERTIFICAZIONE DELLA FIRMA DIGITALE
MANUALE 4	2.0	19.05.2008	---	

**DISPOSITIVO DI VERIFICA DELLA FIRMA:** programma informatico (software) adeguatamente configurato o apparato strumentale (hardware) usati per effettuare la verifica della firma elettronica;

**DISPOSITIVO PER LA CREAZIONE DELLA FIRMA:** programma informatico adeguatamente configurato (software) o l'apparato strumentale (hardware) usati per la creazione della firma elettronica;

**DISPOSITIVO SICURO PER LA CREAZIONE DELLA FIRMA:** apparato strumentale usato per la creazione della firma elettronica, rispondente ai requisiti della vigente normativa in materia di documentazione amministrativa e firma digitale;

**TITOLARE:** persona fisica cui é attribuita la firma elettronica e che ha accesso al dispositivo per la creazione della firma elettronica;

**VALIDITÀ DEL CERTIFICATO ELETTRONICO:** efficacia e opponibilità al titolare dei dati in esso contenuti;

**VALIDAZIONE TEMPORALE:** risultato della procedura informatica, con cui si attribuiscono, ad uno o più documenti informatici, una data ed un orario opponibili ai terzi.

---

Numero d'Oggetto/Part Number	Ed./Issue	Data/Date	Com. Mod./Ch. Notice	
MANUALE 4	2.0	19.05.2008	---	2.3.1 CFD CERTIFICAZIONE DELLA FIRMA DIGITALE