






SERVIZI INFORMATICI E FORNITURA DI BENI CONNESSI ALLA REALIZZAZIONE,  
DISTRIBUZIONE E GESTIONE DELLA CARTA NAZIONALE DEI SERVIZI (CNS)

# Manuale Utente della CNS

## RAGGRUPPAMENTO TEMPORANEO DI IMPRESE

 <i>Società Mandataria (Gruppo AlmavivA)</i>	
 <i>Società Mandante (ora AlmavivA)</i>	 <i>Società Mandante</i>
 <i>Società Mandante (ora SIA SSB)</i>	 <i>Società Mandante</i>

Codice documento: **213 – 01 - 02**

Versione: **02**

Distribuzione: **Pubblica**

<b>ELENCO DELLE MODICHE APPORTATE</b>			
<b>Data</b>	<b>Versione.</b>	<b>Paragrafo</b>	<b>Modifiche</b>
2 gen 2007	01		Prima versione del documento
21 gen 2008	02	2.3.3, 2.3.4, 2.3.5, 2.3.6	Descrizione del software “Universal Middleware” di gestione carte, che sostituisce il software “CNS Manager”
		2.3.7	Revisione descrizione della procedura di verifica funzionamento della CNS
		2.3.9.2	Descrizione nuova funzione “pin on demand”
		2.4.1	Descrizione del nuovo card carrier

## Sommario

<b>1</b>	<b>INTRODUZIONE.....</b>	<b>5</b>
1.1	SCOPO DEL DOCUMENTO .....	5
1.2	VERSIONE E NOVITÀ .....	5
1.3	CONVENZIONI DI LETTURA .....	5
1.4	ABBREVIAZIONI.....	5
1.5	RIFERIMENTI .....	5
1.6	GESTIONE DEL DOCUMENTO.....	6
<b>2</b>	<b>LA CARTA NAZIONALE DEI SERVIZI.....</b>	<b>6</b>
2.1	COS'È LA CARTA, CHI LA EMETTE, A COSA SERVE .....	6
2.2	RISPOSTE ALLE DOMANDE PIÙ FREQUENTI.....	8
2.3	UTILIZZO DELLA CARTA.....	11
2.3.1	<i>Pre-requisiti per l'utilizzo della CNS.....</i>	<i>11</i>
2.3.2	<i>Installazione del lettore di smart card.....</i>	<i>11</i>
2.3.3	<i>Installazione del software di gestione della CNS.....</i>	<i>12</i>
2.3.4	<i>Verifica di base della CNS mediante lo "Smart Card Manager".....</i>	<i>13</i>
2.3.5	<i>Autenticazione online col browser Internet Explorer.....</i>	<i>14</i>
2.3.6	<i>Autenticazione online col browser Mozilla Firefox.....</i>	<i>15</i>
2.3.7	<i>Prova di funzionamento della CNS sul Portale.....</i>	<i>17</i>
2.3.8	<i>Firma digitale con l'applicazione File Protector.....</i>	<i>21</i>
2.3.9	<i>Avvertenze importanti sulla gestione del PIN.....</i>	<i>22</i>
2.3.10	<i>Sblocco del PIN di autenticazione.....</i>	<i>26</i>
2.3.11	<i>Sblocco del PIN di firma digitale.....</i>	<i>26</i>
2.4	PRIVACY E SICUREZZA.....	27
2.4.1	<i>Trattamento dei dati personali.....</i>	<i>27</i>
2.4.2	<i>Sicurezza della carta.....</i>	<i>28</i>
2.5	IL CONTENUTO DELLA CARTA .....	29
2.5.1	<i>Dati anagrafici e generali.....</i>	<i>29</i>
2.5.2	<i>Chiave e certificato di autenticazione.....</i>	<i>29</i>
2.5.3	<i>Chiave e certificato di firma digitale (se previsti).....</i>	<i>29</i>
2.5.4	<i>Dati sanitari (se previsti).....</i>	<i>29</i>
2.5.5	<i>Dati memorizzati nella banda magnetica.....</i>	<i>32</i>
2.5.6	<i>Altri dati (se previsti).....</i>	<i>32</i>
2.6	ADEMPIMENTI PER L'ATTIVAZIONE DELLA CNS .....	33
2.7	OBBLIGHI E RESPONSABILITÀ DEL TITOLARE .....	33
<b>3</b>	<b>COSA FARE SE.....</b>	<b>34</b>
3.1	A CHI RIVOLGERSI .....	34
3.1.1	<i>Portale CNS.....</i>	<i>34</i>
3.1.2	<i>Call Center.....</i>	<i>35</i>
3.2	PROCEDURE.....	36
3.2.1	<i>Smarrimento, furto o manomissione della CNS.....</i>	<i>36</i>
3.2.2	<i>Errori anagrafici o imprecisioni sui dati stampati e contenuti.....</i>	<i>36</i>
3.2.3	<i>Difficoltà di installazione del software e/o anomalie.....</i>	<i>36</i>
3.2.4	<i>Malfunzionamento della CNS.....</i>	<i>36</i>
3.2.5	<i>Richiesta di ulteriori informazioni.....</i>	<i>37</i>
3.3	IN CASO DI PROBLEMI .....	37
<b>4</b>	<b>APPENDICI .....</b>	<b>38</b>
4.1	RIFERIMENTI NORMATIVI .....	38
4.2	RIFERIMENTI TECNICI .....	38

## Indice delle figure

Figura 1: Un esempio di CNS.....	6
Figura 2: Il lettore SCR 355 fornito dal RTI.....	11
Figura 3: Il software Smart Card Manager – informazioni di base sulla CNS inserita.....	13
Figura 4: Verifica impostazione codice Windows.....	14
Figura 5: Internet Explorer: richiesta del PIN.....	14
Figura 6: Internet Explorer: selezione del certificato.....	15
Figura 7: Mozilla Firefox: richiesta del PIN.....	15
Figura 8: Mozilla Firefox: selezione del certificato.....	16
Figura 9: Home page di <a href="http://www.progettocns.it">www.progettocns.it</a> .....	18
Figura 10: <a href="http://www.progettocns.it">www.progettocns.it</a> : “Come usare la Carta” .....	18
Figura 11: Finestra con richiesta del pin di autenticazione.....	19
Figura 12: Esito della prova di funzionamento CNS sul portale: carta senza certificato di firma .....	19
Figura 13: Esito della prova di funzionamento CNS sul portale: carta con certificati di autenticazione e di firma .....	20
Figura 14: File Protector - impostazione del tipo di smart card.....	21
Figura 15: Informazioni contenute nella busta PIN (carta con solo il certificato di autenticazione).....	23
Figura 16: Informazioni contenute nella busta PIN (carta con certificati di autenticazione e di firma) .....	23
Figura 17: Esempio di stampa di codici pin puk per carta senza certificato di firma .....	24
Figura 18: Esempio di stampa codici pin puk per carta con certificato di firma .....	25
Figura 19: Il card carrier spedito insieme alla carta NS.....	27
Figura 20: La home page del Portale CNS .....	34

# 1 Introduzione

## 1.1 Scopo del documento

Questo documento è destinato ai titolari di Carta Nazionale dei Servizi, CNS, fornita da una delle Amministrazioni aderenti al [contratto-quadro del CNIPA](#). Il documento fornisce informazioni generali sulla CNS (cos'è, a cosa serve, ecc) e guida gli utenti nell'utilizzo della stessa e nella risoluzione di eventuali difficoltà.

## 1.2 Versione e novità

Questa è la versione 2.0 del documento

Il documento è stato totalmente rivisto in relazione alla sostituzione del software di gestione carte (da "CNS Manager" a "Universal Middleware") e all'introduzione della nuova funzione di stampa dei codici pin puk.

## 1.3 Convenzioni di lettura

Nel resto del presente documento, col termine "Portale CNS" ci si riferisce al sito web accessibile all'indirizzo <http://www.progettocns.it>, realizzato e gestito dal RTI su commessa del CNIPA. Per ulteriori informazioni si rimanda al paragrafo 3.1.1 (pag. 34)

## 1.4 Abbreviazioni

Di seguito si fornisce l'interpretazione delle principali abbreviazioni usate nel presente documento:

CNIPA	Centro Nazionale per l'Informatica nella Pubblica Amministrazione
PA	Pubblica Amministrazione
PIN	Personal Identification Number: codice numerico segreto, noto solo al Titolare, utilizzato per accedere ai dati riservati della CNS
PUK	PIN Unblocking Key: codice analogo al PIN, usato per sbloccare quest'ultimo
RSA	Rivest.-Shamir-Adleman: il più diffuso sistema crittografico a chiavi pubbliche
RTI	Il Raggruppamento Temporaneo di Imprese (formato da Actalis S.p.A., Finsiel S.p.A., Oberthur Card Systems Italia srl, SIA S.p.A., Trust Italia S.p.A.) che produce, fornisce e gestisce le CNS nell'ambito del contratto-quadro CNS del CNIPA.
SSL	Secure Sockets Layer: il più diffuso protocollo di sicurezza per il web

## 1.5 Riferimenti

Nel presente documento si fa riferimento ai seguenti ulteriori documenti:

[1] "Manuale Utente - UNIVERSAL Middleware – Smart Card Manager"

## 1.6 Gestione del documento

La redazione, approvazione, aggiornamento e pubblicazione del presente documento sono in carico al RTI. Le revisioni ed aggiornamenti del presente documento avvengono in caso di necessità riconosciuta dal RTI e/o su richiesta del CNIPA.

## 2 La Carta Nazionale dei Servizi

### 2.1 Cos'è la Carta, chi la emette, a cosa serve

La Carta Nazionale dei Servizi (CNS) è lo strumento attraverso il quale i cittadini vengono riconosciuti in rete in modo certo, al fine di usufruire dei servizi on-line erogati dalle Pubbliche Amministrazioni (PA). La CNS può essere emessa solo dalle PA (solitamente dalle Regioni, ma può trattarsi anche di Comuni o altri enti pubblici).

Si tratta di una carta di materiale plastico, con le stesse dimensioni di una normale carta di credito, sulla quale è incorporato un dispositivo elettronico "intelligente" (microchip). Una carta di questo tipo, in generale, viene anche chiamata "carta a microchip" oppure "smart card". La Figura 1 mostra un esempio di CNS (si tenga presente che il motivo grafico è diverso per ciascuna PA emittente):



Figura 1: Un esempio di CNS

Sul supporto plastico della CNS sono sempre presenti, obbligatoriamente, il nome della PA emittente e la scritta "CARTA NAZIONALE DEI SERVIZI". Normalmente sono anche riportati i principali dati anagrafici del Titolare (nome, cognome, codice fiscale, data di nascita, ecc) e la data di scadenza della carta. Ciascuna PA emittente, tuttavia, può adottare scelte proprie in merito ai dati riportati sul supporto plastico della CNS e sulla loro disposizione, così come sul motivo grafico di sfondo.

Il microchip della CNS è in grado di svolgere operazioni crittografiche complesse e di memorizzare diversi dati personali. In particolare, il microchip della CNS contiene una "chiave privata di autenti-

cazione” ed un corrispondente “certificato di autenticazione” che consentono il riconoscimento sicuro dell’utente attraverso Internet. In parole povere: una volta dotati di CNS, si può dimostrare la propria identità quando, usando il normale browser, si accede ad un sito web che richiede l’identificazione degli utenti. Questa funzionalità si basa sul sistema noto come SSL, il quale in pratica funziona come segue (spiegazione semplificata):

- 1) quando si cerca di accedere ad un’area del sito web che richiede l’autenticazione dell’utente, il sito web invia al browser una richiesta di autenticazione;
- 2) per rispondere alla richiesta, il browser comanda alla CNS di svolgere una operazione crittografica usando la “chiave di autenticazione” (a questo punto l’utente deve digitare il PIN della CNS);
- 3) il browser, poi, invia al sito web il risultato dell’operazione crittografica insieme al “certificato di autenticazione” dell’utente, estratto dalla CNS;
- 4) il sito web verifica l’esattezza del calcolo effettuato dalla CNS in base anche alle informazioni contenute nel “certificato di autenticazione” dell’utente; se il risultato è corretto, l’identità dell’utente collegato è quella che risulta dal certificato.

Quella sopra descritta è la finalità principale della CNS: consentire una più veloce e sicura interazione tra le PA e il cittadino grazie alla funzionalità di autenticazione sicura on-line.

È importante ricordare che le Pubbliche Amministrazioni hanno l’*obbligo*, per effetto delle vigenti norme di legge, di consentire l’accesso ai propri servizi on-line anche mediante la CNS. Tale obbligo discende, in particolare, dal Codice dell’Amministrazione Digitale [3].

Le PA hanno facoltà di identificare gli utenti attraverso Internet anche con modalità diverse (es. la tradizionale “password”). Tuttavia, l’accesso mediante CNS dev’essere sempre consentito, indipendentemente dalle altre modalità di accesso disponibili e dalla specifica PA che ha emesso la CNS. Diversi servizi on-line accessibili via CNS sono già attivi (un elenco può essere consultato sul sito [www.italia.gov.it](http://www.italia.gov.it)) e in futuro saranno sempre di più. Le norme attuali prevedono che tutte le PA si predispongano per supportare la CNS entro il 31 dicembre 2007.

La Carta può svolgere anche ulteriori funzioni, come spieghiamo più avanti.

## 2.2 Risposte alle domande più frequenti

Di seguito forniamo le risposte ad alcune domande ricorrenti, relative alla CNS. I temi vengono comunque approfonditi nel resto del documento.

Domanda	Risposta
Chi mi ha mandato questa carta?	La carta CNS viene fornita al Titolare da parte di una Pubblica Amministrazione (tipicamente la Regione di residenza, ma può anche trattarsi del Comune o di un altro ente pubblico).
A cosa mi serve questa carta?	La CNS è anzitutto uno strumento di identificazione in rete, ossia serve per accedere ad alcuni servizi erogati dalla PA ai cittadini attraverso Internet. Un elenco dei servizi on-line accessibili via CNS è riportato sul sito <a href="http://www.italia.gov.it">www.italia.gov.it</a> . Altri servizi possono essere disponibili secondo la specifica PA emittente, alla quale ci si deve rivolgere per maggiori informazioni.
Devo pagare per averla o per mantenerla nel tempo?	No, le norme di legge stabiliscono che l'onere economico di produzione e rilascio delle CNS è a carico delle singole amministrazioni che le emettono.
A chi appartiene questa carta?	La carta è di proprietà dell'Amministrazione emittente. Qualora il Titolare non desiderasse utilizzarla, la deve restituire all'ente che l'ha rilasciata.
Quali dati riporta? ci sono anche dati sensibili?	La CNS contiene alcuni dati personali e può anche contenere dati sensibili. Per maggiori dettagli si rimanda al paragrafo 2.5 (pag. 29).
La carta ha una scadenza?	Sì. La data di scadenza è indicata sulla carta stessa. La durata della CNS non è mai superiore a 6 anni.
La carta sostituisce altri documenti?	La carta può sostituire il tesserino fiscale, la tessera sanitaria o altri documenti secondo gli accordi in essere tra la PA emittente ed il Ministero delle Finanze od altri enti governativi.  La CNS non sostituisce la carta d'identità, in ogni caso.
Come faccio a modificare i dati se sono sbagliati o se nel tempo cambiano?	I dati essenziali della CNS (es. dati personali, certificato di autenticazione e/o di firma) non possono essere modificati. Se nel corso del tempo alcuni dati sono cambiati, la carta deve essere revocata ed eventualmente riemessa.  Per quanto riguarda i dati sanitari (se presenti): la possibilità di modificarli dipende dalla specifica PA emittente.



Domanda	Risposta
Quali di questi servizi sono fruibili solo disponendo della carta?	Normalmente i servizi erogati dalle PA sono accessibili anche senza disporre della CNS. L'uso della CNS consente però di accedervi in modo più efficiente.
Che cosa devo avere per poter utilizzare la carta?	Per poter usare la CNS è necessario: un normale Personal Computer (PC), un browser, un collegamento ad Internet ed un lettore di smart card; è poi necessario installare il software di gestione della CNS, reso disponibile dalla PA emittente. Per maggiori dettagli si rimanda al paragrafo 2.3 (pag. 11).
Come faccio ad utilizzarla, in pratica?	Si rimanda al paragrafo 2.3 (pag. 11).
Che vantaggio c'è nell'utilizzo della CNS al posto dei tradizionali "userid" e "password"?	<p>Anzitutto una sicurezza molto maggiore. Le password devono essere inviate al sito web per essere verificate da quest'ultimo, pertanto possono essere "indovinate" dai malintenzionati attraverso una serie di tentativi diretti oppure attraverso la tecnica del <i>phishing</i>. Nel caso della CNS, invece, il PIN non viene mai inviato al sito web.</p> <p>Inoltre c'è il problema della moltiplicazione delle password, perché ogni sito gestisce le proprie. Utilizzando la CNS, non c'è più bisogno di ricordarsi di password diverse per ogni sito: è sufficiente ricordarsi il solo PIN della propria carta.</p>
Cos'è la "chiave privata di autenticazione" contenuta nella CNS?	<p>Si tratta di una chiave crittografica; in pratica è un numero segreto, molto grande (circa 300 cifre), diverso per ciascun utente. Si definisce privata perché il suo valore non viene mai "allo scoperto". La chiave privata è custodita all'interno del microchip e non può essere letta in alcun modo; può solo essere utilizzata dal microchip per svolgere operazioni crittografiche, su richiesta delle applicazioni (per es. su richiesta del browser), previa digitazione del PIN.</p> <p>Ad ogni chiave privata corrisponde una ed una sola "chiave pubblica"; quest'ultima non è segreta ed è contenuta nel "certificato di autenticazione" dell'utente (cfr. la domanda successiva).</p>
Cos'è il "certificato di autenticazione"?	<p>Il certificato di autenticazione è un insieme di dati che include, tra l'altro, la "chiave pubblica" (cfr. la domanda precedente) e l'identità dell'utente Titolare sotto forma di codice fiscale.</p> <p>Il certificato è memorizzato sulla CNS e può essere liberamente letto dalle applicazioni (per es. dal browser).</p>
Cosa succede quando mi viene chiesto di inserire il PIN della CNS?	Il PIN viene inviato alla CNS, dove il microchip lo confronta con quello memorizzato all'interno; se il PIN è giusto, significa che l'utente è veramente il legittimo Titolare della CNS, perché solo il Titolare può essere (lecitamente) a conoscenza del PIN.

Domanda	Risposta
Che cosa posso fare se non riesco ad utilizzare la carta?	Per maggiori dettagli si rimanda al capitolo 3 (pag. 34).  Raccomandiamo di leggere con attenzione questo documento, prima di chiedere assistenza.
Posso usare la CNS con il “Macintosh” oppure con Linux o altri sistemi operativi per PC ?	Tecnicamente è possibile, ma non tutte le PA mettono a disposizione il necessario software. Per maggiori dettagli, contattare la propria PA di riferimento (es. Regione).
Cosa devo fare se perdo la CNS, o si rovina o me la rubano?	Si rimanda al capitolo 3 (pag. 34).
Che rischio corro se la carta è utilizzata da qualcun altro o se il codice segreto viene in possesso di qualcun altro o se qualcun altro riesce a leggerne il contenuto?	La CNS non può essere usata per la sua funzione principale (identificazione in rete) senza conoscerne il PIN.  Se la propria CNS viene usata da altri, insieme al PIN, c'è il rischio che altri ottengano servizi on-line al posto del legittimo Titolare.  Alcuni dati personali contenuti nella carta possono essere letti senza conoscere il PIN. Se vengono letti da altri, c'è il rischio di divulgazione di alcuni dati personali del Titolare.  I dati <i>sensibili</i> eventualmente contenuti nella carta (es. alcuni dati sanitari) possono essere letti solo conoscendo il PIN.  Perciò, in considerazione di quanto detto sopra: <ul style="list-style-type: none"><li>• la CNS non deve mai essere lasciata incustodita;</li><li>• il PIN deve essere custodito in luogo diverso dalla carta.</li></ul> Alcuni dati contenuti nella carta possono essere liberamente letti (sono stati memorizzati sulla carta apposta perché ciò sia possibile).  Altri dati, in particolare i dati personali sensibili, non possono essere letti senza conoscere il PIN della carta.  Alcuni dati (per es. la chiave privata di autenticazione) non possono essere letti in alcun caso, anche conoscendo il PIN.
È possibile copiare i dati contenuti nella carta?	
È possibile “clonare” la carta?	È estremamente improbabile. La certificazione di sicurezza del microchip attesta la sicurezza del medesimo. Vedere anche il paragrafo 2.4 (pag. 27)

## 2.3 Utilizzo della Carta

Di seguito, con la frase “usare la CNS” intendiamo *sfruttare la funzione principale offerta della Carta Nazionale dei Servizi, ovvero l’identificazione on-line del Titolare*. Altri possibili usi della CNS (per esempio nell’ambito dei servizi socio-sanitari, della TV digitale terrestre, ecc) non sono trattati in questo documento; per questi ulteriori usi, gli utenti sono invitati a chiedere informazioni direttamente all’Amministrazione emittente.

### 2.3.1 Pre-requisiti per l’utilizzo della CNS

Affinché sia possibile usare la CNS, è necessario che il Titolare:

- 1) sia dotato di un normale PC con collegamento ad Internet;
- 2) sia dotato di un browser che supporta le smart card per l’autenticazione SSL (per esempio Microsoft Internet Explorer™ oppure Mozilla Firefox™);
- 3) abbia ritirato la busta contenente i codici PIN e PUK, oppure abbia ritirato la stampa parziale dei codici PIN e PUK (vedere il capitolo 2.6, pag. 33).
- 4) abbia installato un idoneo lettore di smart card (vedere il capitolo 2.3.2, pag. 11);
- 5) abbia installato il software di gestione della CNS (vedere il capitolo 2.3.3, pag. 12).

Si noti che per le installazioni di cui ai punti 4) e 5) è solitamente necessaria un’utenza di tipo privilegiato (es. “Administrator” in ambiente Windows).

Per gli operatori delle Amministrazioni che accedono all’area riservata “Amministrazione” del Portale CNS, è inoltre necessaria l’installazione del Java Run-Time (scaricabile dal sito <http://www.java.com>).

Di seguito forniamo le istruzioni operative essenziali, assumendo che l’utente abbia già ritirato i codici PIN e PUK (vedere il capitolo 2.6, pag. 33) e che di conseguenza la sua carta sia già stata attivata.

In caso di difficoltà, è possibile chiedere assistenza con le modalità descritte al capitolo 3 (pag. 34).

### 2.3.2 Installazione del lettore di smart card

Affinché il sistema operativo del PC e le applicazioni (per es. il browser) possano colloquiare con la CNS è necessario anzitutto installare sul proprio PC un lettore di smart card. Si tratta di una piccola periferica che solitamente si collega al PC attraverso la porta USB, anche se esistono modelli per porta seriale e di altro tipo. Il lettore fornito dal RTI alle Amministrazioni che ne fanno richiesta è il modello “SCR 355” prodotto dalla SCM Microsystems, uno dei leader di mercato.



Figura 2: Il lettore SCR 355 fornito dal RTI

Per l'installazione del suddetto lettore si procede come segue:

- scaricare il driver (sotto forma di archivio ZIP) dal Portale CNS, area “Kit per il cittadino”;
- espandere l'archivio ZIP in una directory temporanea, quindi lanciare il programma SETUP per installare il driver, seguendo le istruzioni a video;
- al termine, collegare il lettore alla porta USB del PC.

Se l'utente non ha ricevuto un lettore SCR 355 dalla propria PA di riferimento, dovrà procurarsene uno presso una rivendita di accessori per PC. In commercio sono reperibili lettori di diverse marche e modelli, acquistabili anche via Internet. I test svolti dal RTI portano a concludere che la maggioranza dei lettori di più ampia diffusione è compatibile con la CNS. Qualsiasi lettore che soddisfi i seguenti requisiti dovrebbe risultare compatibile con la CNS:

- conformità allo standard ISO 7816 parti 1, 2, 3
- supporto per carte di Classe A e Classe B (oppure AB)
- disponibilità di un driver conforme allo standard PC/SC

Si raccomanda comunque all'utente di verificare col fornitore la compatibilità del lettore con la CNS, prima di procedere all'acquisto.

### 2.3.3 Installazione del software di gestione della CNS

Dopo aver installato il lettore di smart card, è necessario anche installare il software di gestione della CNS. Questo serve anzitutto per consentire alle applicazioni (es. il browser) di colloquiare con la CNS usando un “linguaggio” standardizzato; inoltre, il software consente alcune operazioni accessorie, come per esempio la modifica o lo sblocco del PIN. Per l'installazione, si procede come segue:

- scaricare il software di gestione carte “Universal Middleware – Smart Card Manager” dal Portale CNS, reperibile nell'area “Kit per il cittadino”;
- lanciare l'installazione seguendo le istruzioni a video;
- riavviare il PC.

A questo punto il PC dovrebbe essere pronto per l'uso della CNS.

NB: alla data di revisione di questo documento, il software “Universal Middleware – Smart Card Manager” è disponibile anche per il sistema operativo Microsoft Windows Vista (per il dettaglio di tutti i requisiti di installazione si rimanda al Manuale Utente Universal Middleware – Smart Card Manager. L'utente che abbia esigenze specifiche (es. installazione su MacOS X oppure Linux) è invitato a chiedere assistenza alla propria Amministrazione di riferimento (es. Regione).

Coloro che utilizzano il software “CNS Manager” possono sostituirlo con la “Libreria Software Universal Middleware – Smart Card Manager” eseguendo le procedure disponibili sul portale CNS nell'area “kit per il cittadino”.

### 2.3.4 Verifica di base della CNS mediante lo “Smart Card Manager”

Per verificare che il lettore ed il software di gestione della CNS siano stati installati correttamente, si raccomanda di procedere come segue:


- dal menu Start di Windows lanciare il programma “Smart Card Manager” cliccando sull'icona  posta in basso a destra (può essere attivato anche dall'area di notifica);
- inserire la CNS nel lettore ed attendere qualche istante affinché la carta venga rilevata, riconosciuta come CNS, e vengano lette da esse alcune informazioni; se tutto procede regolarmente, comparirà la seguente finestra:



Figura 3: Il software Smart Card Manager – informazioni di base sulla CNS inserita

Se quanto abbiamo illustrato combacia con quello che si verifica sul PC dell'utente, questo conferma che il lettore di smart card ed il software di gestione carte sono stati correttamente installati.

Si consiglia inoltre di effettuare un'ulteriore verifica. Nella finestra precedente selezionare **Avanzate** e verificare che compaia la schermata indicata a pagina seguente:



Figura 4: Verifica impostazione codice Windows

Se non presente, selezionate il campo come da schermata precedente.

A questo punto non resta che utilizzare la CNS nel modo previsto, ossia per accedere ai servizi online che richiedono l'autenticazione. Di seguito spieghiamo come farlo con i due più diffusi browser, Microsoft Internet Explorer e Mozilla Firefox.

### 2.3.5 Autenticazione online col browser Internet Explorer

Quando ci si collega ad un sito web che richiede l'autenticazione, il browser Internet Explorer chiede all'utente di inserire il PIN della CNS, come mostrato nella seguente figura:

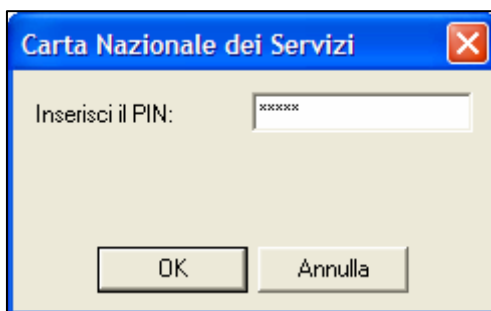
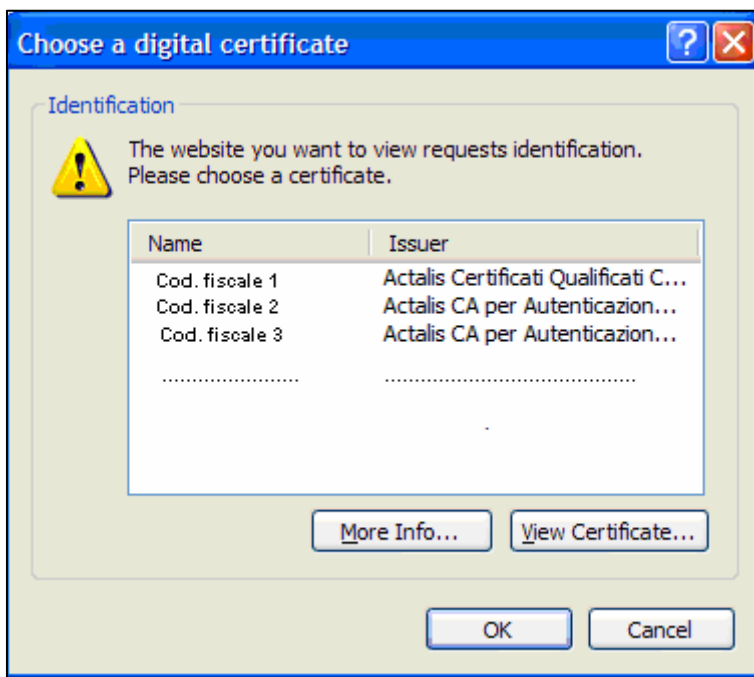


Figura 5: Internet Explorer: richiesta del PIN

In questo caso l'utente non deve far altro che inserire il PIN e premere il tasto OK per completare il processo di autenticazione.

Nel caso in cui l'utente posseda più di un certificato e/o il PC sia utilizzato da più persone, prima di chiedere il PIN il browser chiede di selezionare il certificato desiderato, come mostrato nella seguente figura:

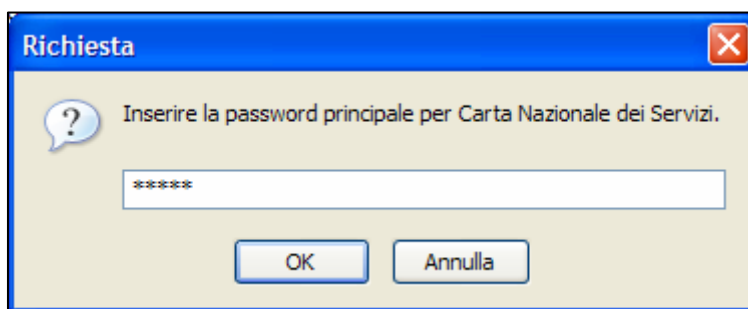


**Figura 6: Internet Explorer: selezione del certificato**

In questo caso si deve selezionare il certificato giusto (in base al proprio codice fiscale) e poi premere il bottone OK.

### 2.3.6 Autenticazione online col browser Mozilla Firefox

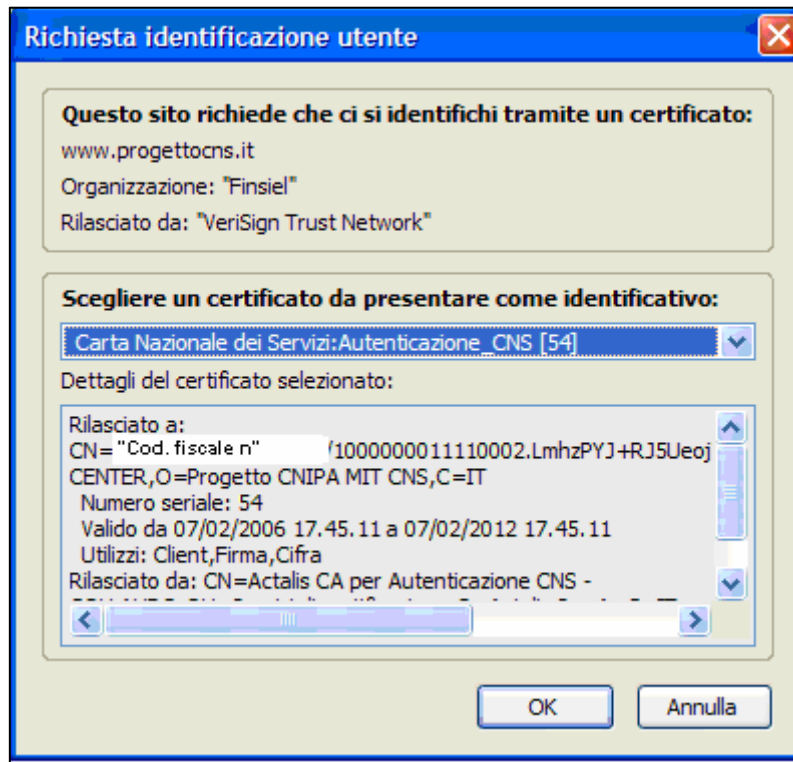
Quando ci si collega ad un sito web che richiede l'autenticazione, il browser Mozilla Firefox chiede all'utente di inserire il PIN della CNS, come mostrato nella seguente figura:



**Figura 7: Mozilla Firefox: richiesta del PIN**

Normalmente, l'utente non deve far altro che inserire il PIN e premere il tasto OK per completare il processo di autenticazione.

Nel caso in cui l'utente posseda più di un certificato e/o il PC sia utilizzato da più persone, il browser chiede di selezionare il certificato desiderato, come mostrato nella seguente figura:



**Figura 8: Mozilla Firefox: selezione del certificato**

In questo caso si deve selezionare il certificato giusto (in base al proprio codice fiscale) e poi premere il bottone OK.



### 2.3.7 Prova di funzionamento della CNS sul Portale

La carta CNS è sempre dotata del certificato di autenticazione, possiede quindi tre codici relativi al certificato di autenticazione:

- Il codice PIN (Personal Identification Number) di autenticazione: composto da 5 cifre, è richiesto dal sistema per permettere l'accesso ai servizi forniti dalla carta. Se il PIN di autenticazione viene digitato errato per 3 volte consecutive, viene automaticamente bloccato. Per sbloccarlo, il Titolare deve utilizzare il codice PUK.
- Il codice PUK (PIN Unblocking Key) di autenticazione: composto da 8 cifre, deve essere utilizzato per sbloccare il PIN di autenticazione, come descritto a pag. 26.
- Il codice di revoca della carta: composto da 10 cifre, deve essere comunicato in caso di revoca in emergenza della carta.

Se la carta CNS possiede anche il certificato di firma, possiede ulteriori tre codici relativi al certificato di firma:

- Il codice PIN (Personal Identification Number) di firma: composto da 5 cifre, è richiesto dal sistema per permettere l'accesso ai servizi forniti dalla carta. Se il PIN di firma viene digitato errato per 3 volte consecutive, viene automaticamente bloccato. Per sbloccarlo, il Titolare deve utilizzare il codice PUK.
- Il codice PUK (PIN Unblocking Key) di firma: composto da 8 cifre, deve essere utilizzato per sbloccare il PIN di firma, come descritto a pag. 26.
- Il codice di revoca del certificato di firma: composto da 10 cifre, deve essere comunicato in caso di revoca in emergenza della carta.

Prima di accedere a servizi on-line reali, si raccomanda di eseguire la procedura di seguito descritta per verificare la correttezza della carta CNS e nel contempo per reperire i codici di revoca associati alla carta stessa.

1. Accedere a [www.progettocns.it](http://www.progettocns.it): viene evidenziata la seguente schermata. Cliccare > **Come usare la carta**

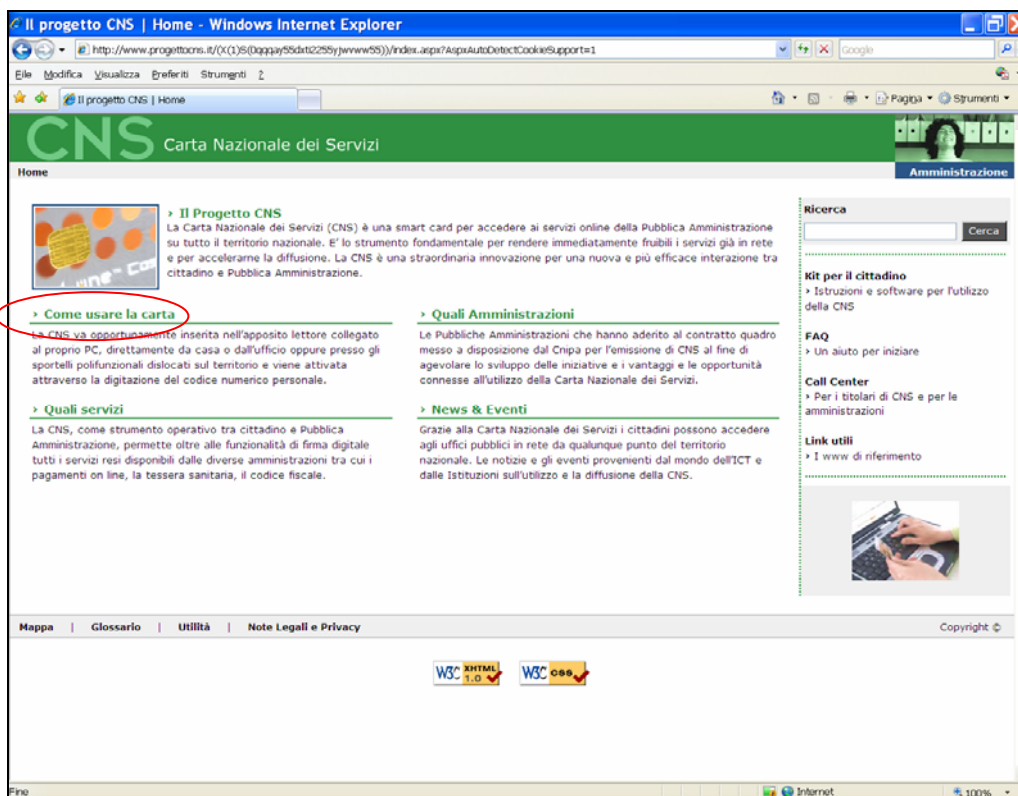


Figura 9: Home page di [www.progettocns.it](http://www.progettocns.it)

2. viene evidenziata la seguente schermata. Cliccare **clickare qui**

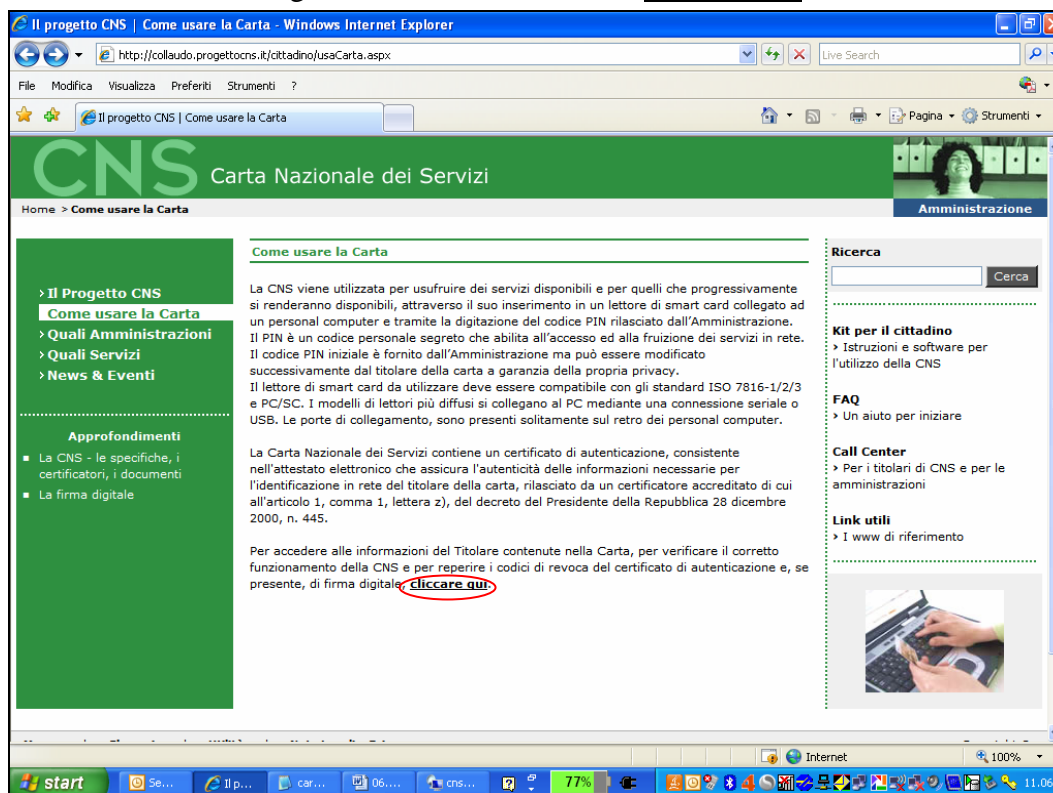


Figura 10: [www.progettocns.it](http://www.progettocns.it): “Come usare la Carta”

- viene evidenziata la seguente finestra nella quale occorre digitare il pin smart card (è il pin di autenticazione, composto da 5 cifre):

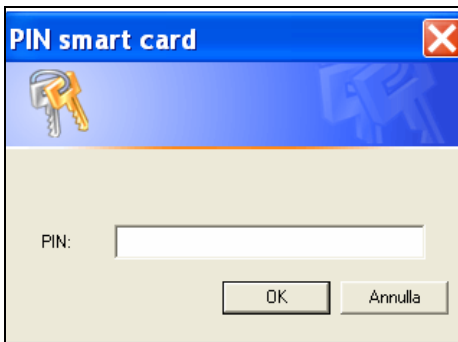


Figura 11: Finestra con richiesta del pin di autenticazione

- viene evidenziata una schermata di informazioni relative alla CNS usata per autenticarsi.  
**Se la carta non possiede il certificato di firma, viene evidenziata la seguente schermata:**

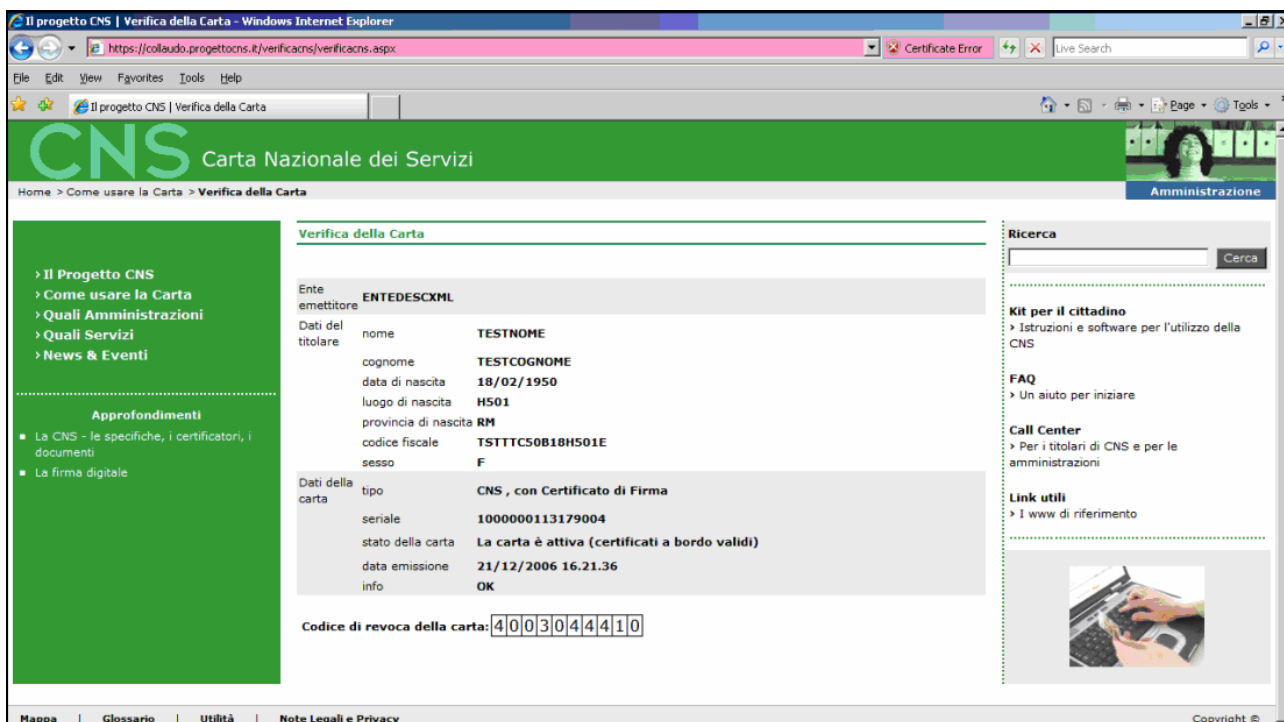


Figura 12: Esito della prova di funzionamento CNS sul portale: carta senza certificato di firma

Se la carta possiede il certificato di firma, viene evidenziata la seguente schermata:

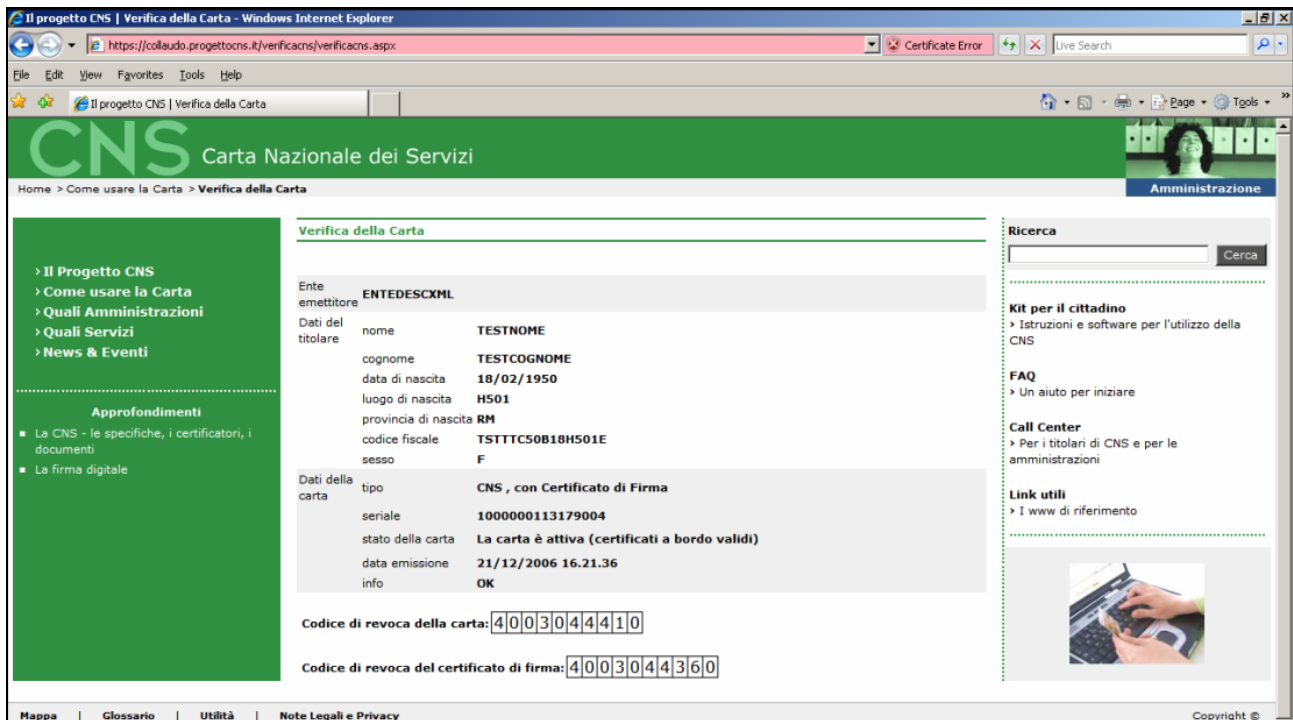


Figura 13: Esito della prova di funzionamento CNS sul portale: carta con certificati di autenticazione e di firma

### 2.3.8 Firma digitale con l'applicazione File Protector

Nel caso in cui la CNS sia stata predisposta per la firma digitale, l'utente riceve dalla propria PA di riferimento anche un'applicazione che consente appunto, mediante la CNS, di apporre firme digitali su file e documenti di ogni tipo; l'applicazione si chiama "File Protector".

Normalmente, solo i funzionari pubblici e gli operatori sanitari sono dotati di CNS predisposta per la firma digitale. Ogni PA emittente, comunque, può applicare la propria politica al riguardo.

Per capire se la propria CNS è predisposta per la firma digitale, è sufficiente esaminare il contenuto della busta PIN: se compare anche il "PIN certificato di firma" (vedere il paragrafo successivo), significa che la carta consente anche la firma digitale (per attivare quest'ultima, infatti, è necessario utilizzare un PIN diverso da quello che si usa per l'autenticazione).

Al primo utilizzo di File Protector è necessario verificare che l'applicazione sia configurata in modo opportuno per poter interfacciare la smart card CNS fornita dal RTI. A tale scopo, si deve:

- 1) inserire la CNS nel lettore;
- 2) verificare ed eventualmente correggere la configurazione di File Protector.

Per svolgere il passo 2) procedere come segue: dalla finestra principale di File Protector, selezionare la voce di menu **Dispositivo > Configurazione**. Nella finestra "Configurazione del dispositivo crittografico" (si veda la seguente Figura 14) selezionare "Hardware" e quindi cliccare sul bottone "Impostare automaticamente"; dopo qualche istante, l'applicazione dovrebbe aver identificato automaticamente la carta inserita come una "**Oberthur CNS**". Nel caso in cui l'identificazione automatica non riesca, selezionare manualmente la voce "Oberthur CNS" dal menu a discesa, come mostrato nella Figura 14. Infine, cliccare sul bottone OK per tornare alla finestra principale. A questo punto File Protector è configurato correttamente.

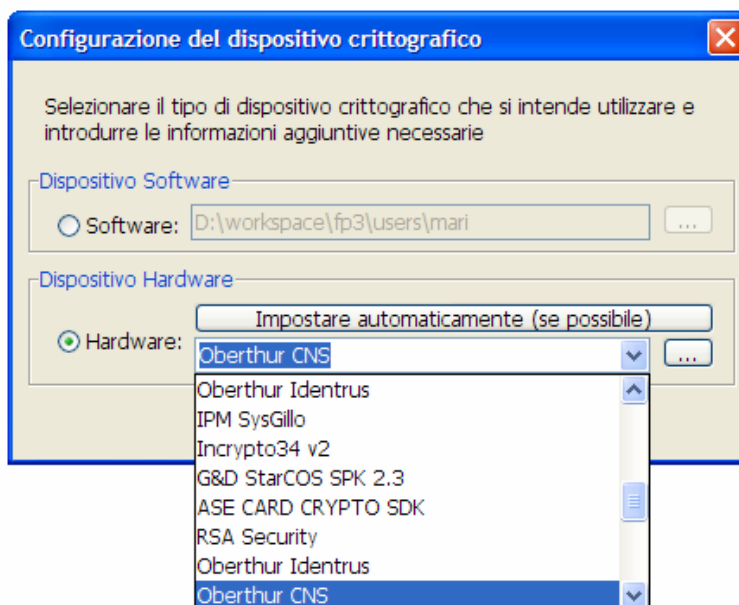


Figura 14: File Protector - impostazione del tipo di smart card

Per le istruzioni da seguire per l'apposizione della firma digitale con l'applicazione File Protector, si rimanda al manuale utente installato insieme all'applicazione stessa.

### 2.3.9 Avvertenze importanti sulla gestione del PIN

Come tutte le smart card, anche la CNS contiene diversi meccanismi di sicurezza atti ad impedirne l'uso da parte di utenti non autorizzati.

Abbiamo visto in precedenza che durante la fase di autenticazione on-line, quando il browser interagisce con la CNS, l'utente deve digitare un PIN. Si tratta di un codice segreto e personale, che si suppone conosciuto solo dal legittimo Titolare della carta. Il PIN viene quindi inviato alla CNS, dove viene confrontato con il valore corretto, memorizzato nel microchip; se il valore del PIN corrisponde, la CNS assume che l'utente sia il vero Titolare e quindi accetta di svolgere l'elaborazione richiesta dal browser (elaborazione che coinvolge la "chiave privata").

Per limitare il rischio di uso non autorizzato della "chiave privata", tutte le smart card applicano la seguente regola: se l'utente inserisce un PIN sbagliato più volte di seguito, è segno che quell'utente non è il legittimo Titolare della CNS; la carta a quel punto si blocca, cosicché non è più possibile fare ulteriori tentativi di "indovinare" il PIN. Quando la carta è bloccata, è possibile sbloccarla solo digitando un altro codice segreto, chiamato PUK.

**ATTENZIONE:** inserendo un PIN errato per 3 volte di seguito, la CNS si blocca; a questo punto può essere sbloccata utilizzando il codice PUK, come descritto di seguito. Tuttavia, se inserite in modo errato anche il PUK per 3 volte di seguito, la carta si blocca in maniera **irreversibile**.

Nel caso della CNS, il PIN è un numero di 5 cifre, mentre il PUK è un numero di 8 cifre.

Il Titolare deve custodire i codici PIN e PUK lontano da occhi indiscreti, in un posto diverso da quello dove viene tenuta la CNS. Solo il Titolare deve conoscere questi codici segreti e personali, se vuole evitare che la propria CNS venga usata da altre persone, con la conseguente possibilità di inconvenienti anche seri.

Il Titolare riceve questi codici in occasione dell'attivazione della sua carta (vedi il paragrafo 2.6, pag. 33). La consegna dei codici è fatta da un Operatore autorizzato dall'Amministrazione, previo riconoscimento del Titolare. I codici possono essere consegnati con due differenti modalità (tra di loro in alternativa):

- a) Consegna dei codici in busta chiusa
- b) Consegna di un foglio che riporta stampate solo le cifre finali dei codici.

### 2.3.9.1 Consegna dei codici in busta chiusa

Il Titolare riceve una busta chiusa, che non contiene il nome del Titolare ma riporta il numero della carta assegnata al Titolare

Di seguito mostriamo l'aspetto del modulo PIN/PUK cartaceo che viene consegnato al Titolare del CNS, in busta chiusa, al momento dell'attivazione (vedere il paragrafo 2.6):

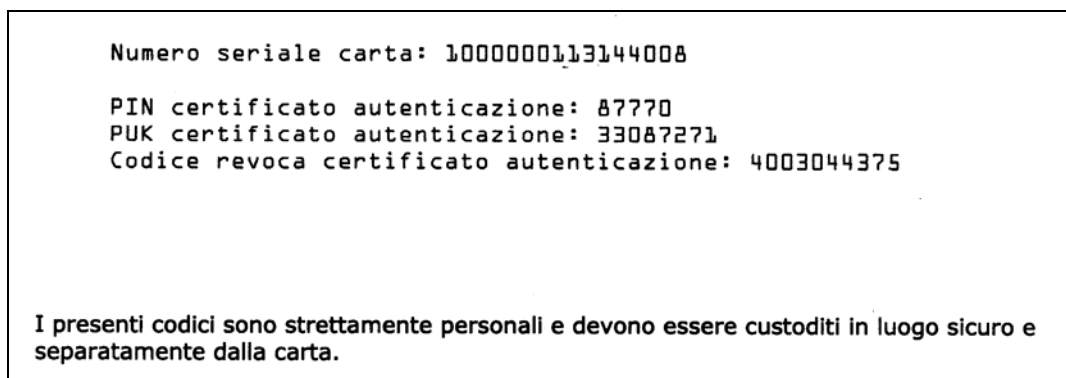


Figura 15: Informazioni contenute nella busta PIN (carta con solo il certificato di autenticazione)

In questo modulo, il “Codice revoca certificato autenticazione” è riportato solo per completezza di informazione; questo codice, normalmente, non è necessario al Titolare della CNS.

Nel caso di CNS predisposta anche per la firma digitale, il modulo riporta anche il PIN e PUK specifici per la firma digitale:

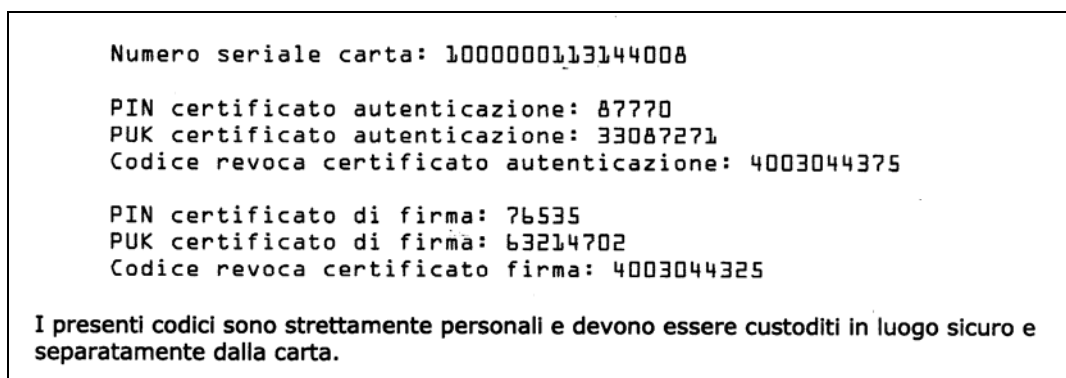


Figura 16: Informazioni contenute nella busta PIN (carta con certificati di autenticazione e di firma)

In questo caso il “Codice revoca certificato firma” è riportato per conformità alle norme di legge relative alla firma digitale. Questo codice può essere utile per richiedere al certificatore (Actalis S.p.A.) una revoca urgente della CNS in caso di furto o smarrimento della stessa.

### 2.3.9.2 Consegna della stampa parziale dei codici (procedura "pin on demand")

In alternativa alla modalità precedente, il Titolare può ricevere dall'Operatore autorizzato, sempre previo riconoscimento del Titolare da parte dell'Operatore, un foglio stampato sul momento che riporta le ultime cifre dei codici pin puk.

Le cifre iniziali di tali codici sono stampate sul foglio (denominato card carrier) inviato insieme alla carta:

Sul card carrier sono riportate:

- Le prime 2 cifre (su 5 cifre) del pin di autenticazione
- Le prime 4 cifre (su 8 cifre) del puk di autenticazione
- Le prime 5 cifre del codice di revoca del certificato di autenticazione

Se la carta possiede anche il certificato di firma, il card carrier riporta anche:

- Le prime 2 cifre (su 5 cifre) del pin di firma
- Le prime 4 cifre (su 8 cifre) del puk di firma
- Le prime 5 cifre del codice di revoca del certificato di firma

Nel caso in cui la carta abbia soltanto il certificato di autenticazione, al Titolare viene consegnato un foglio come da esempio:

The image shows a printed document with the following content:

- Header: "Il progetto CNS | Pin/Puk della Carta" on the left and "Page 1 of 1" on the right.
- Logo: "CNS AREA RISERVATA Carta Nazionale dei Servizi" on the left and a photo of a woman on the right.
- Section: "Pin/Puk della Carta" with a box containing "CNS numero di serie N°: 6140000141430007".
- Section: "Codici di accesso alla carta" with three boxes for PIN, PUK, and revoca codes.
- Footer: "Per motivi di sicurezza, sul presente modulo sono riportati solo in parte i codici Pin, Puk e Revoca. Le prime cifre dei codici sono stampate sul modulo che è stato spedito al Titolare insieme alla CNS. Per eventuali problemi è possibile contattare il Call Center al numero 02.69019975".

Codice PIN:	[ ] [ ] [ ] [ ] [ ]	Codice PUK:	[ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ]	Codice di revoca:	[ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ]
-------------	---------------------	-------------	---------------------------------	-------------------	---

Figura 17: Esempio di stampa di codici pin puk per carta senza certificato di firma




Nel caso in cui la carta abbia anche il certificato di firma, al Titolare viene consegnato un foglio come da esempio:

Il progetto CNS | Pin/Puk della Carta Page 1 of 1

---

# CNS

AREA RISERVATA  
Carta Nazionale dei Servizi



---

**Pin/Puk della Carta**

---

CNS numero di serie N°: **6140000141430007**

---

**Codici di accesso alla carta**

Codice PIN: <input type="text" value="8"/> <input type="text" value="3"/> <input type="text" value="0"/>	Codice PUK: <input type="text" value="5"/> <input type="text" value="3"/> <input type="text" value="7"/> <input type="text" value="1"/>	Codice di revoca: <input type="text" value="7"/> <input type="text" value="5"/> <input type="text" value="3"/> <input type="text" value="1"/> <input type="text" value="0"/>
--	---	--

---

**Codici di firma**

Codice PIN: <input type="text" value="8"/> <input type="text" value="1"/> <input type="text" value="3"/>	Codice PUK: <input type="text" value="1"/> <input type="text" value="5"/> <input type="text" value="4"/> <input type="text" value="5"/>	Codice di revoca: <input type="text" value="7"/> <input type="text" value="5"/> <input type="text" value="2"/> <input type="text" value="1"/> <input type="text" value="4"/>
--	---	--

Per motivi di sicurezza, sul presente modulo sono riportati solo in parte i codici Pin, Puk e Revoca.  
Le prime cifre dei codici sono stampate sul modulo che è stato spedito al Titolare insieme alla CNS.  
Per eventuali problemi è possibile contattare il Call Center al numero 02.69019975

**Figura 18: Esempio di stampa codici pin puk per carta con certificato di firma**

Si fa presente che per motivi di sicurezza, per ciascuna carta è possibile **richiedere una volta sola** la stampa parziale dei codici pin / puk

Il codice di Revoca, nella sua completezza, è sempre reperibile accedendo con la propria CNS direttamente al seguente indirizzo internet:

**<https://www.progettocns.it/verificacns/verificacns.aspx>**

Viene evidenziata la finestra riportata in Figura 11 (pag. 19): digitare il pin di autenticazione per visualizzare la schermata relativa alla propria carta. In tale schermata, oltre ai dati della carta sono indicati i codici di revoca, come da esempi riportati in Figura 12 (carta senza certificato di firma) a pag. 19, o in Figura 13 (carta con certificato di firma) a pag. 20.

In alternativa, il Titolare può utilizzare la procedura **“Prova di funzionamento della CNS sul Portale”**, descritta a pag. 17, per reperire il codice di revoca.

### **2.3.10 Sblocco del PIN di autenticazione**

Per sbloccare il PIN di autenticazione si raccomanda di usare l'utility "Smart Card Manager" la cui installazione è descritta nel paragrafo 2.3.3 (pag. 12). Per ulteriori dettagli si rimanda al documento "Manuale Utente - UNIVERSAL Middleware – Smart Card Manager", disponibile in [www.progettocns.it](http://www.progettocns.it).

In alternativa, gli utenti dotati dell'applicazione File Protector possono usare tale applicazione per lo sblocco del PIN di autenticazione.

### **2.3.11 Sblocco del PIN di firma digitale**

Per sbloccare il PIN di firma digitale si deve usare l'utility "Smart Card Manager" la cui installazione è descritta nel paragrafo 2.3.3 (pag. 12). Per ulteriori dettagli si rimanda al documento "Manuale Utente - UNIVERSAL Middleware – Smart Card Manager", disponibile in [www.progettocns.it](http://www.progettocns.it).

## 2.4 Privacy e sicurezza

### 2.4.1 Trattamento dei dati personali

Il “ Titolare del trattamento” dei dati personali è l’Amministrazione emittente la CNS.

L’informativa all’utente ai sensi del D.Lgs. n.196/03 è riportata sul “card carrier”, ossia sul foglio di carta sul quale si trova incollata la carta (ricordiamo che la CNS viene inviata all’utente per posta).

La seguente figura mostra l’attuale aspetto del card carrier:

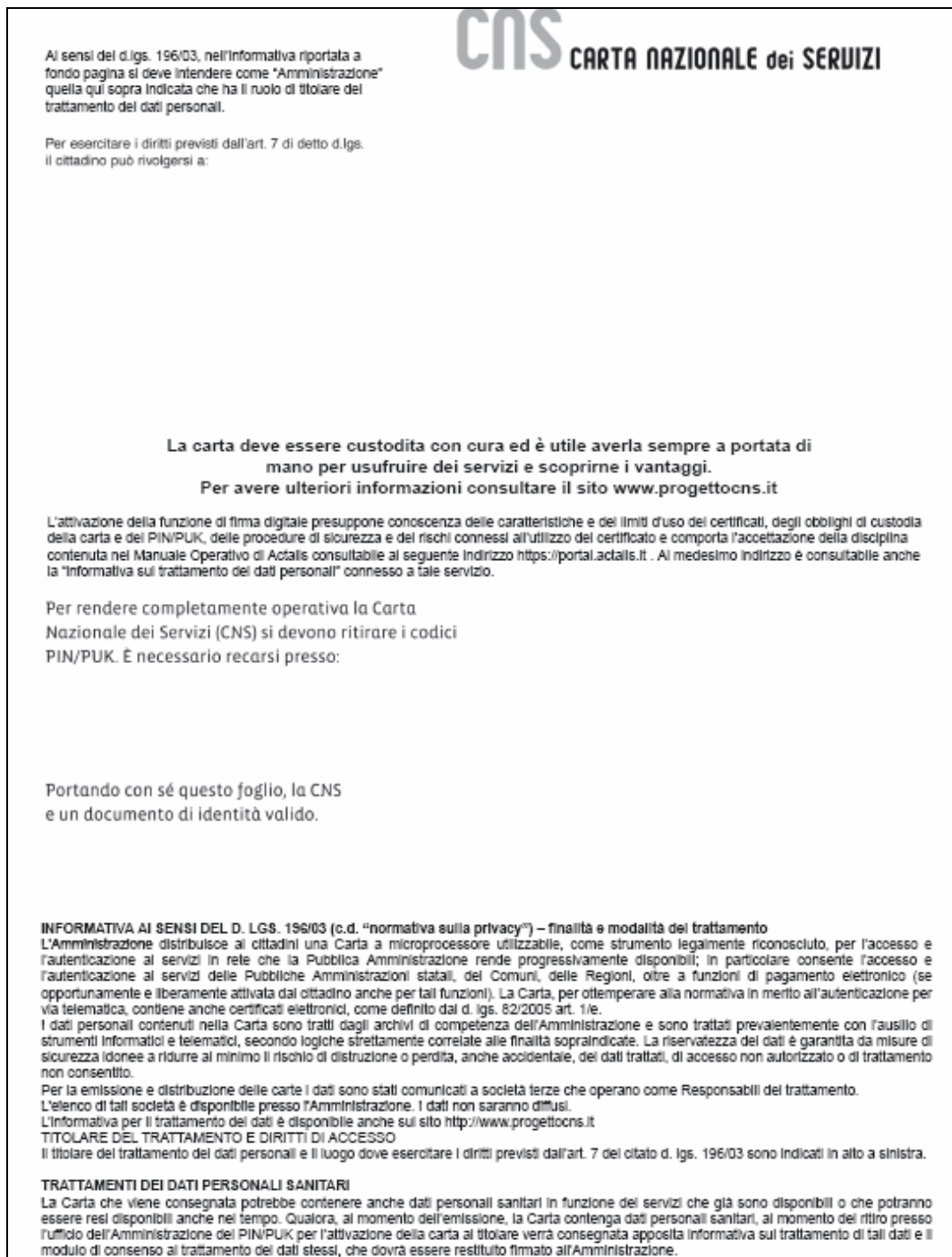


Figura 19: Il card carrier spedito insieme alla carta NS

Per esercitare i diritti previsti dall'art. 7 del D.Lgs. n.196/03, il cittadino deve rivolgersi all'indirizzo indicato sul card carrier.

Qualora, al momento dell'emissione, la Carta contenga dati personali sanitari, al momento del ritiro presso l'ufficio dell'Amministrazione dei PIN/PUK per l'attivazione della carta, al Titolare verrà consegnata apposita informativa sul trattamento di tali dati e il modulo di consenso al trattamento dei dati stessi, che dovrà essere restituito firmato all'Amministrazione

## 2.4.2 Sicurezza della carta

La CNS è realizzata con un microchip che risponde pienamente a tutti i requisiti di sicurezza imposti dalla vigente normativa in tema di CNS e di firma digitale.

I dati memorizzati sul microchip ricadono in due tipologie: dati *pubblici* e dati *privati*; i dati pubblici possono essere liberamente letti da chiunque e da qualsiasi applicazione, seguendo le specifiche tecniche della CNS riportate sul sito del CNIPA ([www.cnipa.gov.it](http://www.cnipa.gov.it)). I dati privati possono essere letti (od utilizzati per svolgere operazioni crittografiche, nel caso delle chiavi) solo previo invio alla carta di un apposito codice segreto, il PIN, che si suppone noto solo al Titolare della CNS. La gestione del PIN da parte della carta è già stata descritta nel paragrafo 2.3.9 (pag. 22).

La CNS è costruita per resistere anche ai più sofisticati attacchi. La cosiddetta “clonazione” della carta è praticamente impossibile e comunque alquanto improbabile. La carta fornita dal RTI è stata sottoposta a scrupolose verifiche di sicurezza da parte di un laboratorio specializzato e indipendente, i cui risultati sono stati certificati da un autorevole organismo governativo.

Per ulteriori dettagli sulle caratteristiche di sicurezza della CNS, si invitano gli utenti a contattare la propria Amministrazione emittente.

## **2.5 Il contenuto della Carta**

Di seguito si descrivono i principali dati di interesse del Titolare contenuti nella CNS.

### **2.5.1 Dati anagrafici e generali**

La CNS contiene i seguenti dati anagrafici e generali:

- codice identificativo della PA che ha emesso la carta
- data di emissione della carta
- data di scadenza della carta
- nome del Titolare
- cognome del Titolare
- data di nascita del Titolare
- sesso del Titolare
- codice fiscale del Titolare
- codice identificativo del comune di nascita del Titolare
- codice identificativo del comune di residenza del Titolare

### **2.5.2 Chiave e certificato di autenticazione**

La CNS contiene sempre una chiave privata di autenticazione ed il corrispondente certificato, rilasciato da un certificatore accreditato nel rispetto delle norme vigenti in tema di CNS.

Nei precedenti paragrafi 2.1, 2.2, 2.3 abbiamo descritto il meccanismo dell'autenticazione on-line e fornito le istruzioni operative per eseguirla con i più diffusi browser.

### **2.5.3 Chiave e certificato di firma digitale (se previsti)**

La CNS può contenere anche una chiave privata di firma ed il corrispondente certificato qualificato, rilasciato da un certificatore accreditato nel rispetto delle norme vigenti in tema di firma digitale.

La predisposizione della CNS per la firma digitale avviene su richiesta dell'Amministrazione emittente, secondo politiche proprie.

### **2.5.4 Dati sanitari (se previsti)**

La CNS può essere predisposta per operare come carta sanitaria. In tal caso la carta può contenere una serie di dati sanitari del Titolare, codificati secondo la specifica europea "Netlink", utili nell'ambito dell'erogazione di servizi socio-sanitari (per es. prescrizione di farmaci ed esami, visite ambulatoriali, ricoveri). Questi dati consentono di gestire in modo più mirato le prestazioni sanitarie mediante una maggiore integrazione tra i diversi attori del processo di diagnosi, cura, riabilitazione e assistenza.

Si tenga presente che, formalmente, con "Tessera Sanitaria" (TS) si intende la carta plastica emessa dal Ministero dell'Economia e delle Finanze. Una CNS che contenga dati sanitari non è necessa-

riamente una TS, salvo in caso di accordi a livello istituzionale per la convergenza delle due carte su un unico supporto (come per es. in Lombardia, Friuli, Sicilia).

I dati sanitari eventualmente contenuti nella CNS possono essere raggruppati come segue:

- dati amministrativi ad accesso libero
- dati amministrativi ad accesso protetto
- dati di emergenza ad accesso libero
- dati di emergenza ad accesso protetto
- puntatori ad eventi sanitari

Di seguito diamo una sintetica descrizione dei diversi gruppi. Si tenga presente che molti dei dati descritti di seguito sono opzionali; anche se la propria CNS è predisposta per operare come carta sanitaria, non è detto che contenga tutti i dati elencati di seguito. I dati effettivamente presenti sono quelli selezionati dall'Amministrazione emittente secondo le proprie esigenze.

#### **2.5.4.1 Dati amministrativi ad accesso libero**

Questo gruppo di dati comprende:

- identificativo del Titolare (nome, cognome, sesso, data di nascita, codice fiscale, ecc.);
- lingue parlate e abilità nel linguaggio (preferito, fluente, discreto, ecc.);
- indirizzo di residenza e/o di domicilio (compreso telefono, fax, internet);
- nominativo e telefono delle persone da contattare in caso di emergenza;
- ASL di appartenenza;
- medico di fiducia del Titolare (nome, indirizzo, telefono, codice regionale, ecc.)
- eventuale diritto di assistenza all'estero
- eventuale persona assicurata di riferimento in caso di minorenne
- codice sanitario regionale del Titolare
- date di inizio e fine validità della carta sanitaria
- decisione relativa alla donazione di organi e tessuti

Tutti questi dati in questione possono essere letti dalla carta liberamente. Normalmente, i dati identificativi del Titolare insieme alla ASL e al medico di fiducia vengono memorizzati dalla ASL sulla Carta prima della consegna della stessa al Titolare. La modifica dei dati può essere effettuata solo da operatori sanitari forniti di una "Carta Operatore" con privilegi adeguati.

#### **2.5.4.2 Dati amministrativi ad accesso protetto**

Questo gruppo di dati comprende principalmente informazioni relative alle esenzioni. In particolare:

- esenzioni per patologia (con data scadenza e codice ICD9CM);
- esenzioni per reddito (con categoria di esenzione e data scadenza);
- esenzioni per invalidità (con categoria esenzione, prefisso e suffisso regionale, ecc.);
- diritto alle protesi e ai presidi (con codice protesi e data scadenza);
- diritto ai dietetici (con data scadenza);
- esenzioni per malattie rare (con codice malattia e data scadenza);
- informazioni per la cremazione;
- registro ASL.

Questi dati possono essere letti dalla Carta solo se il Titolare fornisce il proprio PIN, o se il medico possiede una “Carta Operatore” con privilegi di accesso adeguati. I dati di esenzione possono essere memorizzati dalla ASL sulla Carta prima della consegna della stessa al Titolare. La modifica dei dati può essere effettuata solo da operatori sanitari forniti di “Carta Operatore” con privilegi adeguati.

#### **2.5.4.3 Dati di emergenza ad accesso libero**

Questo gruppo di dati comprende informazioni cliniche utili in caso di emergenza, specialmente quando il Titolare è non cosciente. In particolare:

- malattie (categoria clinica, codice clinico, data prima diagnosi, data di registrazione ecc.);
- gruppo sanguigno e trasfusioni (gruppo, fattore Rh, data ultimo esame, trasfusioni ecc.);
- immunizzazioni (categoria, stato, data ultima immunizzazione, codice clinico, vaccinazioni, ecc.);
- terapie (categoria, codice terapia, posologia, data inizio e fine terapia, registrazioni, quantità autorizzata, data ultima prescrizione, ecc.)
- prescrizione oculistica;
- impianti;
- gravidanza;
- organi mancanti.

I dati in questione possono essere liberamente letti dalla Carta, in quanto è interesse del paziente fornire la propria situazione clinica utile in caso di emergenza. La modifica dei dati può essere effettuata solo da operatori sanitari forniti di una “Carta Operatore” con privilegi adeguati.

#### **2.5.4.4 Dati di emergenza ad accesso protetto**

Questo gruppo di dati comprende informazioni cliniche utili in caso di emergenza, specialmente quando il Titolare è non cosciente. In particolare:

- malattie (categoria clinica, codice clinico, data prima diagnosi, data di registrazione ecc.);
- gruppo sanguigno e trasfusioni (Gruppo, fattore Rh, data ultimo esame, trasfusioni ecc.);
- immunizzazioni (categoria, stato, data ultima immunizzazione, codice clinico, vaccinazioni, ecc.);
- terapie (Categoria, codice terapia, posologia, data inizio e fine terapia, registrazioni, quantità autorizzata, data ultima prescrizione, ecc.)
- impianti;
- gravidanza;
- organi mancanti.

Questi dati possono essere letti solo se il Titolare della Carta fornisce il proprio PIN, o se il medico possiede una “Carta Operatore” con privilegi di accesso adeguati. La modifica dei dati può essere effettuata solo da operatori sanitari, forniti di “Carta Operatore” con privilegi adeguati, a cui il Titolare fornisce il proprio PIN.

#### **2.5.4.5 Puntatori alla storia sanitaria**

Questi dati indicano dove è possibile reperire informazioni dettagliate relative ad eventi della storia sanitaria del Titolare. In particolare:

- struttura alternativa al ricovero;
- eventi sanitari (data, numero pratica, struttura sanitaria dove sono conservate le informazioni di dettaglio, annotazioni pediatriche, ecc.)

I dati di questo tipo possono essere letti solo se il Titolare della Carta fornisce il proprio PIN oppure se il medico possiede una “Carta Operatore” con privilegi di accesso adeguati. La modifica dei dati può essere effettuata solo da operatori sanitari forniti di “Carta Operatore” con privilegi adeguati.

### **2.5.5 Dati memorizzati nella banda magnetica**

La CNS è dotata di una banda magnetica, sulla quale sono memorizzati il *numero di serie della carta* ed il *codice fiscale dell'utente*, liberamente leggibili. Questi dati possono essere utilizzati per svariate finalità (es. accesso a parcheggi, mense aziendali, spettacoli, biblioteche, ecc) secondo le particolari esigenze della PA emittente e le infrastrutture ricettive messe in opera sul territorio.

### **2.5.6 Altri dati (se previsti)**

Al di là dei dati sin qui descritti, gli eventuali altri dati contenuti nella CNS e le loro caratteristiche (codifica, sicurezza, ecc) dipendono dalle specifiche Amministrazioni emittenti e dalle particolari applicazioni che fanno uso di tali dati. Per ulteriori dettagli, gli utenti sono invitati a interpellare la propria PA di riferimento.



## **2.6 Adempimenti per l'attivazione della CNS**

Com'è stato anticipato nei paragrafi precedenti, affinché l'utente possa utilizzare la propria CNS è necessario che venga in possesso del PIN. Questo viene consegnato all'utente al momento della "attivazione": un'operazione che avviene in presenza di un operatore dell'Amministrazione emittente. L'utente che riceve una CNS deve dunque, per farsi attivare la carta, procedere come segue:

- recarsi presso l'ufficio pubblico indicato sul card carrier (vedere il paragrafo 2.4, pag. 27), portando con sé un documento d'identità valido (per es. carta d'identità, passaporto o patente di guida con foto), il card carrier e la carta CNS;
- verificare la correttezza dei dati anagrafici stampati sul card carrier e sulla CNS stessa e segnalare all'operatore eventuali inesattezze (in tal caso la carta verrà ritirata e riemessa);
- nel caso di CNS contenente anche dati sanitari, compilare e firmare il modulo del consenso informato, quindi consegnarlo all'operatore;
- ricevere dall'operatore la busta chiusa contenente i codici riservati PIN/PUK, o in alternativa un foglio stampato sul momento riportante le cifre finali dei codici.

A questo punto, la carta è attivata; l'utente può dunque tornare alla propria abitazione ed installare sul proprio PC il software di gestione della CNS, come illustrato nella sezione 2.3 (pag. 11).

## **2.7 Obblighi e responsabilità del Titolare**

Il Titolare di CNS ha l'obbligo di conservare i codici segreti PIN/PUK in luogo sicuro e diverso da quello dove conserva la carta. Le operazioni on-line svolte dall'utente mediante CNS sono attribuite al Titolare della carta.

Si ricorda che la CNS è di proprietà dell'Amministrazione emittente e deve essere utilizzata solo nel modo previsto. L'Amministrazione emittente non necessariamente sostituirà una CNS che risulti danneggiata per un evidente uso improprio da parte del Titolare.

Nel caso in cui la carta sia predisposta per la firma digitale, il Titolare è tenuto a conoscere e rispettare le norme di legge relative alla firma digitale nonché a conoscere e rispettare le disposizioni contenute nel Manuale Operativo del certificatore. Per ulteriori dettagli si rimanda alle indicazioni riportate sul card carrier.

## 3 Cosa fare se...

### 3.1 A chi rivolgersi

#### 3.1.1 Portale CNS

Il RTI ha realizzato il circuito di emissione delle CNS per le Amministrazioni che aderiscono al contratto-quadro del CNIPA (bando di gara n.1/2005). Un componente essenziale del circuito di emissione è rappresentato dal Portale CNS, accessibile all'indirizzo [www.progettocns.it](http://www.progettocns.it), che funge da sistema di raccordo tra Amministrazioni, RTI ed utenti.

Il Portale CNS contiene aree riservate alle Amministrazioni ed aree ad accesso libero, destinate agli utenti (titolari di CNS e non).

La seguente figura mostra la home page del Portale CNS alla data di revisione del presente documento:

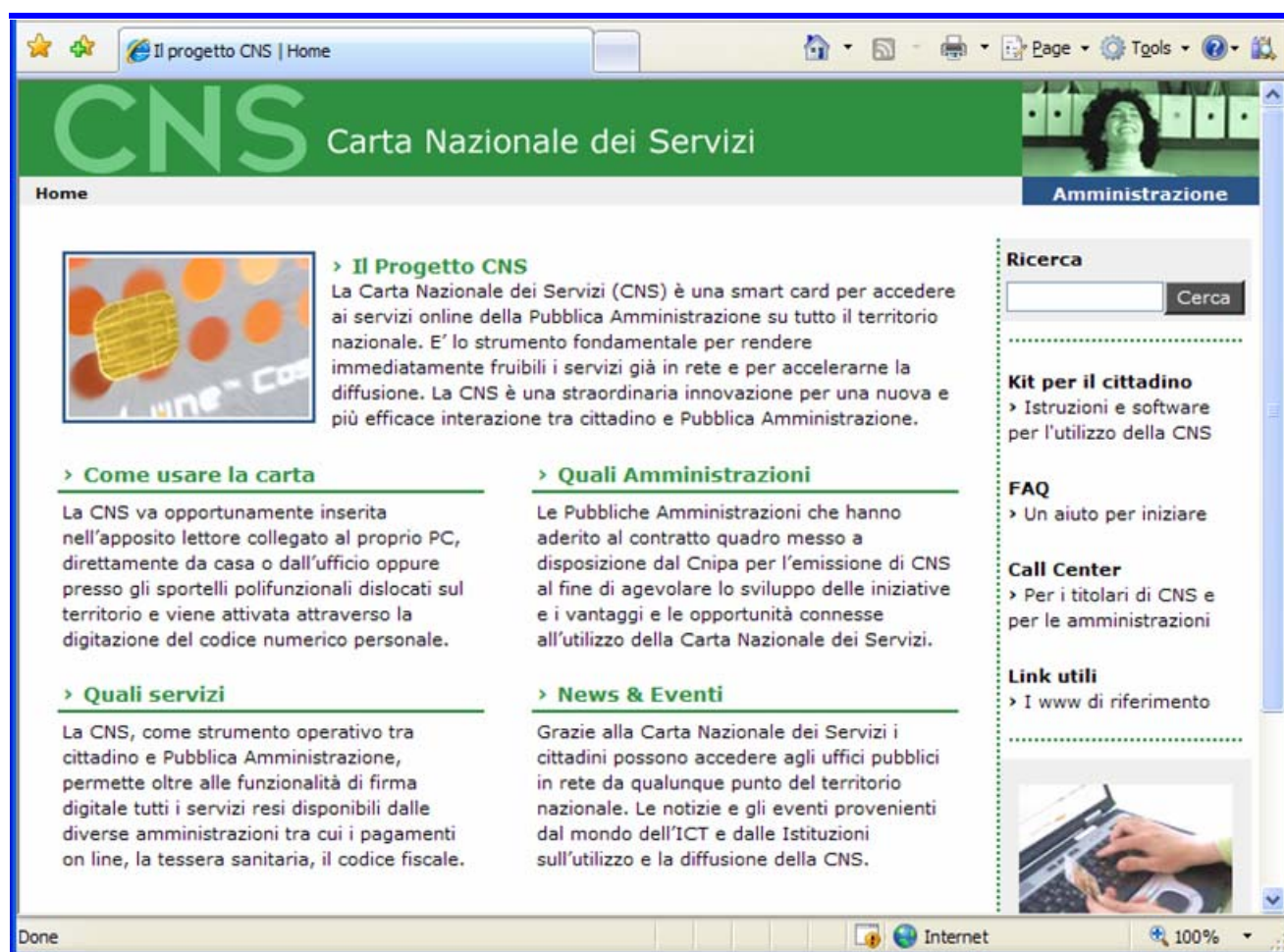


Figura 20: La home page del Portale CNS

Sul Portale CNS il cittadino trova tutte le informazioni necessarie per:

- conoscere le finalità, le caratteristiche e i vantaggi dell'utilizzo della CNS (in particolare attraverso il presente documento);
- individuare le Amministrazioni che hanno aderito al contratto-quadro del CNIPA e che dunque distribuiscono la CNS;
- attrezzare la propria postazione di lavoro ed essere istruito sul funzionamento del software e dei dispositivi previsti;
- ottenere assistenza in caso di problemi connessi all'uso della CNS.

### 3.1.2 Call Center

Il servizio di Call Center, messo a disposizione dal RTI, fornisce assistenza ed informazioni ai cittadini titolari della carta e alle amministrazioni che hanno stipulato contratti esecutivi per la fornitura di CNS.

Il numero di telefono **02-69019975** è a disposizione dei cittadini e delle amministrazioni 24 ore al giorno, per 365 giorni all'anno.

Il Call Center è inoltre contattabile, oltre che per telefono, anche via fax o per e-mail ai recapiti:

Fax: **02-60842154**

E-mail: [csc@siassb.eu](mailto:csc@siassb.eu)

Il Call Center è a disposizione per fornire:

- indicazioni sul progetto CNS, sulla carta CNS e sul suo utilizzo, a chi rivolgersi e come ottenerla;
- assistenza sull'uso della CNS e sull'installazione del software, diagnostica sul funzionamento della carta, informazioni ed assistenza sull'uso del software a corredo, modalità per effettuare il blocco e lo sblocco della carta;
- informazioni sui servizi per bloccare o sbloccare la carta CNS in caso di furto, smarrimento o ritrovamento;
- informazioni alle amministrazioni sulle modalità per l'adesione al progetto di distribuzione e al contratto quadro, assistenza sull'uso delle applicazioni e dei servizi forniti per richiedere, attivare, bloccare o sbloccare una carta.

## 3.2 Procedure

### 3.2.1 Smarrimento, furto o manomissione della CNS

In caso di smarrimento, furto o manomissione da parte di terzi della propria CNS, il Titolare deve darne tempestiva comunicazione all'Amministrazione emittente, *attraverso l'ufficio di attivazione* o con altre modalità eventualmente comunicate al Titolare dall'Amministrazione stessa. Questa provvederà a bloccare la carta ed eventualmente a rimetterne una nuova.

Nel caso di smarrimento o furto di una CNS abilitata per la *firma digitale*, l'utente è tenuto a darne tempestiva comunicazione al certificatore Actalis. Il personale del Call Center provvederà a sospendere o revocare il certificato di firma digitale secondo che l'utente sia in grado o meno di fornire il codice riservato di revoca stampato sul card carrier (si veda la Figura 16).

Si noti che, a fronte di una richiesta di blocco di una CNS motivata da smarrimento o furto, il Call Center può contestualmente bloccare anche le eventuali carte bancarie (carte Bancomat, carte di credito) dell'utente. Questo servizio aggiuntivo è disponibile solo per gli utenti delle Amministrazioni che lo hanno richiesto al RTI.

### 3.2.2 Errori anagrafici o imprecisioni sui dati stampati e contenuti

Nel caso in cui il Titolare riscontri inesattezze nei dati anagrafici stampati sulla carta e/o contenuti nel microchip, successivamente all'attivazione, è tenuto a darne tempestiva comunicazione all'Amministrazione emittente, *attraverso l'ufficio di attivazione* o con altre modalità eventualmente comunicate al Titolare dall'Amministrazione stessa. Questa provvederà a bloccare la carta ed eventualmente a rimetterne una nuova.

### 3.2.3 Difficoltà di installazione del software e/o anomalie

Nel caso in cui il Titolare non riesca ad installare con successo il driver del lettore e/o il software di gestione della CNS, oppure nel caso in cui l'utente riscontri delle anomalie, contattare il Call Center (vedere il paragrafo 3.1.2) preparandosi a fornire le seguenti informazioni:

- i propri dati anagrafici e i propri contatti (telefono, e-mail);
- il nome dell'Amministrazione che ha emesso la carta;
- il numero di serie della CNS (stampato sulla plastica);
- il tipo di PC e la versione del sistema operativo;
- descrizione delle operazioni svolte e dei messaggi di errore eventualmente apparsi a video.

### 3.2.4 Malfunzionamento della CNS

Nel caso vi sia il fondato sospetto di un malfunzionamento della CNS, l'utente deve restituire la carta all'Amministrazione affinché sia trasmessa al Centro di Raccolta Carte.

Si raccomanda all'utente di verificare il funzionamento della propria CNS e segnalare l'eventuale malfunzionamento al Call Center entro un massimo di 10 giorni.

### 3.2.5 Richiesta di ulteriori informazioni

Nel caso l'utente desideri ulteriori informazioni sulla CNS, sulle sue caratteristiche e funzionalità, sulle Amministrazioni aderenti al progetto, ecc., contattare il Call Center (vedere il paragrafo 3.1.2) preparandosi a fornire le seguenti informazioni:

- i propri dati anagrafici e i propri contatti (telefono, e-mail);
- il nome dell'Amministrazione emittente, nel caso l'utente sia Titolare di CNS.

### 3.3 In caso di problemi

In caso di problemi, l'utente è invitato anzitutto a verificare con attenzione di aver svolto correttamente le operazioni di installazione hardware e software.

In questa sede non è possibile fornire una guida completa alla risoluzione di tutti i possibili problemi che possono capitare, per quanto raramente, nell'uso di carte a microchip e relativi lettori e nell'autenticazione online. Ci limitiamo pertanto a suggerire alcune verifiche fondamentali che l'utente può facilmente svolgere da solo e che spesso risultano efficaci:

Verifica	Descrizione
Presenza del lettore tra le periferiche del sistema	Un lettore di smart card correttamente installato deve comparire nell'elenco delle periferiche del PC. Per verificare, dal pannello di controllo, selezionare "Strumenti di amministrazione", poi "Gestione computer" e infine cliccare sulla voce "Gestione periferiche".
Stato del servizio "Smart card"	Il servizio "Smart card" è una componente software del sistema operativo che fa da intermediario tra i lettori di smart card e le applicazioni. Se questo servizio essenziale non è attivo, la CNS risulterà inutilizzabile. Per verificare, si procede come segue: dal pannello di controllo, selezionare "Strumenti di amministrazione" e poi "Servizi". Individuare il servizio "Smart card" e controllarne lo stato.

Se le difficoltà permangono, l'utente può rivolgersi al Call Center con le modalità indicate in precedenza, fornendo tutte le informazioni che gli saranno richieste. Il Call Center, direttamente oppure previo consulto con gli specialisti del caso, provvederà a fornire la necessaria assistenza nel più breve tempo possibile.

## 4 Appendici

### 4.1 Riferimenti normativi

Di seguito si elencano i principali riferimenti normativi relativi alla Carta Nazionale dei Servizi:

- [1] Decreto del Presidente della Repubblica 2 marzo 2004, n.117: “Regolamento concernente la diffusione della carta nazionale dei servizi, a norma dell'articolo 27, comma 8, lettera b), della legge 16 gennaio 2003, n. 3” (G.U. n. 105 del 6 maggio 2004).
- [2] Decreto del Presidente del Consiglio dei Ministri 9 dicembre 2004, “Regole tecniche e di sicurezza relative alle tecnologie e ai materiali utilizzati per la produzione della Carta nazionale dei servizi”.
- [3] D.Lgs. 7 marzo 2005, n. 82 aggiornato con le modifiche introdotte dal D.Lgs. 4 aprile 2006 recante disposizioni integrative e correttive: “Codice dell’Amministrazione Digitale”.
- [4] Decreto legislativo 30 giugno 2003, n. 196, “Codice in materia di protezione dei dati personali” (GU n. 174 del 29-7-2003 - Suppl. Ord. n. 123).

### 4.2 Riferimenti tecnici

Di seguito si elencano i principali standard tecnici relativi alla Carta Nazionale dei Servizi:

- [5] CNIPA, “CNS - Functional Specification Release 4b”, giugno 2005.
- [6] NK/4/FNS/T/2/1.1, “Netlink – Specifiche HPC”, v1.1, 12/09/2003.
- [7] NK/4/FNS/T/3/1.1, “Netlink – Specifiche PDC”, v1.1, 12/09/2003.
- [8] NK/4/FNS/T/4/2.0, “Dati PDC” , v2.0, 18/04/2005.
- [9] NK/4/FNS/T/21/1.1, “Gestione del Serial Number delle Carte Sanitarie”, v1.1, 01/06/2005.
- [10] ISO/IEC 7816-4:2005, “Information technology - Identification cards - Integrated circuit(s) cards with contacts - Part 4: Interindustry commands for interchange”.
- [11] ISO/IEC 7816-8:2004, “Identification cards - Integrated circuit cards - Part 8: Commands for security operations”.
- [12] ISO/IEC 7816-9:2004, “Identification cards - Integrated circuit cards - Part 9: Commands for card management”.