

## **Sistema Cartografico di Riferimento**

### **SICUREZZA NELLA DISTRIBUZIONE DELLA CARTOGRAFIA DIGITALE**

#### **Studio di Fattibilità**

## Indice

1	Sezione prima – La situazione attuale.....	3
1.1	Il contesto dello studio .....	3
1.2	Descrizione della problematica.....	4
1.2.1	La gestione dei servizi.....	4
1.2.2	La certificazione del buon esito delle transazioni.....	5
1.2.3	La certificazione dei prodotti forniti .....	5
1.2.4	Identificazione dei soggetti destinatari e dei loro diritti .....	7
1.2.4.1	Obiettivi .....	7
1.2.4.2	Aspetti applicativi e problematiche.....	7
1.2.5	Certificazione e riconoscibilità dei prodotti forniti.....	11
1.2.5.1	Obiettivi .....	11
1.2.5.2	Aspetti applicativi e problematiche.....	12
1.2.6	Certificazione del buon fine delle transazioni.....	13
1.2.6.1	Obiettivi .....	13
1.2.6.2	Aspetti applicativi e problematiche.....	13
1.3	Tipologie di utenti.....	14
2	Sezione seconda – Progetto di massima della soluzione .....	15
2.1	Caratteristiche del prodotto cartografico certificato .....	15
2.2	Caratteristiche generali .....	16
2.2.1	Soggetti destinatari e loro diritti.....	16
2.2.2	Certificazione e riconoscibilità .....	19
2.2.3	Buon fine delle transazioni .....	25
2.3	Dettaglio dei processi coinvolti.....	31
2.3.1	Identificazione utenti.....	31
2.3.2	Processi per la gestione della firma digitale.....	33
2.3.3	Procedure di verifica .....	34
2.3.4	Processi per il trasferimento dei dati cartografici .....	35
2.3.5	Sistemi di Pagamento.....	36
3	Sezione terza - Raccomandazioni per le fasi realizzative .....	41
3.1	Riepilogo degli elementi utili alla stesura del capitolato .....	41
3.2	Aspetti Economici.....	42
3.2.1	Identificazione Utenti.....	42
3.2.2	Sistemi Trasferimento Dati .....	43
3.2.3	Procedura Firma Digitale .....	43
3.2.4	Procedura Pagamento.....	44

# 1 Sezione prima – La situazione attuale

## 1.1 Il contesto dello studio

Lo studio di fattibilità sulla *Sicurezza nella distribuzione della cartografia digitale*, è parte di un più ampio insieme di studi progettuali finalizzati alla realizzazione di un *Sistema Cartografico di Riferimento* a livello regionale, costituito da un archivio informatizzato sulla cartografia, le foto aeree ed i database cartografici esistenti, consultabile in rete. Il materiale disponibile sarà classificato e caratterizzato attraverso informazioni (metadati) utili agli utenti per valutare l'utilizzabilità dei dati rispetto alle proprie specifiche esigenze.

Il repertorio cartografico potrà comprendere informazioni relative all'intero territorio nazionale, prodotte sia dagli Enti Centrali della Pubblica Amministrazione, sia dagli Enti Regionali, Sub-regionali e Provinciali.

Tale repertorio cartografico si rivolge a tutti coloro, in particolare amministratori responsabili della gestione del territorio, che necessitano di un quadro conoscitivo sulla esistenza, disponibilità e contenuto degli strumenti cartografici.

Si rivolge inoltre ad aziende, professionisti ed altri utenti privati che abbiano la necessità di accedere ai dati cartografici ed eventualmente di rielaborarli secondo le proprie specifiche finalità.

Il repertorio prevede diversi livelli di "certificazione" dei dati:

- dati ufficiali;
- dati la cui qualità sia stata in qualche misura sottoposta a verifica;
- dati dei quali è nota solo la disponibilità, senza che sia stato ancora possibile operarvi un controllo di qualità.

La struttura di metadati associati sarà tale da assicurare una corretta gestione di questi livelli di certificazione e da permettere a tutti gli utenti di identificare le informazioni di loro interesse ed essere allo stesso tempo correttamente informati sui limiti di applicabilità di ciascun dato.

La gestione dell'archivio cartografico, della relativa struttura informatica, dei servizi rivolti agli utenti esterni e interni verrà svolta, per ciascun ente regionale, da una struttura che chiameremo nel seguito "Centro Servizi".

## 1.2 Descrizione della problematica

Gli utenti, siano essi enti pubblici o studi privati, accederanno ai servizi di cartografia principalmente (anche se non esclusivamente) attraverso un sito Web che sarà dotato di programmi applicativi in grado di interagire con l'utente e di gestire la maggior parte delle richieste senza interventi da parte del personale del Centro Servizi.

Nel seguito verranno analizzati gli aspetti riguardanti:

- 1) la gestione degli utenti e delle loro richieste;
- 2) l'invio di materiale cartografico in forma digitalizzata e la certificazione dell'avvenuto ricevimento;
- 3) i meccanismi atti a rendere sempre distinguibile il materiale originale inviato dal Centro Servizi da sue copie modificate dagli utenti.

### 1.2.1 La gestione dei servizi

Il Centro Servizi erogherà tramite il proprio sito due tipologie di servizi:

- servizi e informazioni pubbliche, disponibili a chiunque si colleghi (ad es. informazioni sui servizi disponibili, informazioni istituzionali);
- servizi e informazioni che richiedono una preventiva registrazione (ad es. richiesta di cartografia in formato digitale).

Alcuni servizi saranno gratuiti, altri potranno essere a pagamento con fasce di prezzo differenziate per tipologia di utente ( attualmente servizi simili forniti da altri Enti quali la Regione Toscana, prevedono tre fasce di prezzo: pieno, ridotto e gratuito a seconda che il cliente sia uno studio privato, un ente convenzionato o un ente pubblico).

Inoltre alcune tipologie di dati saranno disponibili soltanto per determinate categorie di utenti: ad esempio, dati cartografici non ancora definitivamente validati e integrati potrebbero essere disponibili per gli enti pubblici ma non per soggetti privati.

Per poter trattare questi aspetti, tra le funzionalità del sito Web dovrà essere inclusa una gestione degli utenti che permetta la loro classificazione e associazione a delle tipologie contrattuali che specificheranno i diritti di accesso ai differenti servizi, e per ciascuno le modalità di pagamento.

Naturalmente il sistema di gestione degli utenti potrà comprendere molte altre funzionalità, come ad esempio la gestione dell'iter delle richieste fino al buon esito delle stesse, e la capacità di inviare automaticamente al sistema di fatturazione le informazioni necessarie.

I programmi del Centro Servizi dovranno includere:

- una procedura automatica di registrazione dei nuovi utenti comprensiva della notifica dell'avvenuta accettazione, che potrà essere inviata immediatamente o in un momento successivo se, ad esempio, il Centro Servizi debba verificare l'applicabilità di particolari condizioni contrattuali;
- identificazione dell'utente registrato e la sua autenticazione per l'accesso a quei servizi che lo richiedono.

### **1.2.2 La certificazione del buon esito delle transazioni**

Quando l'utente richiede l'invio di materiale cartografico, l'iter della richiesta si conclude ad avvenuta ricezione di quanto ordinato. A questo punto il Centro Servizi può autorizzare la fatturazione.

Quando l'invio viene effettuato tramite supporti informatici fisici (CD, DVD,...), il sistema di fornitura dei prodotti agli utenti può basarsi sui tradizionali strumenti messi a disposizione dai servizi postali che garantiscono il mittente dell'avvenuta ricezione da parte del destinatario per mezzo di una semplice *ricevuta di ritorno*.

Quando l'invio avviene in rete e gestito in modo automatico dai programmi del sito, è necessario che le modalità di trasmissione che permettano al Centro Servizi di ricevere e conseguentemente gestire una notifica automatica del buon fine della transazione.

### **1.2.3 La certificazione dei prodotti forniti**

La cartografia in formato digitale viene in generale richiesta per produrne successivamente copie e per elaborarle tramite sistemi GIS. Un ente pubblico, ad esempio potrà eseguire uno studio per il nuovo piano regolatore, riportando sulla cartografia ricevuta nuovi insediamenti, tracciati di nuove strade, modifiche alle reti di servizi quali canali, reti di distribuzione di gas e acqua, energia elettrica. A sua volta l'ente appalterà parte delle attività a studi professionali fornendo loro sia file cartografici conformi all'originale ricevuto dal Centro Servizi, sia files modificati.

Il singolo file cartografico potrà quindi subire diversi passaggi attraverso enti, studi professionali, aziende fornitrici di beni e servizi. In ognuno di questi passaggi potranno essere prodotte copie conformi all'originale e copie modificate.

Acquista importanza fondamentale sia per il Centro Servizi sia per il singolo utente la possibilità di riconoscere in ogni momento una copia come conforme all'originale distinguendola da quelle che hanno subito modifiche.

Tali operazioni di verifica dovranno poter essere attuate in qualsiasi momento da parte di qualsiasi utente (primo destinatario o successivo ricevente), ed indipendentemente dalla sua tipologia di appartenenza (utente pubblico o privato, con rapporti frequenti con il Centro Servizi o occasionale).

Dalle analisi fatte non si reputa necessaria, e di conseguenza non viene analizzata nel seguito, la possibilità di individuare, sulla base di una qualsiasi copia conforme, anche il primo destinatario cui il Centro Servizi abbia inviato la cartografia.

Avere escluso questa necessità permette, come verrà meglio spiegato nel seguito, di semplificare le procedure per rendere i prodotti identificabili. Il prodotto cartografico può essere realizzato, integrato con le informazioni per la sua identificazione e certificazione e archiviato nel database del sito corredato dei suoi metadati, una volta per tutte.

Il successivo invio ai richiedenti non comporta ulteriori operazioni sul prodotto.

Le problematiche precedentemente descritte:

- Identificazione dei soggetti destinatari e dei loro diritti
- Certificazione e riconoscibilità dei prodotti forniti
- Certificazione del buon fine delle transazioni

saranno approfondite nella *Sezione Prima*, ai Paragrafi 1.2.1 (*"Identificazione dei soggetti destinatari e dei loro diritti"*), 1.2.2 (*"Certificazione e riconoscibilità dei prodotti forniti"*) e 1.2.3 (*"Certificazione del buon fine delle transazioni"*).

Nella *Sezione Seconda* verranno indicate e caratterizzate le soluzioni proposte; la *Sezione Terza* contiene il riepilogo degli elementi utili alla stesura del capitolato.

## **1.2.4 Identificazione dei soggetti destinatari e dei loro diritti**

### **1.2.4.1 Obiettivi**

Per tutti i servizi offerti, ad eccezione di informazioni generali disponibili a tutti e di informazioni istituzionali, è necessario poter identificare il richiedente allo scopo di:

- selezionare i servizi e le informazioni a cui può accedere;
- determinare il costo del servizio e le modalità di pagamento;
- avere la possibilità di tracciare le transazioni effettuate in relazione, ad esempio, ad elementi quali:
  - soggetto destinatario
  - tipologia di contratto (in termini di tariffe e modalità di pagamento)
  - data della transazione e ogni altra informazione atta ad identificarla
  - oggetto della transazione
  - iter della richiesta (data di invio, avvenuta ricezione, avvenuto pagamento,..)

### **1.2.4.2 Aspetti applicativi e problematiche**

Il Centro Servizi interagirà con gli utenti (enti pubblici, enti privati, aziende e professionisti) tramite un sito Web con modalità che permetteranno di automatizzare in larga parte le procedure e la gestione delle richieste.

In questa prospettiva il sito dovrà includere i seguenti servizi:

- La definizione dei diritti e delle condizioni da applicare attraverso la gestione interna di strutture informative assimilabili a contratti. Questa modalità assicura un livello di flessibilità, di semplicità operativa e di completezza che compensa il maggior sforzo implementativo iniziale ed è quindi consigliabile rispetto a una casistica rigida definita nel codice di gestione, anche se ad oggi le variabilità non appaiono rilevanti.

Una gestione dei contratti dovrà includere i seguenti aspetti:

- La predisposizione da parte dei programmi di gestione del sito ad operare riconoscendo eventi correlati a voci contrattuali e conseguentemente gestire vincoli nell'accesso alle informazioni ed inoltre raccogliere i dati per le successive fasi di fatturazione.  
E' bene che la granularità degli eventi trattati sia abbastanza alta, in modo tale da rendere poco probabile la necessità di intervenire successivamente sul codice a fronte di nuove esigenze. A questo scopo è bene che le condizioni da controllare vengano tabulate in modo che nuove situazioni comportino l'aggiornamento di tabelle e non interventi sul codice.

A titolo esemplificativo:

ad ogni categoria di informazioni all'interno della struttura dei metadati è associata una prima tipologia che determina sotto quali condizioni contrattuali può essere fornita e una seconda tipologia che determina il tipo di sconto che può essere applicato rispetto a quello di listino. A loro volta le singole voci che caratterizzano le due tipologie sono tabulate per un facile aggiornamento.

Altre condizioni contrattuali possono determinare come sono erogati i servizi (ad es. invio via rete, invio tramite supporti quali CD o DVD, invio su canali particolari).

La definizione del contratto può essere estesa ad aspetti tipicamente amministrativi se questi non sono già coperti da altri servizi (ad es. modalità di pagamento).

Un tipo di contratto è costituito dall'elenco delle condizioni applicabili che a loro volta determinano sia come i singoli servizi vengono presentati nella fase in cui l'utente interroga il sito, sia come il sistema raccoglie automaticamente le informazioni che determinano le modalità di erogazione dei servizi e le voci di fatturazione.

- Le funzioni che permettano al personale del Centro Servizi di definire un contratto come insieme dei diritti associati, delle modalità di fatturazione e delle altre condizioni previste;
- le funzioni che permettano al personale del Centro Servizi di associare un contratto a uno specifico utente.
- La gestione di un database atto a contenere:
  - tutte le informazioni relative agli utenti necessarie per la loro gestione;
  - per ciascun utente le condizioni contrattuali applicate;
  - una gestione degli iter relativi alle operazioni svolte per soddisfare le diverse richieste.
- L'invio dei dati raccolti verso il sistema di fatturazione o più in generale verso i sottosistemi gestionali.
- La possibilità per tutte tipologie di utenti (Pubblici, privati, singoli soggetti occasionali) di registrarsi attraverso le pagine Web del sito con una procedura eventualmente differenziata di validazione e accettazione della registrazione, che dovrà permettere al Centro Servizi di verificare l'identità dei richiedenti, per esempio nel caso di enti pubblici o privati che possano accedere a livelli di servizio particolare o che godano di facilitazioni di pagamento;

- L'invio agli utenti registrati dei certificati (*user name e password*) che consentono l'accesso ai servizi, sia a fronte della prima registrazione, sia in caso di smarrimento;
- Una politica di gestione dei certificati ai fini della sicurezza.

## **Aspetti connessi alla tutela della riservatezza nel trattamento dei dati personali**

Il Centro Servizi dovrà gestire un archivio Clienti contenente dati personali e, di conseguenza, dovrà procedere al trattamento di tali dati in conformità alla normativa nazionale ed europea in materia di riservatezza dei dati personali.

Le informazioni personali che verranno raccolte avranno lo scopo di permettere l'identificazione degli interlocutori del Centro Servizi in quanto alla loro identità personale (*nome, cognome, indirizzo, indirizzo di posta elettronica,...*); eventualmente, potranno essere raccolti e conservati ulteriori dati necessari per la gestione delle procedure di fatturazione.

Questi dati appartengono alla categoria dei dati personali *così detti comuni*. Tale categoria è dedotta dalla lettera della legge stessa che, nel definire il *dato sensibile* \*, identifica come residuale il *dato comune*.

Ad essi si applicano le norme previste per il trattamento di *dati personali comuni* effettuati con l'ausilio di strumenti elettronici o comunque automatizzati (DPR 318/1999), mentre risulta non pertinente l'applicazione delle norme relative al trattamento dei dati personali di tipo *sensibile* (art. 22 e 24, legge 675/1996).

Il quadro normativo di riferimento è rappresentato in particolare dalla Legge 675/1996 sulla "Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali", dal DPR 318/1999, "Regolamento recante norme per l'individuazione delle misure minime di sicurezza per il trattamento dei dati personali" e dalla recente Raccomandazione delle Autorità per la protezione dei dati personali dell'Unione Europea in materia di "Raccolta di dati personali on line" (Raccomandazione del 17 Maggio 2001).

L'applicazione delle norme citate comporta l'osservanza delle disposizioni in materia di:

**Adempimenti documentali:** previsti allo scopo di realizzare un rapporto di comunicazione corretto con gli utenti e l'Autorità Garante per la protezione dei dati personali. Rientra in questa tipologia di adempimenti anche la documentazione inerente alla nomina delle figure interne di riferimento coinvolte nei processi di trattamento.

**Misure di sicurezza:** predisposte a protezione dell'integrità, disponibilità, riservatezza dei dati personali degli utenti e applicate secondo il modello indicato dalle norme in materia di dati raccolti on line e trattati con strumenti informatici.

**Organizzazione:** caratterizzata dalla definizione di una corretta gestione delle procedure interne e dalla distribuzione di responsabilità ed incarichi attribuiti alle figure interne coinvolte nei processi di trattamento. Un'organizzazione normativamente conforme deve essere prevista sia per assicurare una gestione puntuale delle richieste di esercizio dei diritti da parte degli utenti, sia per garantire l'esito favorevole delle eventuali attività di audit disposte dall'Autorità Garante.

\* NOTA: Legge 675/1996, Capo IV, art.22, comma 1 – Dati sensibili: "I dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale, possono essere oggetto di trattamento solo con il consenso scritto dell'interessato e previa autorizzazione del Garante".

## **1.2.5 Certificazione e riconoscibilità dei prodotti forniti**

### **1.2.5.1 Obiettivi**

Tutti i prodotti informatici (file cartografici digitalizzati) che possono essere resi disponibili agli utenti dovranno essere strutturati in modo tale che sia possibile a chiunque riconoscere se è in possesso di una copia non modificata dell'originale.

Il metodo adottato dovrà permettere a chiunque di fare copie del materiale acquisito e di modificarlo secondo le proprie esigenze.

La certificazione dovrà consentire al Centro Servizi di verificare l'autenticità di un prodotto, anche a fini probatori, rendendolo così opponibile, in caso di contestazione, sia nei confronti del referente originario sia nei confronti dei terzi.

Non rientra tra gli obiettivi dello studio l'individuazione di sistemi in grado di impedire la duplicazione dei documenti cartografici forniti dal Centro Servizi, né sistemi che impediscano di modificarli.

Infatti, una delle finalità principali perseguite dal Progetto di distribuzione della cartografia digitale, è quello di rendere tali documenti accessibili ed utilizzabili all'utenza che ne faccia richiesta. Spesso la cartografia viene richiesta in forma digitalizzata proprio per poterla successivamente rielaborare. Impedirne la duplicazione e la modifica potrebbe in molti casi rendere inutile la loro acquisizione.

In ogni caso, un esplicito divieto di duplicazione, modifica, alterazione o diffusione dei documenti di cartografia digitale acquisiti dall'utente, potrà essere previsto a livello contrattuale.

### 1.2.5.2 Aspetti applicativi e problematiche

Nella valutazione delle possibili soluzioni al problema della certificazione e riconoscibilità dei prodotti forniti dovranno essere considerati i seguenti aspetti:

- osservare quanto indicato nelle deliberazioni AIPA che, per quanto pertinente, vengono richiamate nei capitoli successivi, in modo che la soluzione possa essere inquadrata nel più generale contesto degli indirizzi della Autorità per l'Informatica nella Pubblica Amministrazione;
- impostare una soluzione che, ove si renda necessario, sia riconosciuta a fini probatori;
- minimizzare l'impegno gestionale del Centro Servizi nel processo di fornitura, rendendo in larga parte automatizzati:
  - l'identificazione del richiedente;
  - il reperimento e l'invio di quanto richiesto in una forma certificata e riconoscibile;
  - la produzione di una notifica di conferma dell'avvenuta consegna.

Tali processi dovranno potersi svolgere automaticamente senza la necessità di un intervento umano.

- Permettere al richiedente di ricevere un file cartografico su cui possa operare immediatamente, senza la necessità di attivare preventivamente un processo di verifica della sua autenticità.  
Dovrà comunque essere garantita all'utente la facoltà di procedere alla verifica in ogni momento successivo;
- consentire a ciascun soggetto destinatario di documenti di cartografia di applicare la procedura di verifica su ciascuna delle eventuali copie.

## **1.2.6 Certificazione del buon fine delle transazioni**

### **1.2.6.1 Obiettivi**

Allo scopo di fornire al Centro Servizi la garanzia del buon fine delle transazioni, a seguito delle quali attivare le fasi successive alla consegna al richiedente del materiale cartografico (*fatturazione, registrazione dell'avvenuta consegna, sia a scopi amministrativi sia per la gestione di successive richieste o contestazioni*), il sistema dovrà prevedere un procedimento di notifica automatica che l'utente abbia ricevuto quanto richiesto.

Questo aspetto assume particolare rilevanza quando l'invio del materiale avviene tramite Internet, soluzione questa che, pur non essendo l'unica possibile, si presenta come la più frequente per le sue caratteristiche di maggiore semplicità.

Tale soluzione, se opportunamente supportata dalle funzioni applicative del sito Web, non richiede l'intervento dell'operatore e quindi minimizza i costi di gestione del Centro Servizi.

### **1.2.6.2 Aspetti applicativi e problematiche**

Un processo di invio ed acquisizione dei files di cartografia che utilizzi Internet quale ambiente di trasmissione, dovrà soddisfare i requisiti sopra indicati indipendentemente dalle dimensioni dei files trasferiti, che può essere dell'ordine di decine di megabytes.

Tale caratteristica dei file di cartografia suggerisce l'utilizzo di strumenti in grado di supportare il trasferimento di files di grandi dimensioni e capaci di gestire automaticamente eventuali interruzioni ed il successivo completamento della trasmissione.

La semplicità di utilizzo e il maggior grado di automatizzazione dell'operazione di notifica dell'avvenuto trasferimento, saranno ulteriori requisiti che lo strumento selezionato dovrà soddisfare.

### 1.3 Tipologie di utenti

Per quanto si riferisce agli obiettivi che sono oggetto di questo documento possiamo suddividere gli utenti in due categorie:

- “*utenti istituzionali*” e “*grandi utenti*” che accedono con frequenza ai servizi del Sistema Cartografico; tale tipologia è costituita da soggetti che potrebbero dotarsi di strumenti informatici specifici e definire al proprio interno procedure particolari per interagire con il Centro Servizi;
- “*piccoli utenti*” e “*utenti occasionali*” che potrebbero incontrare difficoltà a dotarsi preventivamente di strumenti informatici *ad hoc* e ad attivare specifiche procedure, anche se non particolarmente complesse.

Quest'ultima tipologia di utenti suggerisce la scelta di soluzioni semplici e che facciano uso di metodi e strumenti “standard”.

Si è evitato inoltre di proporre modalità operative e tecniche diverse per le due categorie di utenti sia per una semplicità generare della soluzione, sia perché non si sono evidenziati particolari vantaggi nell'adottare soluzioni *ad hoc* per gli enti pubblici e le grandi aziende che in ogni caso comporterebbero un progetto più complesso con costi più alti di realizzazione delle procedure applicative che gestiranno il sito.

Questo non esclude che utenti istituzionali che abbiano ad esempio già in atto modalità di connessione particolari con il Centro Servizi possano concordare modalità di trasmissione dei file cartografici e procedure di certificazione del buon esito delle transazioni diverse da quelle indicate nel presente documento.

Anche se esula dagli obiettivi di questo studio, è importante rilevare che esiste una terza categoria di utenti di cui tenere conto nella progettazione del sito, costituita dal personale del Centro Servizi.

Questi ultimi utilizzeranno le funzioni del sito per svolgere specifiche attività di amministrazione e gestione, ma anche per svolgere delle operazioni al posto e per conto dell'utente. Tutti i controlli e le azioni che il sistema svolge quando interrogato direttamente dall'utente finale dovranno essere eseguiti anche quando viene sostituito da un operatore del Centro. Se il sistema genererà per ciascun utente un iter delle richieste è bene che venga registrato l'intervento dell'operatore.

## 2 Sezione seconda – Progetto di massima della soluzione

### 2.1 Caratteristiche del prodotto cartografico certificato

Per soddisfare le esigenze di certificazione e riconoscibilità dei prodotti evidenziate nella *Sezione prima*, il Centro archiverà e distribuirà un prodotto cartografico costituito dai seguenti oggetti:

1. file di cartografia
2. impronta crittografata
3. Certificato della chiave pubblica del Centro Servizi

Il complesso di tali oggetti costituisce il documento informatico certificato con firma digitale, come verrà illustrato nel successivo paragrafo 2.2.2 “*Certificazione e riconoscibilità*”.

I primi due elementi indicati, il file e la sua impronta, costituiscono il vero e proprio documento autenticato. Il terzo elemento, il Certificato di firma digitale, viene incluso quale parte integrante del prodotto cartografico in quanto permette di semplificare le operazioni di verifica di autenticità del file da parte del ricevente (v. *Paragrafo 2.2.2 “Certificazione e riconoscibilità – Il procedimento di verifica”*).

L'utente, ricevuto il prodotto potrà operare direttamente sul file di cartografia ignorando gli altri oggetti, poiché quest'ultimo non è crittografato.

Chiunque invece produca una copia del prodotto ricevuto, se vorrà poter certificare e garantire la sua autenticità, dovrà riprodurre tutti e tre gli oggetti, il cui insieme costituisce la “copia conforme”.

La firma del file cartografico è un'operazione “delicata” non tanto per la sua complessità tecnica, perché basta eseguire un programma, ma perché richiede di fare uso della chiave privata del Centro Servizi che deve essere assolutamente mantenuta segreta.

Poiché il singolo prodotto non viene personalizzato sul richiedente (vedi *Paragrafo 1.2.3*) l'operazione di firma e di composizione del prodotto cartografico viene eseguita solo una volta. Quest'ultimo viene archiviato nel database del sito, classificato e corredato dei metadati che lo caratterizzano e può essere inviato automaticamente al richiedente, senza ulteriori manipolazioni.

## 2.2 Caratteristiche generali

### 2.2.1 Soggetti destinatari e loro diritti

#### Premessa

Il sito si presenterà al pubblico sostanzialmente suddiviso in due aree:

- un'area pubblica ai cui servizi e informazioni chiunque potrà accedere;
- un'area riservata a cui si potranno accedere solo utenti registrati nel sistema

L'utilizzo del tradizionale sistema di identificazione tramite User-Id e Password è il più adatto per accedere a servizi in rete. Tramite lo User-Id il sistema di gestione del sito è grado di riconoscere l'utente e di accedere a tutte le informazioni che lo riguardano, tramite la password il sistema può verificare se l'utente è abilitato ad accedere ai servizi.

La gestione degli utenti e dei loro diritti dovrà fare parte integrante dell'insieme di prodotti e servizi software che costituiranno il sito. Nel seguito vengono richiamati i punti essenziali che dovranno essere presi in considerazione nella fase di progettazione.

#### Modalità operative

La realizzazione di un sistema di gestione degli utenti e dei diritti comporta le seguenti modalità operative:

##### Il Centro Servizi:

- definisce e cataloga nel sistema le forme contrattuali che determinano i servizi disponibili, il prezzo, le forme di pagamento. Le diverse tipologie di contratto (o parte di esse) possono essere pubblicate sul sito perché l'utente possa scegliere la propria;
- quando un nuovo utente si registra, gli viene associato un contratto. Questa operazione può essere completamente automatica per utenti che si registrano tramite il sito e scelgano un tipo di contratto che non richieda particolari controlli sull'identità del richiedente (ad es. perché prevedono il prezzo pieno o servizi di tipo generale). Negli altri casi deve intervenire il personale del Centro Servizi per concordare la forma contrattuale da applicare .

##### L'utente:

- si registra la prima volta tramite il sito Web attraverso la compilazione dei campi di un apposito modulo. Tra i dati obbligatori c'è l'indirizzo di e-mail che verrà usato per ogni comunicazione e la forma contrattuale da applicare.
- il sistema assegna un codice identificativo univoco e personale, costituito da *user-id* e *password*. La comunicazione all'utente avviene tramite un messaggio di posta elettronica;
- consulta il sito e accede all'area riservata dando il proprio identificativo (*user-id* e *password*).

### Il sistema:

- gestisce per ogni utente un ITER delle richieste, tracciando tutte le azioni che, automaticamente o per scelta dell'operatore, vengono eseguite per suo conto;
- interagisce con le componenti gestionali, inviando ad esempio i dati di fatturazione secondo quanto previsto dal contratto.

### **Specifiche tecniche**

La concreta realizzazione dei diversi servizi dipenderà dall'architettura generale del sistema. Si possono ipotizzare soluzioni anche molto diverse ma equivalenti. In ogni caso, a livello logico possiamo identificare i seguenti sottosistemi:

- Sottosistema di gestione dei contratti comprendente un archivio informatizzato e i servizi di amministrazione, direttamente gestito dal personale del Centro Servizi.
- Sottosistema di gestione degli utenti comprendente il database degli utenti con l'associazione con i relativi contratti, gli iter delle richieste, i dati personali necessari.

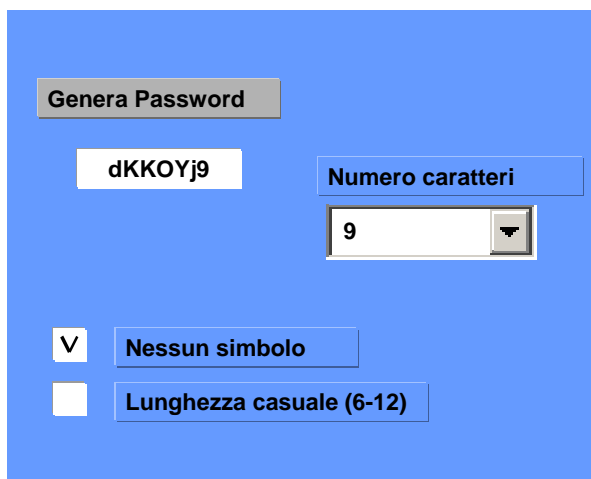
Questo sottosistema offre servizi sia al personale del Centro Servizi sia all'utente collegato al sito

- Sottosistema operativo che include tutti i servizi che possono essere attivati nella gestione di una richiesta dell'utente, incluso l'invio dei prodotti di cartografia e la conseguente gestione della conferma del buon esito delle transazioni, ognuno dei quali dovrà poter verificare le modalità operative imposte dalla forma contrattuale in essere e aggiornare l'iter relativo

Relativamente alla gestione delle password possiamo svolgere qualche considerazione: la password determina se l'utente ha o no accesso ai servizi. Essa deve rimanere segreta e un estraneo non deve poterla facilmente ricavare. La gravità del rischio che una password venga conosciuta da chi non ne ha diritto dipende da che cosa può concretamente fare l'estraneo, ma in ogni caso può accedere a dati personali dell'utente che devono essere garantiti e mantenuti riservati dalla già citata legge sulla privacy. E' importante quindi che le procedure di generazione della password offrano il massimo livello di sicurezza.

A questo scopo non dovrebbe essere l'utente a sceglierla (potrebbe scegliere delle combinazioni facili da ricavare), ma il sistema a fornirla e a gestire inoltre una politica di scadenze temporali, eventualmente diverse per tipologia di utente.

Un ulteriore livello di sicurezza si ha se il Centro Servizi dota di un programma di generazione automatica di password. Tali programmi producono parole d'accesso, in modo casuale, attraverso la combinazione di diversi criteri predefiniti e tramite l'applicazione di un algoritmo. Il programma genererà la password in conformità a criteri di sicurezza, quali il numero dei caratteri della parola d'accesso e le caratteristiche della sua composizione (simboli e caratteri alfanumerici).



**Fig. 1 – Esempio di interfaccia di programma di generazione password**

Per garantire la generazione di una password particolarmente sicura la cui individuazione ad opera di terzi sia particolarmente difficile si adotta normalmente la così detta “*strong password*” basata sulle seguenti caratteristiche:

- contiene un numero di caratteri superiore a 5 ed inferiore a 9;
- contiene almeno due caratteri alfabetici e almeno un carattere numerico o un carattere speciale (caratteri di punteggiatura o simboli);
- non contiene né si basa su elaborazioni di dati anagrafici dell’utente (nome e cognome o loro iniziali, altri dati personali o altrimenti ricollegabili al soggetto);
- non corrisponde a termini di lingua italiana o straniera contenuti nei dizionari di lingua.

Il Centro Servizi dovrà inoltre predisporre un adeguato sistema di assistenza agli utenti che abbiano smarrito o dimenticato la propria parola d’accesso.

Una possibile procedura che non richiede l’intervento del personale del centro è la seguente: all’atto della prima registrazione l’utente introduce nel sistema una domanda e una risposta di carattere “riservato” che solo lui possa conoscere (ad esempio il titolo di un libro, la data di un particolare episodio, etc..). Nel caso di smarrimento della password, l’utente, dopo essersi identificato dando il proprio user name, risponde alla domanda e il sistema invia la password via e-mail.

## 2.2.2 Certificazione e riconoscibilità

### Premesse

La certificazione e riconoscibilità dei prodotti erogati viene garantita con l'adozione di uno strumento atto a certificare la provenienza del documento digitale trasferito (*autenticità*), nonché la sua non alterazione durante la fase di trasferimento e fino alla fase di acquisizione da parte del destinatario (*integrità*).

Attraverso le procedure di certificazione del materiale cartografico, l'utente destinatario dovrà essere in grado di verificare in modo certo che la documentazione ricevuta proviene dalla fonte dichiarata.

Allo stesso modo, la procedura di certificazione dovrà permettere al Centro Servizi di riconoscere e dimostrare l'autenticità del documento digitale, quale prodotto autentico ed integro inviato all'utente destinatario, distinguendolo da copie modificate.

Nell'ipotesi di contestazioni rispetto alla paternità ed integrità del documento, il Centro Servizi dovrà poter utilizzare le garanzie offerte dalla procedura di certificazione allo scopo di confermare, o eventualmente negare, la sua originalità.

Dovrà essere inoltre considerata l'opportunità di progettare una procedura di risposta alle istanze di verifica provenienti da terzi, originariamente estranei al rapporto con il Centro Servizi.

### Modalità operative

Attualmente esiste una vasta gamma di tecnologie, strumenti ed applicazioni idonei a garantire i requisiti di autenticità e integrità di documenti digitali trasmessi con modalità automatiche.

Il più adatto, che risponde a tutti i requisiti ed è riconosciuto dalla normativa vigente si basa sull'impiego della firma digitale a chiavi asimmetriche, in grado di conferire al documento cartografico i fondamentali requisiti di *integrità*, *paternità*, *riservatezza* e *non ripudio*.

### Specifiche

La procedura di **apposizione della firma digitale** su un documento consiste nella applicazione al testo di una funzione di *hash* che genererà l'*impronta* del documento. La funzione di hash è in grado di ottenere una sequenza di bit di lunghezza fissa, qualunque sia la dimensione del file originario. La modifica di un singolo bit in un file anche di considerevoli dimensioni comporterà la generazione di una impronta nettamente differente da quella originaria. Infatti, la corrispondenza tra l'impronta e il file originario è quasi assolutamente univoca, considerato che per ottenere un'impronta identica da un documento differente, anche se solo di un bit, è necessario procedere ad un numero di tentativi concretamente irrealizzabili.

Questa caratteristica del sistema di certificazione con firma digitale consente di garantire, oltre alla *paternità* del documento, anche l'*integrità* del documento stesso, ovvero di assicurare che esso non sia stato modificato e non abbia subito alterazioni.

Pertanto, un file di cartografia a cui corrisponda una determinata impronta non potrà in alcun modo venir contraffatto o manipolato senza che la nuova impronta che si verrebbe a produrre sia palesemente diversa da quella originaria.

La firma digitale vera e propria viene prodotta attraverso la crittografia dell'impronta del file con la chiave privata; dall'applicazione della chiave privata all'impronta del documento digitale si ottiene la firma digitale certificata.

Il documento al quale verrà applicata la firma digitale non verrà crittografato, conservando così il suo aspetto "in chiaro", la sua intelligibilità, e potrà essere immediatamente utilizzato e rielaborato dal destinatario.

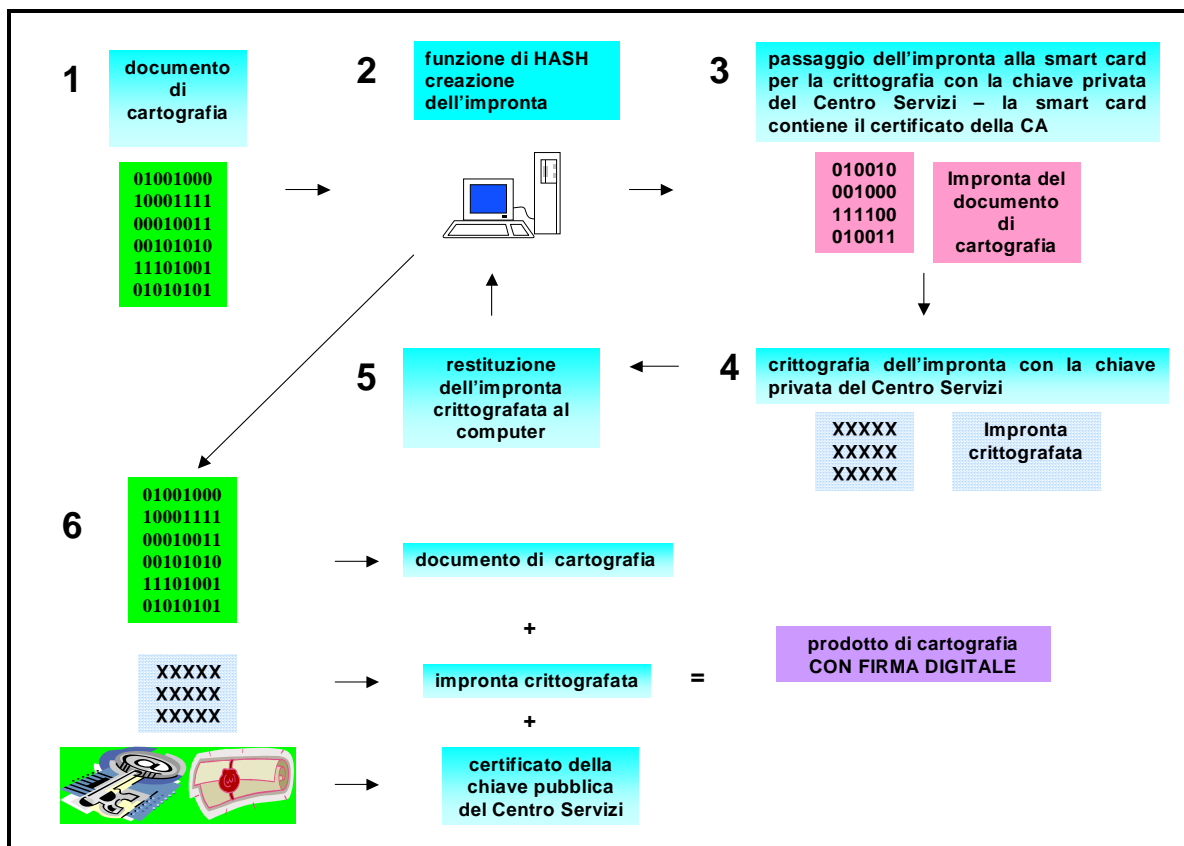


Fig. 2 - Processo di creazione ed apposizione di firma digitale su un documento informatico

**Il procedimento di verifica** circa l'originalità del documento è di semplice esecuzione: il destinatario del file dovrà applicare alla firma digitale del mittente la chiave pubblica del sottoscrittore, ottenendo in tal modo l'impronta del documento. La corrispondenza tra l'impronta originaria e l'impronta calcolata tramite la procedura di verifica garantisce la genuinità e l'integrità del documento sotto ogni profilo.

Essendo necessario conoscere la chiave pubblica del mittente per poter procedere alla suddetta verifica, è opportuno allegare al file inviato anche il certificato di firma digitale che contiene l'indicazione della chiave pubblica stessa nonché la denominazione dell'Ente Certificatore che ha emesso il certificato, oltre ad altri elementi identificativi del titolare del certificato stesso, nella fattispecie il Centro Servizi.

Consultando il Registro dei certificati dell'Ente Certificatore, il destinatario potrà verificare che il certificato di chiave pubblica, allegato al documento ricevuto, sia efficace, non sottoposto a sospensione né a revoca.

In ogni caso gli elenchi delle chiavi pubbliche sono disponibili e consultabili on line presso i siti Web di ciascuno degli Enti Certificatori.

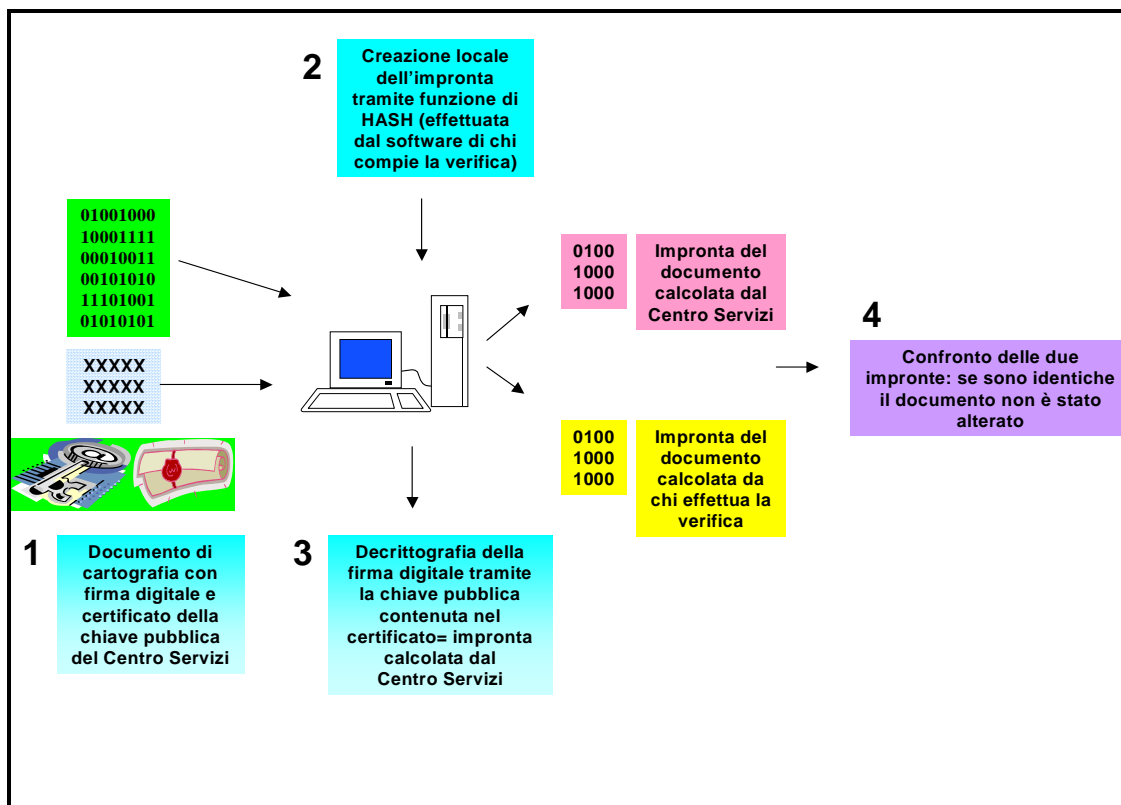


Fig. 3 – Processo di verifica di un documento firmato digitalmente (integrità)

Il servizio di verifica viene offerto dagli stessi Enti Certificatori: generalmente il processo di verifica è applicabile esclusivamente rispetto a firme e certificati di firma digitale emessi dall'Ente stesso.

In alcuni casi (  *cfr. Infocamere – Ente Certificatore – [www.infocamere.it](http://www.infocamere.it)* ) gli Enti Certificatori offrono un servizio di verifica della firma digitale eseguibile direttamente presso il proprio sito Web. In una apposita sezione del sito il soggetto che intenda effettuare la verifica potrà sottoporre il file all'analisi semplicemente selezionandolo: un programma presente nel sistema del Certificatore valuterà l'integrità e l'autenticità della firma digitale dandone comunicazione all'utente del servizio tramite la visualizzazione di un messaggio.

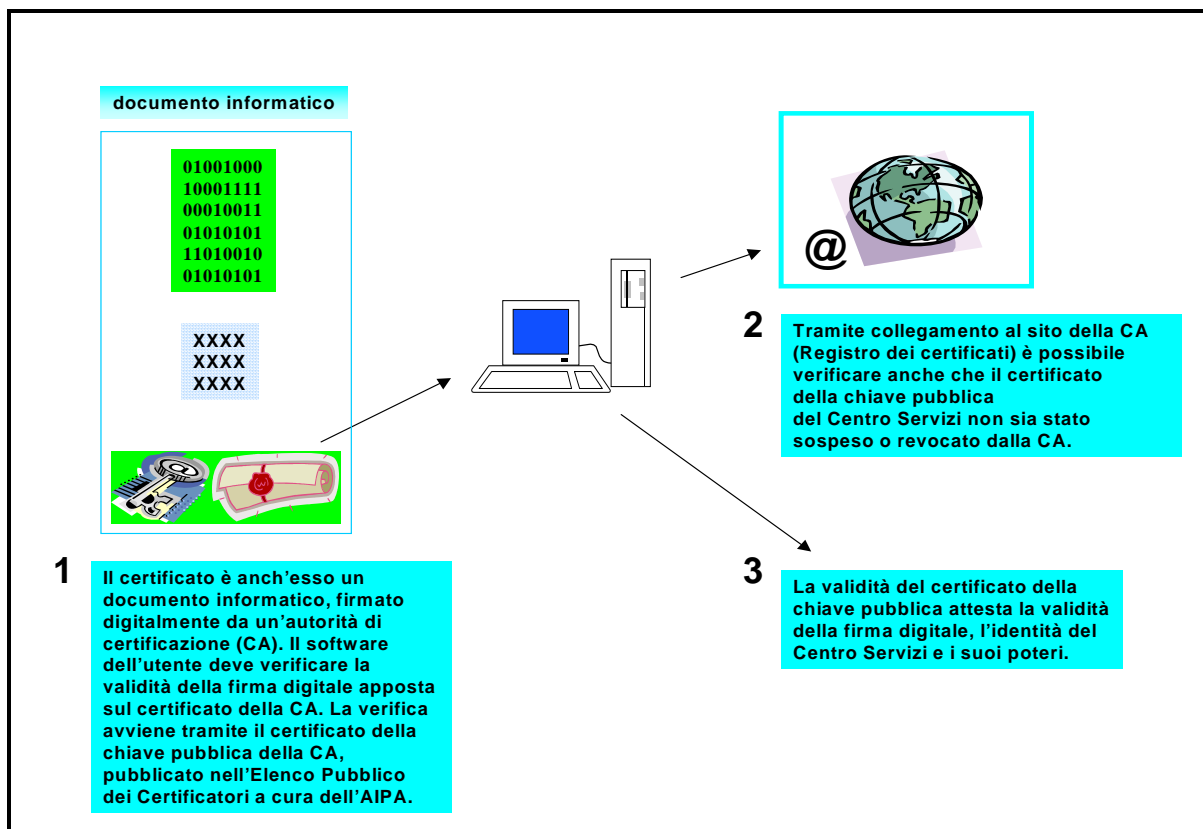
Una procedura alternativa di verifica offerta da tutti gli Enti Certificatori consente di eseguire l'operazione di controllo *in locale*, presso il sistema dell'utente.

Ciò avviene tramite la previa acquisizione da parte dell'utente dell'apposito *programma di verifica* (ad es. "*Dike*", programma offerto da *Infocamere*) da conservare nel proprio sistema; l'acquisizione del programma è gratuita, di estrema semplicità e rapidità.

Le firme digitali valide ai sensi di legge possono essere rilasciate esclusivamente da Enti Certificatori (Certification Authorities – CA) autorizzati dall'Autorità per l'Informatica nella Pubblica Amministrazione (AIPA).

L'Ente Certificatore fornirà al Centro Servizi il *kit* di prodotti per l'operatività delle procedure di apposizione e gestione della firma digitale. In particolare l'Ente Certificatore provvederà a dotare il Centro Servizi dei seguenti prodotti:

- smart card : ovvero il *dispositivo di firma* contenente il Certificato di chiave pubblica e la chiave privata; la smart card personalizzata è protetta da un codice PIN generato in modo casuale dall'Ente Certificatore e a conoscenza esclusivamente del Centro Servizi, quale Titolare del Certificato di firma digitale, e dell'Ente Certificatore che lo conserva in modo protetto nei propri sistemi;
- lettore di smart card: componente hardware in grado di effettuare la lettura delle informazioni contenute nella smart card interfacciato dal software di firma;
- software di firma: è il software necessario alla gestione dell'ambiente locale di firma digitale, e consente di apporre e/o verificare una o più firme su qualunque tipo di file.



**Fig. 4 – Processo di verifica di un documento informatico firmato digitalmente (verifica del certificato di chiave pubblica)**

Per la procedura di firma digitale viene fatta una distinzione tra chiavi di sottoscrizione e chiavi di certificazione:

Chiavi di sottoscrizione

Le chiavi di sottoscrizione dell'utente sono generate dall'utente stesso, attivando con il software fornito dal Certificatore, il dispositivo di firma personalizzato.

L'accesso al dispositivo di firma è protetto da un codice riservato di accesso assegnato dall'utente. Questo codice di accesso deve essere digitato dal titolare del certificato ogni qualvolta egli intenda apporre una firma tramite l'uso del dispositivo.

Chiavi di certificazione

Le chiavi di certificazione sono generate dal Certificatore, in particolare per ciascuna coppia di chiavi di certificazione viene generato un certificato firmato con la chiave privata della coppia di chiavi.

### **Fonti normative**

L'introduzione di servizi basati su meccanismi di certificazione con **firma digitale** comporta l'applicazione della normativa vigente in materia:

Legge n. 59/1997 (*c.d. Legge Bassanini*);

DPR n. 513/1997 *“Regolamento recante criteri e modalità per la formazione, l'archiviazione e la trasmissione di documenti con strumenti informatici e telematici”*;

DPCM 8 febbraio 1999 *“Regole tecniche per la formazione, trasmissione, conservazione, duplicazione, riproduzione e la validazione dei documenti informatici”*;

DPR n. 318/1999 *“Misure minime di sicurezza”*;

DPR 445/2000 *“Testo Unico delle disposizioni Legislative e Regolamentari in materia di Documentazione Amministrativa”*.

### 2.2.3 Buon fine delle transazioni

#### Premesse

Per una corretta operatività della procedura di distribuzione di documenti cartografici in formato digitale acquistano particolare rilevanza le seguenti considerazioni:

- il Centro Servizi ha la necessità di ottenere la garanzia che l'operazione di trasferimento del prodotto cartografico si sia svolta correttamente e che quindi sia documentabile l'esito positivo dell'avvenuta transazione;
- è necessario che venga mantenuta traccia delle operazioni effettuate e che la gestione dell'archivio delle operazioni sia integrabile nella procedura applicativa o direttamente gestibile dal personale del Centro Servizi;
- i documenti cartografici solitamente raggiungono elevate dimensioni; ne consegue che il loro trasferimento all'utenza deve prevedere meccanismi di compressione dei dati;
- la trasmissione dei dati via posta elettronica, benchè costituisca uno dei sistemi più diffusi e di più immediato accesso, e nonostante offra funzioni di notifica di avvenuta ricezione a garanzia del buon esito del trasferimento dei files inviati in allegato, non è generalmente in grado di garantire l'invio di documenti di grandi dimensioni (nonostante la loro compressione), sia a causa della maggiore possibilità di caduta della connessione sia perchè alcune categorie di utenti potrebbero avere a disposizione uno spazio limitato presso il server di posta del fornitore di servizi (Internet Service Provider - ISP);
- il sistema di invio basato su servizi di posta elettronica, specialmente per utenti che dispongano di risorse di sistema limitate, non garantisce al Centro Servizi la comunicazione di avvenuta transazione con esito positivo fintantochè l'utente non acceda al servizio di posta e acquisisca i messaggi in arrivo; ne consegue che il materiale potrebbe restare in giacenza presso il Service Provider per un tempo indeterminato;
- l'invio dei documenti cartografici, per quanto possibile, dovrebbe avvenire utilizzando canali sicuri, senza che questo prerequisito debba imporre all'utenza di acquisire strumenti hardware e software specifici;
- gli strumenti utilizzati per la ricezione dei documenti cartografici dovrebbero far parte della dotazione standard dei sistemi normalmente in uso; in alternativa dovrebbero essere forniti direttamente dal sito del Centro Servizi;
- nonostante l'eterogeneità dell'utenza, la procedura di invio dei dati cartografici dovrà seguire regole univoche in modo da non richiedere un maggiore impegno del personale del Centro Servizi;
- se durante l'operazione di invio dei documenti la connessione dovesse interrompersi, è indispensabile prevedere un sistema di riattivazione automatica che prosegua l'operazione dall'esatto punto dell'interruzione.

## **Modalità operative**

Dall'esposizione delle precedenti premesse, sono ipotizzabili le seguenti soluzioni che verranno successivamente descritte in dettaglio :

- **invio dei dati tramite l'utilizzo della *posta elettronica***
- **invio dei dati con *download da Internet***
- **invio dei dati con modalità *file transfer***

Ognuna delle soluzioni sopra elencate è caratterizzata da vantaggi e svantaggi:

la posta elettronica è certamente uno degli strumenti di "comunicazione" attualmente più diffusi e alla portata di ogni tipologia di utente, dall'ente pubblico all'utente privato.

Il file cartografico può essere inserito in un messaggio di posta elettronica come allegato e il messaggio può essere inviato con la modalità *ricevuta di ritorno* per verificarne l'avvenuta ricezione.

Inviare i files di cartografia utilizzando questo strumento potrebbe dunque apparire la soluzione più semplice. D'altro canto è però necessario considerare alcuni aspetti non trascurabili:

- gli archivi di cartografia possono raggiungere dimensioni notevoli ed è quindi necessario comprimerli e creare un *file eseguibile* che comprenda le funzioni di decompressione;
- la comunicazione di avvenuta ricezione non fornisce alcun tipo di conferma sulla corretta trasmissione dei dati, e sull'integrità dei dati ricevuti;
- la funzionalità di *ricevuta di ritorno* non è gestibile per tutti gli utenti privati che utilizzano cassette di posta gratuite (Netscape, HotMail, etc.) tramite collegamenti a Internet;
- le caselle di posta spesso hanno capacità di ricezione limitate (3 o 5MB) e quindi non hanno la possibilità di memorizzare allegati di grandi dimensioni;
- il messaggio di posta elettronica può venire intercettato poichè viene trasmesso "in chiaro";
- alcuni client di posta elettronica memorizzano automaticamente l'indirizzo del mittente e quindi, se attaccati da un virus, potrebbero facilmente *infettare* anche il server del Centro Servizi;
- poichè il messaggio di *ricevuta di ritorno* è l'unico riscontro dell'avvenuta ricezione, è necessario prevedere un controllo continuo dei messaggi ricevuti dal Centro Servizi; questa verifica non può essere automatizzata se non in minima parte;
- spesso l'utente non accede quotidianamente alla casella di posta e quindi le verifiche indispensabili all'attivazione delle successive procedure non possono essere completate contestualmente all'invio, creando particolari problemi di gestione ed archiviazione delle operazioni svolte.

Esaminando i punti sopra elencati si può concludere che l'invio dei dati di cartografia tramite l'utilizzo della posta elettronica non soddisfa i requisiti richiesti.

La seconda possibilità, e cioè l'invio dei dati con download da Internet permette all'utente, dopo la connessione al sito WEB del Centro Servizi e successiva identificazione tramite user-id e password, di procedere con l'operazione di scarico dei dati selezionati senza ulteriori richieste da parte del Centro o operazioni da effettuare, eccetto per l'eventuale procedura di pagamento che verrà analizzata successivamente.

Ogni operazione di *download* viene registrata in un file di log facilmente accessibile e quindi la registrazione stessa fornisce conferma di avvenuto trasferimento con esito positivo.

Le dimensioni dei files di cartografia non costituiscono un ostacolo poichè è sufficiente che i supporti magnetici del sistema ricevente siano in grado di contenere i dati scaricati.

Alcune caratteristiche di questo sistema di trasferimento non forniscono però le garanzie richieste:

- il file in cui vengono registrate le operazioni di download è comune a tutta la struttura WEB server, cioè tiene traccia di ogni operazione effettuata dal server WEB, con conseguente difficoltà nel reperire i dati relativi alle sole operazioni di download per il singolo utente;
- nel caso in cui l'operazione di *download* dovesse interrompersi, in seguito alla caduta o al blocco della connessione, l'utente dovrà ripetere la procedura dall'inizio poichè non è prevista la funzionalità di restart automatico;
- il trasferimento tramite *download* può essere intercettato poichè i dati trasmessi non vengono crittati;
- considerate le notevoli dimensioni dei files di cartografia l'operazione di *download* può impegnare significativamente sia il sistema del Centro Servizi che il sistema richiedente. Inoltre i tempi di trasmissione possono divenire particolarmente lunghi. Compattare i dati prima dell'invio comporta la creazione di un file eseguibile che comprenda la funzionalità di decompressione una volta archiviato sul sistema ricevente, con conseguente ulteriore impegno, nella fase di preparazione del materiale cartografico, del personale del Centro Servizi.

Le considerazioni sopra descritte portano alla conclusione che il trasferimento dei dati cartografici tramite *download da Internet* non soddisfa pienamente i requisiti richiesti.

L'invio dei dati con modalità *file transfer* è reputato lo strumento adatto per meglio rispondere alle esigenze descritte. E' costituito da uno dei prodotti di trasferimento file - *file transfert* – facilmente reperibili sul mercato e di cui il Centro Servizi dovrà dotarsi. La procedura applicativa dovrà quindi comprendere opportunamente il "pacchetto" di file transfert che verrà attivato in modo automatico all'atto dell'invio del materiale cartografico.

Vantaggi della soluzione:

- compressione dei dati con relativo *risparmio sui tempi* di trasmissione ed impegno del sistema;

- trasmissione su *linea sicura*: il materiale inviato viene criptato durante la trasmissione e decriptato a destinazione;
- *comunicazione di avvenuta transazione* con esito positivo;
- *traccia di tutte le operazioni* di trasferimento dati raccolte in un file di log facilmente consultabile e gestibile sia direttamente dal personale del Centro Servizi sia integrabile nella procedura applicativa;
- *restart automatico* dal punto di interruzione in caso di caduta della connessione;
- *nessuna richiesta all'utente* destinatario tranne lo spazio disco necessario per l'archiviazione delle informazioni inviate.

Naturalmente, in alternativa alla modalità di file transfert, sarà sempre possibile procedere alla fornitura di prodotti cartografici tramite canali tradizionali:

- o il Centro Servizi dovrà organizzare, in caso di documenti di notevoli dimensioni o in risposta a specifiche esigenze dell'utente, l'invio del materiale a mezzo corriere autorizzato e/o servizio di posta ordinaria tramite raccomandata r.r.;
- o la ricevuta sottoscritta dall'utente al momento della consegna del materiale cartografico, assolverà lo scopo di garantire la notifica dell'avvenuta ricezione. Le ricevute sottoscritte dovranno essere archiviate e conservate. La procedura applicativa dovrà mantenere traccia anche delle consegne effettuate con strumenti di tipo non informatico.

### **Specifiche**

Una serie di prodotti attualmente disponibili, permettono il trasferimento di dati ed informazioni utilizzando le connessioni ad Internet e basandosi sulle peculiarità delle piattaforme Web.

Si tratta di moduli software strutturati in architettura *client/server*.

Il software della parte server viene installato e configurato sul sistema del Centro Servizi, costituendo il soggetto erogatore delle informazioni. Il software della parte client viene invece integrato nel sistema dell'utente che richiede il trasferimento dei dati.

Il meccanismo che permette all'utente di scaricare dal sito web del sistema server il modulo software necessario può essere gestito, a seconda del prodotto scelto, in modalità "*plug-in*" oppure tramite *applet Java*.

Nel primo caso (*plug-in*) il modulo software client è parte integrante del prodotto stesso e quindi verrà utilizzato solo per le funzioni relative alle attività di trasferimento dei dati, nel secondo caso (*applet java*) il software utilizza alcune funzioni specifiche di *Java Runtime Environment*, usate per le applicazioni Java che normalmente popolano i siti Web.

La trasmissione delle informazioni viene richiesta via Web dall'utente che attiva la procedura sul sistema server: questo a sua volta, interfacciandosi con il software client, dà inizio al trasferimento vero e proprio.

## Caratteristiche principali e comuni ai prodotti di file transfert presenti sul mercato

La gestione ed il controllo delle informazioni trasmesse sono essenziali per le organizzazioni che trasferiscono archivi critici utilizzando Internet.

I prerequisiti soddisfatti dai prodotti presi in esame includono:

- controllo centralizzato degli accessi e delle destinazioni;
- garanzia dell'avvenuto trasferimento;
- registrazione dei trasferimenti effettuati e del loro buon fine.

In caso di interruzione durante la trasmissione, il trasferimento può essere riattivato automaticamente dal punto di interruzione senza perdita di dati (*operazione di restart*).

Ciò acquista particolare rilevanza nel trasferimento di archivi di notevoli dimensioni attraverso canali a larghezza di banda ridotta e/o in assenza di canali dedicati.

L'operazione di *restart* prevede l'attivazione del trasferimento dal momento in cui è stato interrotto oppure dà la possibilità di iniziare interamente una nuova trasmissione dei dati.

L'accesso al server di file transfer è regolato in modo da poter attribuire ad ogni utente solo determinate facoltà: in questo modo è esclusa la possibilità che l'utente possa avere accesso a dati che gli siano preclusi.

Inoltre, questa funzionalità permette di attribuire ad utenti privilegiati facoltà aggiuntive, quali la determinazione di specifici parametri dei dati.

La sicurezza viene ulteriormente garantita poichè i dati vengono trasferiti in forma crittografata. Benchè il livello di protezione e riservatezza richiesto a tutela dei dati da trasferire non sia particolarmente elevato, è comunque opportuno privilegiare l'adozione di strumenti che, a parità di prestazioni e funzionalità, siano in grado di garantire il maggior grado di sicurezza possibile.

L'algoritmo di crittografia utilizzato è solitamente proprietario e quindi più difficile da riprodurre.

I prodotti in esame comprendono funzionalità di compressione dei dati da trasferire.

La compressione dei dati permette di ridurre significativamente i tempi di trasmissione e di conseguenza consente di ridurre le probabilità che si verifichino eventi in grado di influire sulla continuità del trasferimento.

Al termine della trasmissione, i dati verranno automaticamente decompressi ed archiviati in chiaro.

Le funzionalità di *accodamento* integrate nei prodotti maggiormente diffusi sul mercato, rappresentano una ulteriore caratteristica che permette di gestire in modo organizzato e sicuro la procedura di trasferimento.

Ad ogni utente è collegata una "coda" dedicata nella quale vengono inseriti, ad ogni richiesta, i documenti da inviare; il trasferimento effettivo avviene quindi prelevando i dati dalla coda specifica dell'utente senza mai coinvolgere le aree di archiviazione sul server che rimangono protette da possibili accessi non autorizzati.

Le code, inoltre, sono facilmente gestibili dagli operatori che amministrano la procedura di file transfer.

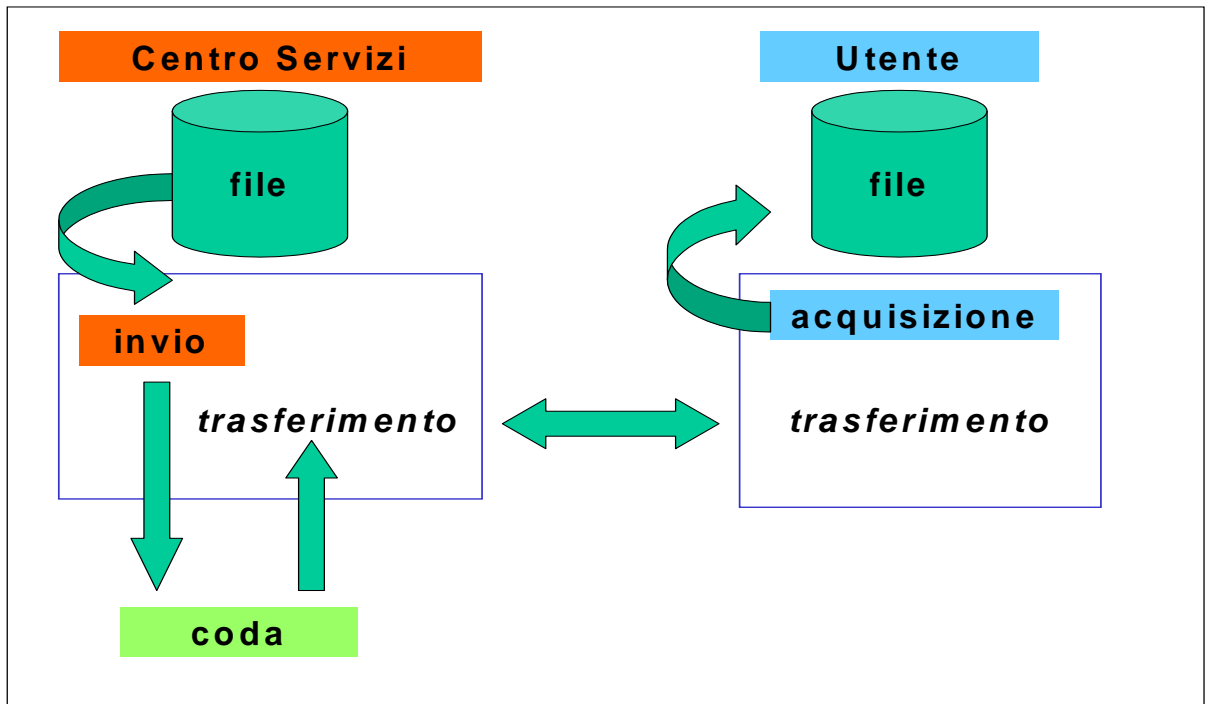


Fig. 5- Processo di trasmissione dei dati con modalità *file transfert*

## 2.3 Dettaglio dei processi coinvolti

### 2.3.1 Identificazione utenti

La procedura di identificazione ed autorizzazione consente di verificare l'identità dell'utente e di associare all'identificativo (user-id e password) i parametri che individuano i servizi erogabili e le caratteristiche di pagamento relative a ciascuna tipologia di utente.

All'atto del primo collegamento al sito Web del Centro Servizi (utente non registrato) viene attivata una procedura di registrazione che raccoglie le informazioni necessarie alla profilazione dell'utente. In questa fase viene generato un nuovo identificativo utente (user-id e password).

I processi di competenza del Centro Servizi sono riassunti nei seguenti punti:

- Utente al primo collegamento:
  - raccolta dati utente: tramite una opportuna maschera visualizzata vengono raccolti i dati necessari alla profilazione dell'utente, tra cui , obbligatorio, l'indirizzo di posta elettronica che verrà usato in tutte le successive comunicazioni;
  - autorizzazione al trattamento dei dati personali: visualizzazione dell'informativa e del modulo per il consenso al trattamento dei dati personali;
  - determinazione di un nuovo identificativo (user-id e password personale) attribuito all'utente;
  - invio all'utente di un messaggio di posta elettronica con l'indicazione dello user-id e della password assegnata.
  
- Utente noto (già registrato ed in possesso del proprio identificativo):
  - verifica automatica identificativo utente: visualizzazione dell'opportuna maschera che permetterà all'utente di introdurre il proprio identificativo (user-id e password);
  - autorizzazione a procedere con le operazioni consentite.

I processi di pertinenza dell'utente sono:

- Utente al primo collegamento:
  - collegamento al sito Web del Centro Servizi;
  - richiesta di registrazione;
  - introduzione dei dati richiesti e loro conferma;
  - consenso al trattamento dei dati personali;
  - acquisizione dell'identificativo - utente ricevuto tramite messaggio di posta elettronica.

- Utente noto (già registrato ed in possesso del proprio identificativo):
  - collegamento al sito Web del Centro Servizi;
  - inserimento nell'apposita maschera dell'identificativo personale.

### 2.3.2 Processi per la gestione della firma digitale

La procedura per l'acquisizione del certificato di firma digitale (cioè la facoltà di disporre di una propria firma digitale certificata) si articola nelle seguenti fasi:

- Richiesta del certificato;
- Generazione del certificato;
- Pubblicazione del certificato.

La richiesta e rilascio del certificato di firma digitale richiede che Centro Servizi si registri attraverso la seguente procedura:

- richiesta di registrazione rivolta alla CA (Certification Authority), qualificata da elementi che assicurino l'Ente Certificatore circa l'identità del richiedente;
- verifica della validità della richiesta ad opera della CA e attribuzione al Centro Servizi di un identificatore;
- inserimento dell'identificatore del Centro Servizi nei cataloghi della CA contenenti l'elenco degli utenti registrati;
- ricezione da parte del Centro Servizi della chiave crittografica da utilizzarsi per le richieste di certificazione delle chiavi e per effettuare l'accesso ai registri della CA.

Il Centro Servizi procederà quindi alla generazione di una coppia di chiavi: una di esse, detta *chiave privata*, verrà utilizzata per la generazione della firma e sarà mantenuta segreta; l'altra, detta *chiave pubblica*, sarà destinata alla verifica e verrà resa nota attraverso la sua pubblicazione.

La certificazione della chiave pubblica consta delle seguenti tre fasi:

- Il Centro Servizi invierà alla CA la richiesta di certificazione della chiave pubblica, autenticandola mediante la chiave fornita dalla CA durante il processo di registrazione;
- la CA genererà il certificato sottoscrivendolo, in modo da garantirne la provenienza che potrà essere accertata da chiunque con l'utilizzo della chiave pubblica della CA;
- il Centro Servizi riceverà il certificato di firma digitale.

### 2.3.3 Procedure di verifica

La procedura di verifica di un file di cartografia permette di controllare che il file ricevuto sia autentico (*originato effettivamente dal Centro Servizi*) ed integro (*non alterato né modificato*). Il processo di verifica prevede in primo luogo l'acquisizione da parte dell'utente del programma che consente di operare tali controlli (v. *Paragrafo 2.2.2 "Certificazione e riconoscibilità – Il procedimento di verifica"*). Il programma potrà essere reso disponibile agli utenti direttamente dal sito Web del Centro Servizi: una volta acquisito e salvato nel sistema locale, potrà essere conservato per ogni futura operazione di controllo.

Il prodotto cartografico che l'utente potrà sottoporre a verifica integra tutte le informazioni necessarie affinché il programma sia in grado di operare automaticamente (v. *Paragrafo 2.1 "Caratteristiche del prodotto cartografico certificato"*). Tali informazioni includono infatti sia il file cartografico, sia la firma digitale, ma anche il certificato rilasciato dalla CA contenente la chiave pubblica del Centro.

L'utente inoltre avrà sempre la possibilità di verificare la validità del certificato allegato al prodotto consultando il Registro dei Certificati della CA emittente.

Il programma di controllo è in grado di svolgere in modo completamente automatico le operazioni di verifica, che si articolano nelle seguenti fasi:

- rilevazione dell'impronta contenuta nel documento
- ricalcolo dell'impronta del documento
- operazione di raffronto delle due impronte

Attraverso tale procedura gli utenti saranno in grado di effettuare autonomamente le operazioni di controllo, indipendentemente da qualsiasi intervento degli operatori del Centro Servizi.

#### **NOTA:**

In ogni caso il Centro Servizi potrà istituire e gestire un *servizio di verifica* su richiesta degli utenti.

In questa ipotesi l'interessato invierà al Centro Servizi il prodotto cartografico richiedendone la verifica, ad esempio indirizzando al Centro un messaggio di posta elettronica.

Le istruzioni ed ogni altra indicazione sulle modalità di accesso alle procedure di verifica saranno indicate in una apposita sezione del sito Web.

Il Centro Servizi comunicherà successivamente al richiedente le risultanze dell'operazione di verifica dell'autenticità del file, attraverso la trasmissione di un messaggio di posta elettronica.

### 2.3.4 Processi per il trasferimento dei dati cartografici

Il trasferimento del prodotto di cartografia avrà luogo tramite un processo che si articola in una prima fase di acquisizione da parte dell'utente della parte *client* del programma di file transfer (v. *Paragrafo 2.2.3 "Buon fine delle transazioni – Invio dei dati con modalità file transfer"*), e in una successiva fase di trasmissione vera e propria.

A seguito di una precisa richiesta di materiale cartografico il Centro Servizi valuterà, in relazione alla tipologia dell'utente, alle caratteristiche e alle dimensioni del documento da inviare, quale metodo utilizzare per la spedizione del materiale: con modalità file transfer, oppure a mezzo corriere e/o posta ordinaria.

La trasmissione del prodotto cartografico potrà avvenire, in relazione alle diverse caratteristiche di pagamento, in invio "immediato" e "differito":

- in caso di invio *immediato* il prodotto costituito dal documento, dalla relativa firma digitale ed dal certificato di firma verranno inseriti nell'area di trasferimento dati (coda gestita dal prodotto di file transfer e corrispondente all'utente richiedente);
- in caso di invio *differito* verrà inviato all'utente un messaggio di posta elettronica che, oltre a confermare la transazione e ad indicare la data di disponibilità del materiale, conterrà un *URL* configurato con opportuni parametri. Alla data indicata, l'utente potrà attivare il trasferimento vero e proprio del materiale cartografico effettuando il collegamento all'*URL* precedentemente indicato.

E' buona norma che l'utente duplichi il materiale ricevuto e ne conservi copia.

Come già specificato in precedenza (v. *Paragrafo 2.2.3 "Buon fine delle transazioni - – Specifiche"*) il prodotto di file transfer si basa su una architettura client/server. E' necessario dunque che nel sistema dell'utente venga installato un modulo software in grado di colloquiare con la procedura server installata nel sistema del Centro Servizi.

L'utente potrà scaricare direttamente dal sito Web del Centro Servizi il software client del prodotto di file transfer. L'operazione, che verrà effettuata soltanto la prima volta, a meno di perdita del software o suo deterioramento, potrà essere attivata durante due diverse fasi:

- fase di registrazione dell'utente;
- prima richiesta di materiale e successivo trasferimento delle informazioni.

La procedura di acquisizione del software client segue un semplice percorso:

- durante la fase di registrazione, tramite un pulsante di plug-in, l'utente attiverà la procedura che copierà direttamente la componente client sul sistema dell'utente;
- durante la prima trasmissione di dati, l'utente dovrà in primo luogo acquisire, attraverso lo stesso procedimento sopra descritto, il modulo client del prodotto di file transfer e successivamente dare inizio alla trasmissione vera e propria.

### 2.3.5 Sistemi di Pagamento

L' esame delle procedure di pagamento per l'acquisto di prodotti attraverso Internet, ha portato alla selezione di alcune procedure, di seguito descritte in dettaglio. Esiste una vasta panoramica di metodi di pagamento on-line le cui caratteristiche garantiscono, a diversi livelli, sicurezza, affidabilità, riservatezza e rapidità delle transazioni riguardanti prodotti offerti via WEB.

#### Sistemi di pagamento off-line

Corrispondono alle modalità di pagamento cosiddette "tradizionali", tramite le quali le transazioni si svolgono con strumenti non telematici. Queste procedure di pagamento incontrano tuttora un alto grado di fiducia e familiarità presso il pubblico.

Gli strumenti in questione sono rappresentati dai pagamenti a mezzo:

- bonifico bancario
- conto corrente postale
- assegno
- contrassegno
- carta di credito

Nel caso specifico di pagamento con *carta di credito* l'invio da parte dell'utente del numero di carta di credito può avvenire con due diversi sistemi:

- *off-line*, che implica la trasmissione del numero della carta con metodologie tradizionali, ad esempio via posta, fax, oppure attraverso comunicazione telefonica;
- *on-line*, attraverso la stessa comunicazione via Internet, sia essa un messaggio di posta elettronica, sia l'invio di uno specifico modulo tramite WEB.

Con la prima modalità, pur configurandosi alcuni aspetti positivi ai fini dell'attività contrattuale (l'invio del numero della carta con modalità tradizionali consente sempre di acquisire elementi sufficienti ad individuare con maggiore sicurezza l'identità della controparte, permettendo quindi di scegliere se procedere o meno alla conclusione del contratto), sono preponderanti gli aspetti negativi rispetto alle modalità *via Internet*. Le caratteristiche che rendono meno adatti tali strumenti di pagamento sono costituite dalla *lentezza* della transazione, dai *costi* connessi e dal possibile utilizzo indebito del numero della carta da parte di personale non autorizzato.

Nel caso invece di invio del numero di carta tramite sistemi *on-line*, possono essere sfruttate le caratteristiche della connessione Internet (rapidità e bassi costi), pur aumentando i rischi: non soltanto per l'utente (rischio di intercettazione del numero di carta di credito), ma anche per il Centro stesso, in particolare nelle ipotesi in cui la carta di credito sia stata sottratta al proprietario, sia falsa, oppure con disponibilità finanziarie non sufficienti.

### **Sistemi di pagamento on-line**

Si tratta di sistemi di pagamento per via telematica che riguardano il pagamento attraverso un "intermediario elettronico", in modo da garantire la sicurezza e l'identità di chi acquista in rete.

L'acquirente, dopo essersi collegato al sito WEB del Centro Servizi, aver digitato il proprio identificativo utente (user-id e password), aver selezionato il materiale cartografico di suo interesse, vedrà visualizzato, nell'apposita pagina riepilogativa del sito del Centro Servizi, oltre all'indicazione del totale dell'ordine, anche un pulsante di conferma che oltre a svolgere la funzione di accettazione dell'ordine stesso ridirigerà l'acquirente alla pagina di pagamento residente su un server sicuro di un Istituto di Credito o Azienda di Servizi Bancari con i quali il Centro Servizi avrà stipulato apposito accordo.

La pagina di pagamento conterrà, in uno speciale modulo, la valuta e l'importo dell'acquisto, indicando il Centro Servizi quale beneficiario dell'accredito; l'acquirente dovrà selezionare il tipo di carta di credito usata per il pagamento, inserire il numero della carta, la data di emissione, la data di scadenza, il nome del titolare della carta (indicato sulla carta stessa) ed un indirizzo di posta elettronica. Per garantire un livello maggiore di sicurezza a favore degli utenti, i dati delle carte di credito non vengono memorizzati nei database del Centro Servizi.

L'inserimento di dati particolarmente riservati, quali il nominativo e il numero di carta di credito, avviene in modalità sicura poiché generalmente supportato da protocollo SET (*Secure Electronic Transaction*) o SSL (*Secure Socket Layer*) crittografia a 128 bit, a totale garanzia per l'acquirente.

I dati relativi alla transazione (dati della carta e importo) verranno raccolti ed inviati ai *circuiti autorizzativi internazionali* per le opportune verifiche (validazione della carta e capacità solutoria del soggetto titolare), con le stesse modalità correntemente utilizzate per il pagamento effettuato tramite P.O.S. fisici (*Point Of Sale*).

I circuiti autorizzativi internazionali raggiungeranno l'Istituto emittente della carta di credito e, ottenuto l'esito della richiesta di autorizzazione al pagamento, lo comunicheranno alla Banca o all'Azienda di Servizi Bancari.

In tempo reale l'esito della richiesta di pagamento verrà comunicato sia all'acquirente, attraverso la visualizzazione di una nuova finestra del browser, sia al Centro Servizi.

L'acquirente verrà nuovamente indirizzato sul server del Centro Servizi in una pagina WEB di conferma prodotta e gestita dal Centro Servizi.

Contestualmente, verranno trasmessi due messaggi di posta elettronica, uno indirizzato al Centro Servizi e uno all'acquirente, nei quali saranno riassunti gli elementi essenziali della transazione effettuata: l'identificativo del Centro Servizi, la data e l'ora della transazione, l'importo e l'esito dell'operazione.

A questo punto il Centro Servizi potrà autorizzare l'operazione di trasferimento dei dati cartografici acquistati o effettuarne la consegna, secondo le modalità più adatte (v. infra).

Esistono Istituti di Credito in grado di fornire l'intero servizio di pagamento on line e che, oltre alla sottoscrizione di uno specifico contratto, non richiedono ulteriori impegni quali l'apertura di un conto presso una delle proprie sedi. In alternativa è possibile rivolgersi a società che forniscono servizi bancari e che si appoggiano a banche convenzionate.

Il processo di pagamento on line può quindi svolgersi tra Centro Servizi e Istituto di Credito oppure tra Centro Servizi e Azienda di Servizi Bancari che interfaccia direttamente l'Istituto di Credito convenzionato.

## **Protocolli**

### SET (Secure Electronic Transaction)

Lo standard denominato SET è stato definito da alcuni dei rappresentanti di maggior rilievo del mondo informatico ed economico tra cui Visa, Mastercard, Microsoft, Netscape e IBM. Si tratta dello standard di partenza per la realizzazione di piattaforme applicative orientate al commercio on-line. Attualmente la versione disponibile di SET è la 2.0 e si basa su di un algoritmo a chiavi asimmetriche.

Affinchè l'utente possa effettuare transazioni su un sito *SET-enabled*, è necessario che segua i seguenti passi:

- Acquisire una carta di credito SET (*Visa, Mastercard, Amex*);
- Sottoscrivere una richiesta di certificato digitale SET presso una società autorizzata;
- Ottenere il certificato digitale;
- Installare il certificato sul proprio sistema

Un vantaggio offerto da questo standard è rappresentato dal fatto che le informazioni riservate, quale il numero di carta di credito, non sono gestite dal proprietario del sito di e-commerce.

### SSL (Secure Socket Layer)

Questo protocollo, standardizzato da Microsoft e Netscape, è stato realizzato al fine di inibire la rilevazione di informazioni riservate attraverso il percorso tra il sito di e-commerce e l'utente finale. Il protocollo è infatti in grado di criptare le informazioni prima che siano trasmesse sulla rete, dove intrusi potrebbero intercettarle.

A differenza del protocollo SET, lo standard SSL non richiede all'utente l'installazione di particolari certificati, ma solamente di possedere un browser che supporti SSL (*Internet Explorer 3.01, Netscape Navigator 4.01 e successive versioni*). Per riconoscere l'utilizzo del protocollo SSL, la pagina "sicura", sulla quale viene reindirizzato l'utente, utilizzerà un URL del tipo "HTTPS://....." dove "HTTPS" sta per "HTTP+SSL".

## Integrazione delle funzioni di e-Commerce

Il Centro Servizi per implementare una soluzione di pagamento on line dovrà considerare i seguenti punti:

- sottoscrizione di accordo con “*Payment Gateway*” – la situazione italiana vede attualmente pochi attori in questo ruolo; le soluzioni proposte sono comunque complete (gestiscono cioè le più diffuse carte di credito) e richiedono uno sforzo minimo per abilitare un sito WEB alle transazioni economiche. Il ruolo di “*Payment Gateway*” viene solitamente svolto da Istituti di Credito o Aziende fornitrici di Servizi Bancari che si appoggiano a banche convenzionate;
- integrazione delle funzionalità a supporto del pagamento on line nel sito WEB - esiste un ampio numero di Aziende specializzate nelle soluzioni di commercio elettronico capaci di integrare sul sito WEB del cliente le funzionalità di vendita on-line senza apportare modifiche radicali al sito e operando in tempi molto brevi. Partendo da un sito già realizzato, il servizio offerto mette a disposizione il modulo d'ordine, il *gateway* con uno degli istituti convenzionati ed eventualmente la funzione “carrello” che permette all'acquirente di selezionare ed acquistare un certo numero di articoli durante la stessa sessione. Il livello di integrazione con le procedure applicative esistenti, il database dei dati cartografici e quant'altro necessario dovrà essere valutato in fase progettuale.

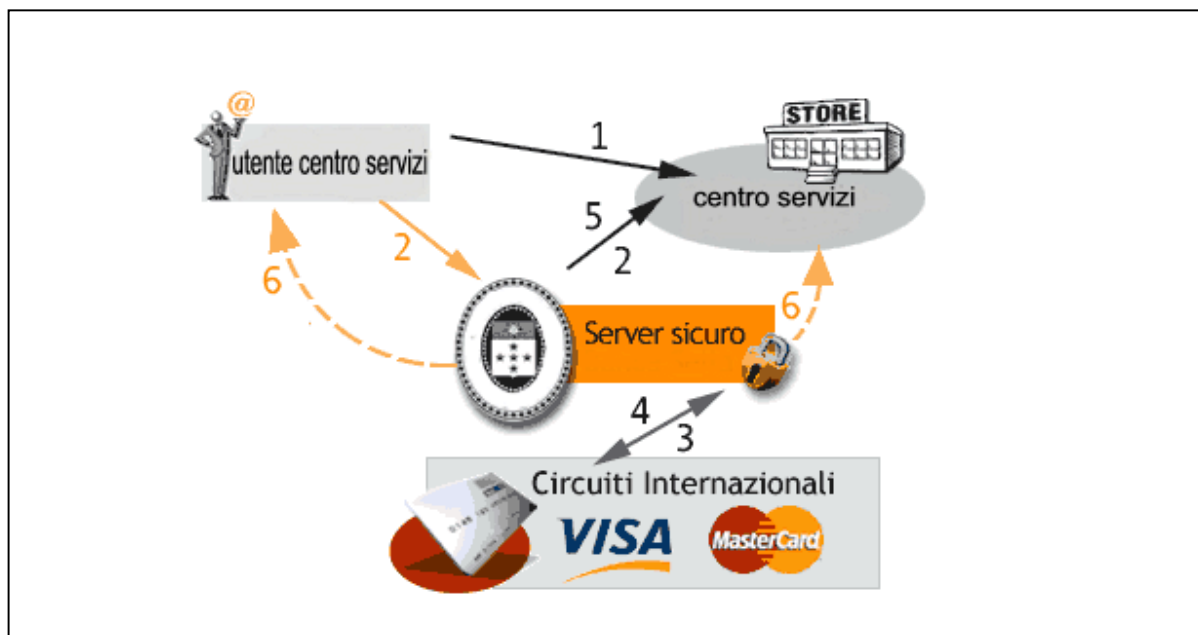


Fig. 6 - Procedura di acquisto e pagamento on-line con carta di credito

## Sistemi di pagamento di III Generazione

Per concludere la panoramica dei metodi di pagamento on line è necessario prendere in considerazione anche i cosiddetti “Sistemi di pagamento di *III Generazione*”, anche questi metodi utilizzano la “via telematica” con la particolarità di consentire il pagamento delle transazioni sostituendo al denaro una somma “*virtuale*”. Ne costituiscono esempi, sulla base delle sperimentazioni finora svolte:

assegni elettronici: certificati digitali (*documenti elettronici*) sottoscritti con firma digitale, che vengono inviati dall’acquirente al Centro Servizi e da questo, dopo aver a sua volta firmato con la propria firma digitale, inviati alla Banca per l’incasso.

“borsellino elettronico”: carta prepagata e ricaricabile. Tecnicamente si tratta di una *smart card*, cioè una tessera contenente un chip che permette di memorizzare informazioni (*simile alla smart card fornita dalle Certification Authorities emittenti i certificati di firma digitale*). Nella card viene registrata una stringa di bit alla quale è attribuito un certo valore in denaro che potrà essere prelevato al momento del pagamento digitando un codice specifico. Ad ogni utilizzo, viene scalata dalla carta una somma corrispondente all’importo dell’acquisto. La smart card può essere ricaricata a seconda dell’esigenza dell’utente.

digicash (*moneta elettronica in senso stretto*): in questo caso la stringa di bit corrispondente alla somma di denaro viene memorizzata direttamente sul computer dell’utente. In sostanza l’acquirente procede al pagamento in favore del Centro Servizi attraverso “*cyberdollar*”. Il Centro Servizi procede insieme alla Banca al controllo del numero di serie delle banconote digitali con un apposito software, per verificare che non si tratti di denaro contraffatto o già speso in precedenza. La gestione del sistema avviene attraverso l’uso della crittografia asimmetrica.

Questi metodi di pagamento vengono solitamente consigliati per acquisti effettuati saltuariamente e di limitato valore.

Anche l’utilizzo di sistemi di pagamento on line di “*III Generazione*” comporta la stipula di accordi specifici con “*Payment Gateway*” che si fa carico della gestione della transazione economica vera e propria.

## 3 Sezione terza - Raccomandazioni per le fasi realizzative

### 3.1 Riepilogo degli elementi utili alla stesura del capitolato

Nella “Sezione prima” del presente documento sono stati discussi i requisiti di sicurezza nella distribuzione della cartografia digitale e in particolare:

- *scambio di informazioni in modo controllato* e in grado di soddisfare tutte le esigenze di comunicazione tra il Centro Servizi e gli utenti nell’ambito dell’utilizzo e della fornitura del servizio;
- *garanzia di sicurezza e di inviolabilità* dei dati trasferiti;
- *osservanza delle prescrizioni normative* tramite l’invio agli utenti di documenti firmati, in linea con i requisiti definiti nel DPR 513/97, con garanzia di piena validità legale e giuridica dei documenti di cartografia prodotti e trasmessi in forma elettronica;
- *rapporto di proporzionalità* delle soluzioni rispetto alle reali necessità del Centro Servizi e alle concrete possibilità di ciascun interlocutore;
- *interoperabilità e cooperazione applicativa* con altri Enti Pubblici, attraverso l’adozione di strumenti e metodologie standard;
- *trasparenza* nella gestione del rapporto cliente/fornitore tra utenti e Centro Servizi.

Le caratteristiche del sistema in grado di soddisfare i requisiti sopra sintetizzati è descritto nella *Sezione Seconda – “Progetto di massima della soluzione”* - coinvolge le seguenti aree:

1) Dotazione di un sistema di firma digitale comprendente:

- il certificato, le chiavi pubblica e privata e la pubblicazione della prima, con i relativi programmi di gestione forniti da una Certification Authority;
- messa in opera delle procedure per la firma dei documenti cartografici e loro archiviazione;
- i programmi applicativi in grado di gestire in modo automatico l’invio della cartografia richiesta attraverso una procedura di file transfer e di registrare il buon esito delle transazioni;
- i programmi applicativi per l’invio della procedura di file transfer e di quella per la verifica della validità del documento.

2) Acquisizione dei seguenti prodotti/servizi:

- un prodotto di trasferimento file - file transfer – che consenta la compressione dei dati, la trasmissione su linea sicura, la notifica al Centro Servizi dell’avvenuta transazione con esito positivo e la registrazione di tutte le operazioni di trasferimento dati effettuate secondo le specifiche al *Paragrafo 2.2.3.*

- 3) Progettazione dei programmi di gestione del sito Web in modo da rendere automatica l'erogazione dei servizi e in particolare le funzioni di seguito sintetizzate:
- Identificazione ed autorizzazione comprendente (v. *Paragrafo 2.3.1 "Identificazione utenti"*):
    - la registrazione automatica di nuovi utenti con la generazione di password rispondenti a requisiti di sicurezza;
    - l'identificazione e la validazione dell'utente;
    - la gestione delle disposizioni contrattuali in termini di funzioni rese disponibili e di modalità di pagamento.
  
  - Invio dei prodotti con modalità file transfert, per entrambe le ipotesi di trasmissione (v. *Paragrafo 2.3.4 "Processi per il trasferimento dei dati cartografici"*):
    - invio immediato
    - invio differito
  
  - Gestione delle notifiche automatiche di buon esito delle transazioni (v. *Paragrafo 2.2.3 "Buon fine delle transazioni"*);
  - Fornitura del programma di verifica di autenticità del prodotto (v. *Paragrafi 2.2.2 "Certificazione e riconoscibilità – Il procedimento di verifica"* e *2.3.3 "Procedure di verifica"*);
  - Fornitura del servizio di verifica di autenticità operata dal Centro Servizi (v. *Paragrafo 2.3.3 "Procedure di verifica"*).

## 3.2 Aspetti Economici

Lo studio delle informazioni raccolte consente una valutazione dei costi di implementazione delle diverse soluzioni suggerite. L'esame dei costi è stato effettuato considerando i valori minimi e massimi per ogni "categoria" sotto elencata.

### 3.2.1 Identificazione Utenti

La valutazione dei costi di una procedura di identificazione "sicura" degli utenti del Centro Servizi, la sua integrazione con gli ambienti operativi esistenti, con le attuali procedure applicative, con l'archivio di cartografia, con le procedure di pagamento (on line e non) e con le procedure gestionali, è strettamente legata sia al livello di integrazione, sia al livello di automazione che si intende ottenere tra le diverse operazioni che devono essere effettuate per giungere al completo svolgimento di tutti i processi coinvolti.

L'impegno per implementare la funzionalità di "identificazione utenti" integrandola nell'attuale ambiente potrebbe coprire, approssimativamente, una fascia di tempo che varia dai dieci giorni ai quaranta giorni uomo.

Per una stima più precisa è necessario conoscere in modo approfondito la realtà del Centro Servizi, analizzare nel dettaglio le procedure applicative ed identificare il livello di integrazione ed automazione che si desidera raggiungere.

### **3.2.2 Sistemi Trasferimento Dati**

Sul mercato sono attualmente reperibili diversi prodotti che garantiscono i prerequisiti richiesti. La valutazione è legata al numero di utenti che utilizzano le funzionalità di trasferimento dati ed al numero delle operazioni effettuate contemporaneamente.

Alcuni di questi prodotti sono indirizzati a realtà complesse e di notevoli dimensioni che movimentano grandi quantità di dati.

L'utilizzo di questi prodotti comporta inoltre investimenti economici piuttosto gravosi che superano facilmente le centinaia di milioni.

Altri prodotti, altrettanto efficaci e più adatti alle attività gestite dal Centro Servizi, possono essere quotati tra Lire 40.000.000 e Lire 60.000.000.

Al costo del software è necessario aggiungere gli indispensabili servizi di installazione, configurazione, personalizzazione e formazione che vengono valutati in Lire 15.000.000 circa.

### **3.2.3 Procedura Firma Digitale**

Come è stato in precedenza sottolineato, per l'attivazione della procedura di "firma digitale" è necessario rivolgersi ad una delle Certification Authorities italiane iscritte nell'elenco pubblico AIPA (Autorità per l'Informatica nella Pubblica Amministrazione).

Ogni C.A. segue politiche diverse per quanto riguarda:

- la validità del certificato di firma, che varia da un anno a tre anni ed in alcuni casi è legata alle condizioni contrattuali e alla validità legale;
- la fornitura del kit di firma che comprende: smart card, lettore di smart card e software per firma e gestione della smart card;
- la possibilità o meno di rinnovo del certificato di firma.

I costi relativi all'attivazione della procedura di "firma digitale" possono essere quindi suddivisi in:

- costo della *Prima Emissione*, che varia da un minimo di Lire 12.000 per arrivare ad un massimo di Lire 90.000;
- costo del *Rinnovo* che, se previsto, viene valutato da Lire 10.000 a Lire 43.000;
- costo del *Kit di Firma* che viene quotato da un minimo di Lire 90.000 ad un massimo di Lire 200.000.

Oltre ai costi sopra elencati è necessario prevedere i costi di installazione di software e hardware e di formazione del Personale del Centro Servizi. Queste attività possono essere effettuate entro un massimo di una giornata lavorativa.

### **3.2.4 Procedura Pagamento**

Nella valutazione dei costi relativi alla procedura di pagamento on line è necessario in primo luogo considerare l'integrazione delle funzionalità a supporto di questa modalità nel sito WEB del Centro Servizi.

I costi di implementazione, in questa fase, sono difficilmente valutabili poichè direttamente dipendenti dal livello di personalizzazione e integrazione che si intende ottenere, nonché dalle caratteristiche dell'ambiente operativo e di quello applicativo esistenti.

E' invece possibile valutare, anche se in modo non preciso, i costi legati all'accordo da stipulare con il "payment gateway" cioè con l'Istituto di Credito o la Società di Servizi Bancari.

La valutazione prevede:

- *costo delle licenze d'uso del software utilizzato;*
- *costo dell'attivazione del servizio;*
- *percentuale di commissione* sul valore delle transazioni effettuate e stornate.

Il costo delle *licenze d'uso* varia da Lire 15.000 a Lire 35.000 mensili in relazione alla complessità delle funzionalità richieste.

Il costo di *attivazione del servizio* è di circa Lire 200.000.

La *percentuale di commissione* sul transato è variabile in funzione dell'importo globale della movimentazione e al massimo può raggiungere il 4% sul totale dell'intero valore.