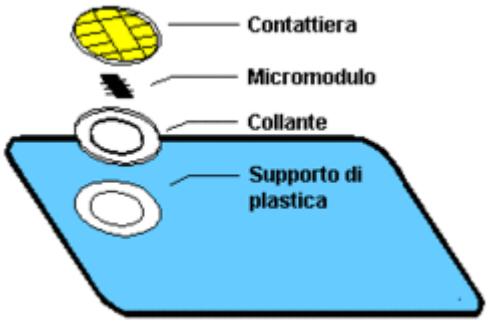
La SMART CARD: Alcune informazioni tecniche



*La smart card (**SC**) è un dispositivo hardware delle dimensioni di una carta di credito che possiede potenzialità di elaborazione e memorizzazione dati ad alta sicurezza. Più in generale, il termine smart card sottintende un insieme di tecnologie, comprendenti circuiti integrati, microprocessori, memorie RAM, ROM, EEPROM, antenne, ecc., integrate nello stesso circuito elettrico per formare un microchip che è il "cuore" della smart card.*

La smart card è costituita da un supporto di plastica nel quale è incastonato un microchip connesso ad un'interfaccia di collegamento che può essere una contattiera o un'antenna. Il microchip fornisce funzionalità di calcolo e memorizzazione dati; la contattiera o l'antenna consentono al microchip di dialogare con uno speciale terminale di lettura collegato solitamente ad un computer mediante porta seriale, parallela, USB, ecc. **[Fonte: Wikipedia]**

La SMART CARD: in Agrea

Al momento l'attivazione della SC è dedicata solo alle utenze internet allo scopo di autenticarsi al Sistema Operativo Pratiche (SOP).

Il lettore di SC deve essere già configurato, cioè integrato con il browser. **Agrea non potrà farsi carico delle eventuali problematiche tecniche di configurazione, né fornire qualsiasi supporto tecnico in questo senso (considerate le innumerevoli specificità di lettori esistenti).**

Protocollo https →SSL (Secure Sockets Layer) è un protocollo aperto e non proprietario, utilizzato per stabilire comunicazioni sicure tra un Server ed un Client.

ACCESSO STANDARD cioè senza certificato
es: l'accesso alle applicazioni regionali (cartellino, ecc.)

ACCESSO CON CERTIFICATO

La SC contiene 2 certificati: uno per operare la firma digitale e uno per l'autenticazione.

Per il rilascio del certificato è necessario rivolgersi ad una **certification autority (CA)** o Autorità Certificativa, che è un ente di terza parte, pubblico o privato, abilitato a rilasciare un certificato digitale tramite procedura di certificazione.

La **lista** delle certification autority (CA) che al momento sono accettate da Agrea sono:

- ⇨ Actalis
- ⇨ Infocamere
- ⇨ Postecert

Non è esclusa la possibilità di implementare questa lista a seguito di richieste esplicite da parte degli utenti.

Nel certificato è contenuto il CODICE UNICO DI IDENTIFICAZIONE AZIENDE AGRICOLE (CUAA) (per gli utenti internet è la username).

Il vantaggi principali di questa scelta sono:

- ⇨ **meno** burocrazia
- ⇨ **più** sicurezza

(non ci si dovrà più preoccupare della scadenza della password o della scadenza dell'utenza causa suo inutilizzo per lungo tempo; non occorre attivare la procedura di "registrazione" presso il Servizio Tecnico di Agrea)

Ovviamente il certificato dovrà essere in corso di validità e non revocato.

A monte esiste un controllo effettuato da un server regionale (criptoserver) che "verifica" i certificati (scaduti e/o revocati).

Importante! Con entrambe le modalità di accesso, le funzionalità a cui l'utente è abilitato rimangono invariate.

La SMART CARD: Requisiti necessari all'accesso

Per poter accedere utilizzando la propria smart card è necessario che:

- ⇨ la smart card contenga un certificato per l'**autenticazione client**;
- ⇨ sia installato correttamente un lettore compatibile con la smart card;
- ⇨ il browser sia configurato per l'utilizzo della smart card.

Le autorità di certificazione che rilasciano la smart card di solito forniscono anche il lettore di smart card e le istruzioni per la loro specifica configurazione sui browser più comuni: Microsoft Explorer o Mozilla Firefox.
Di seguito si riporta un esempio **generico** di configurazione che funziona con la maggior parte delle smart card e dei lettori in commercio. Consigliamo all'utente in possesso di documentazione specifica proveniente dal fornitore del lettore o della smart card, di utilizzare quest'ultima piuttosto che le istruzioni di seguito riportate.

La SMART CARD: Esempi di configurazione

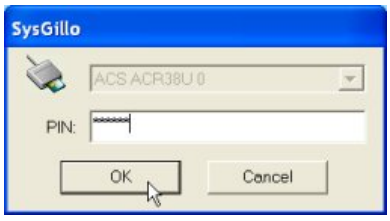
Configurazione di Internet Explorer

Importazione dei certificati di autenticazione.

1. Scaricare un software per l'importazione dei certificati; ad esempio il programma Sysgillo è scaricabile da http://sysgillo-csp-pkcs11.software.informer.com/ ; le istruzioni seguenti si riferiscono all'utilizzo di Sysgillo
2. Per estrarre i file compressi utilizzare WinZip, WinRar o altra utilità di decompressione
3. Chiudere eventuali applicazioni attive in Windows
4. Lanciare il file appena estratto e seguire le istruzioni per l'installazione
5. Una volta installato il software è necessario avviarlo per l'importazione dei certificati dalla smart card ad Internet Explorer; cliccare due volte sull'icona

6. Inserire la smart card nel lettore e cliccare su Importa

7. Digitare il codice PIN e cliccare su «OK» per importare tutti i certificati presenti sulla smart card. Se l'importazione ha avuto successo comparirà un messaggio riportante il numero di certificati importati, ad esempio:

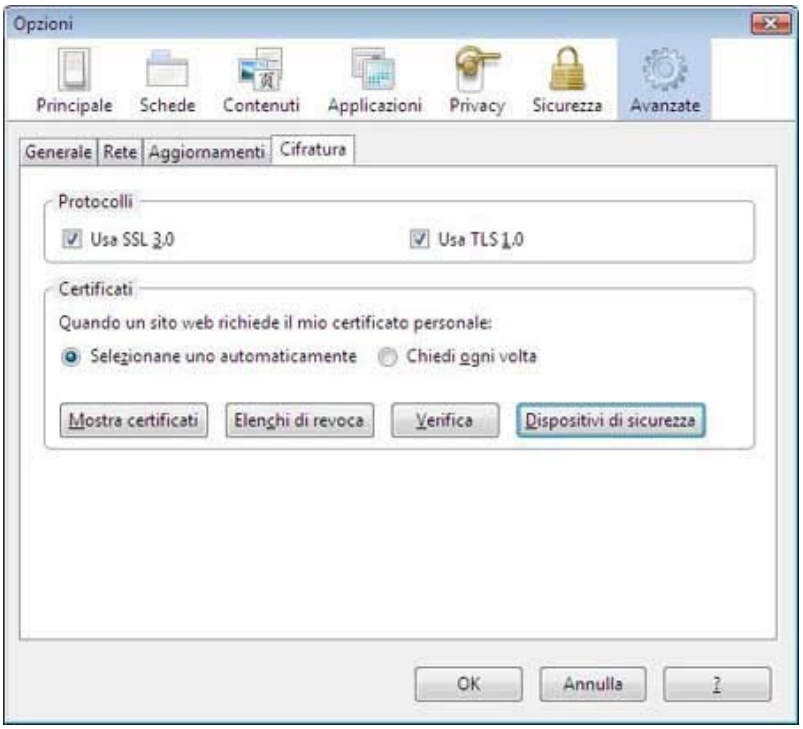


Configurazione di Mozilla Firefox

1. Aprire Mozilla Firefox

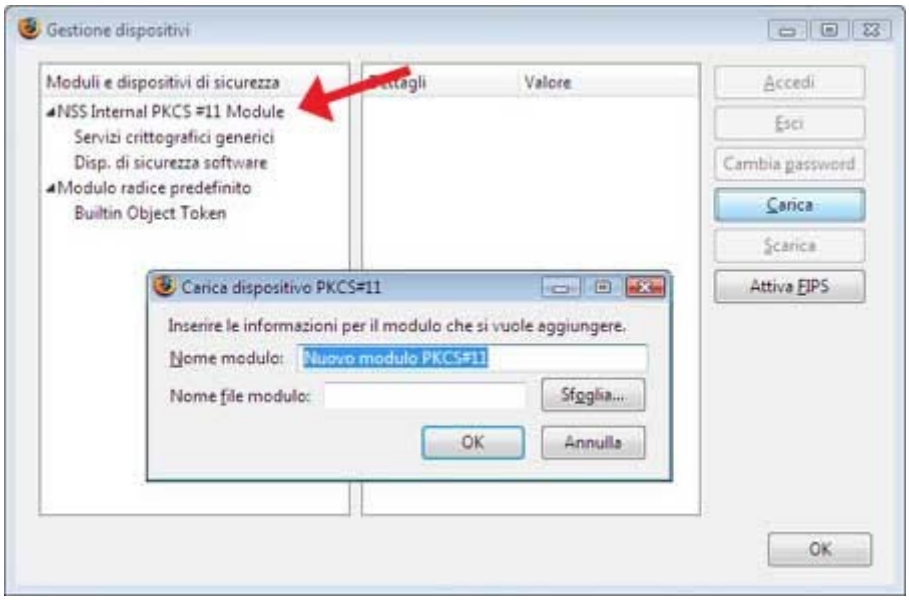
2. Scegliere da menu: Strumenti/Opzioni

3. Nella finestra "Opzioni"/Avanzate/Cifratura, verificare che sia attivata la voce "*Selezionane uno automaticamente*" e selezionare "Dispositivi di sicurezza"

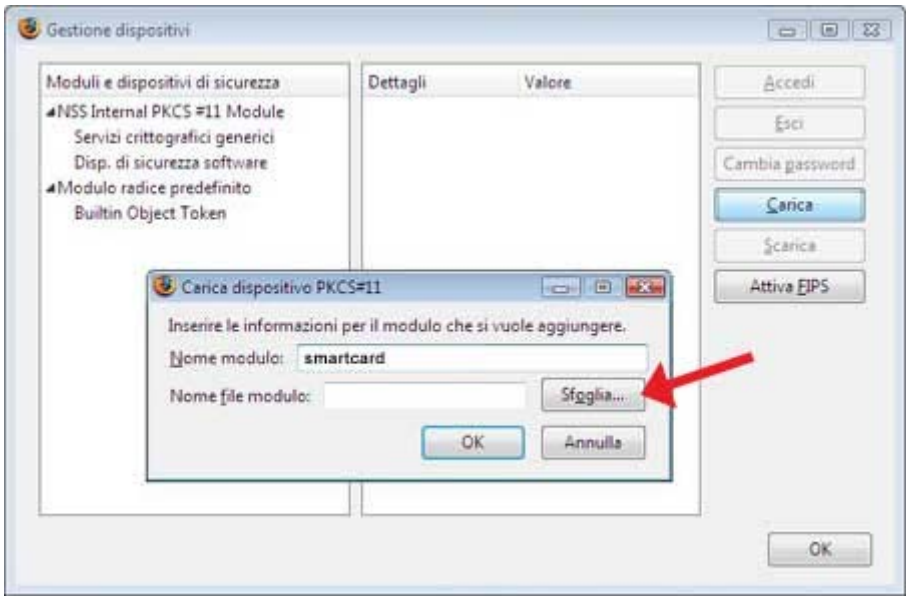


4. Nella finestra "Gestione dispositivi" selezionare a sinistra NSS Internal PKCS # 11 Module

- Premendo il pulsante **Carica** si apre la finestra "Carica dispositivo PKCS#1



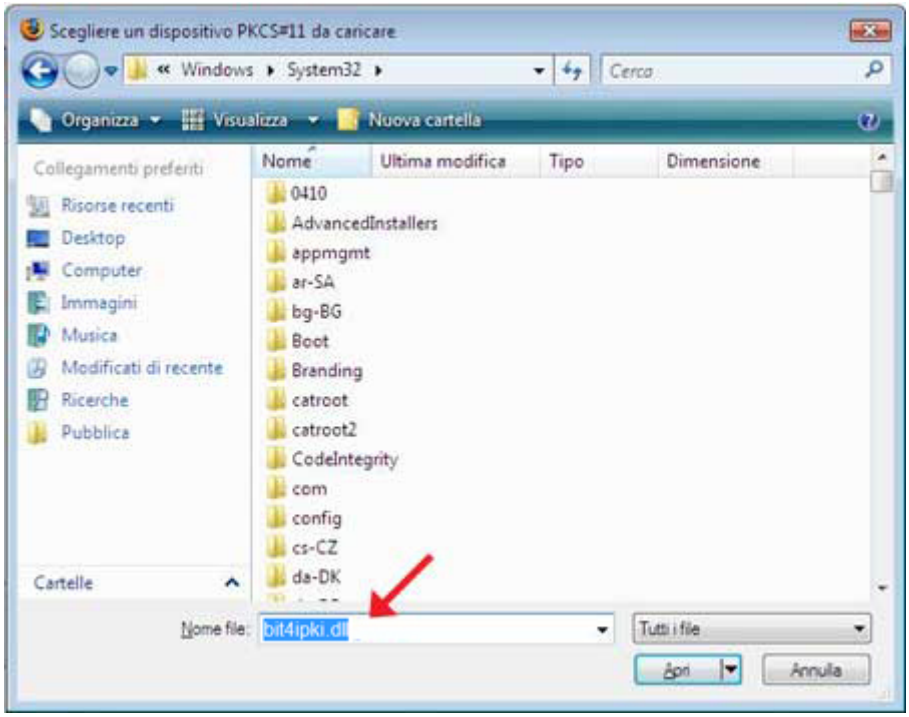
5. Nella finestra "Carica dispositivo PKCS#11", digitare nel campo "Nome modulo": **Smart Card** e premere il pulsante "Sfoglia"



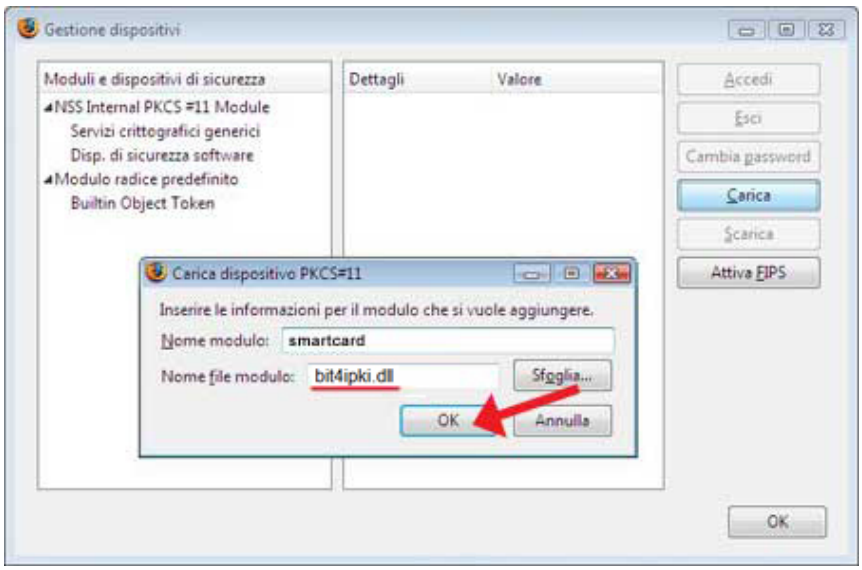
6. Selezionare il file **.dll** specifico per la propria smart card (solitamente è posizionato nella cartella di sistema di Windows, oppure in C:\windows\system32 oppure in C:\winnt\system32) e premere Apri.

Di seguito si riportano alcuni esempi di file .dll compatibili con alcune smart card (fonte *Infocert*).

- incryptoki2.dll / ipmpki32.dll per smartcard: 1201.., 1202.., 1203..,
- bit4ipki.dll per smartcard: 7420.., 1204.., 1205.., 6090..
- bit4opki.dll per smart card Oberthur: 170.., 190..
- cvP11_M4.dll per smartcard: 16..
- si_pkcs11.dll per smartcard: 1401.., 1402.., 1501.., 1502..
- cmp11.dll per smart card: 1503..



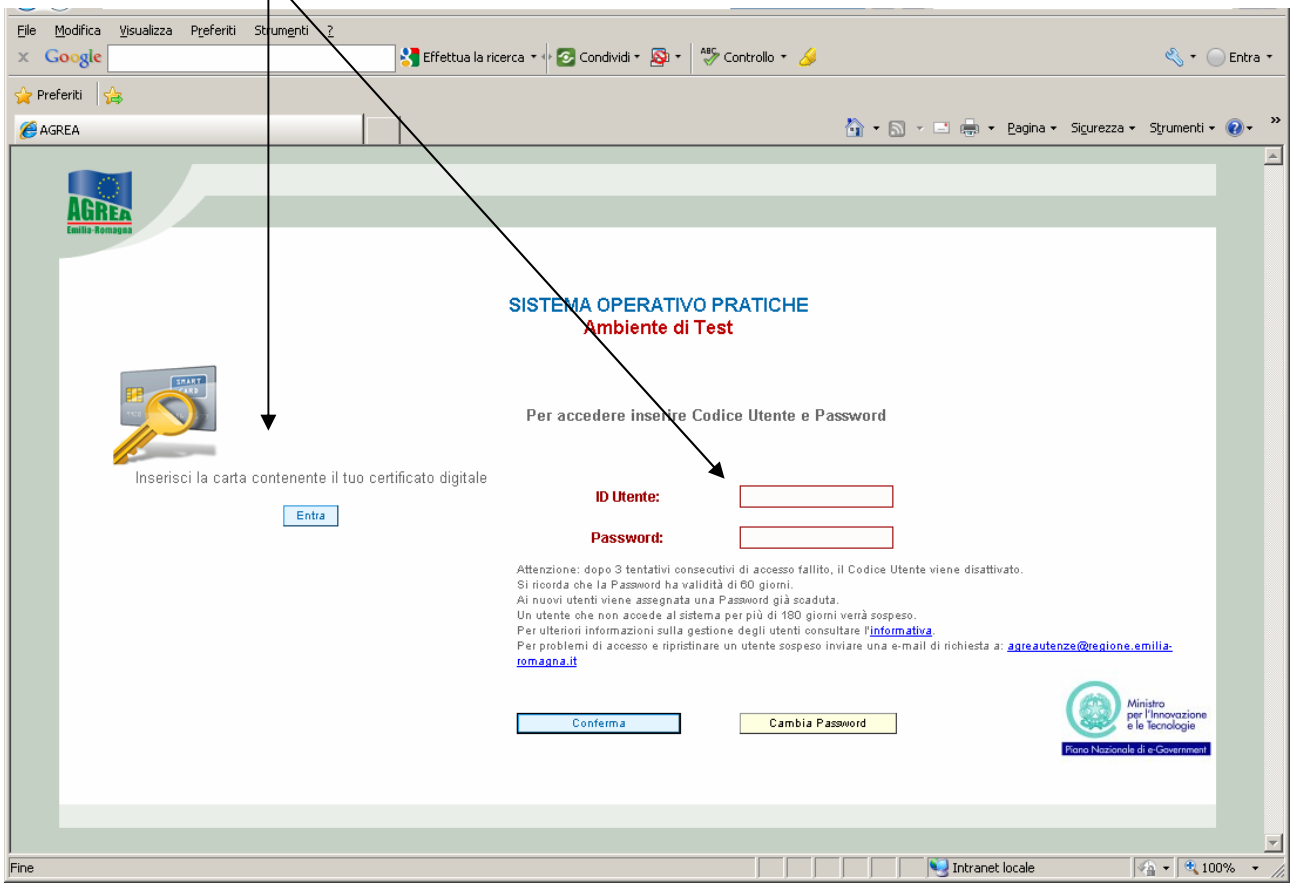
7. Nella finestra "Carica dispositivo PKCS#11" premere **OK**



La SMART CARD: L'accesso a SOP

La maschera di ingresso è la medesima con qualsiasi browser. Esiste un software di dialogo tra il browser e il certificato.

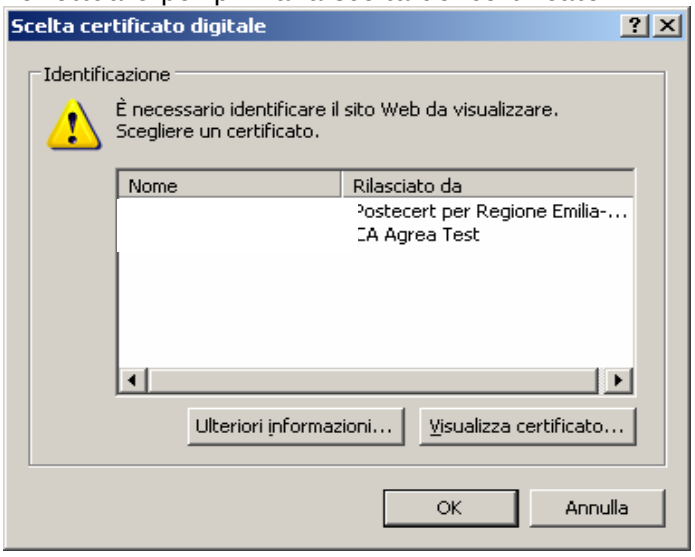
Attenzione! Le due modalità sono alternative (SC o accesso con userid+psw)



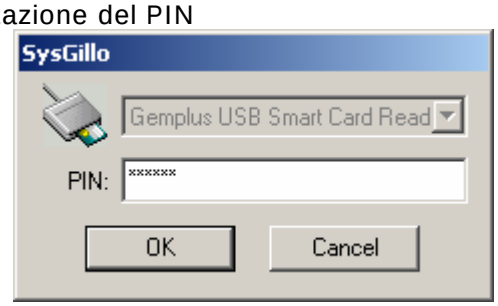
A seconda del browser utilizzato, possono presentarsi maschere diverse per i passaggi successivi.

Con **Internet Explorer** una volta cliccato sul pulsante ENTRA:

1) viene chiesto di effettuare per prima la scelta del certificato:

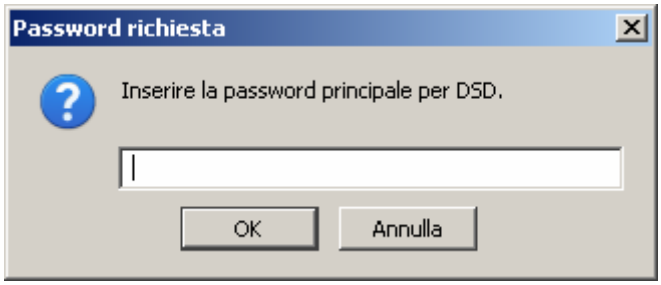


2) e successivamente l'imputazione del PIN

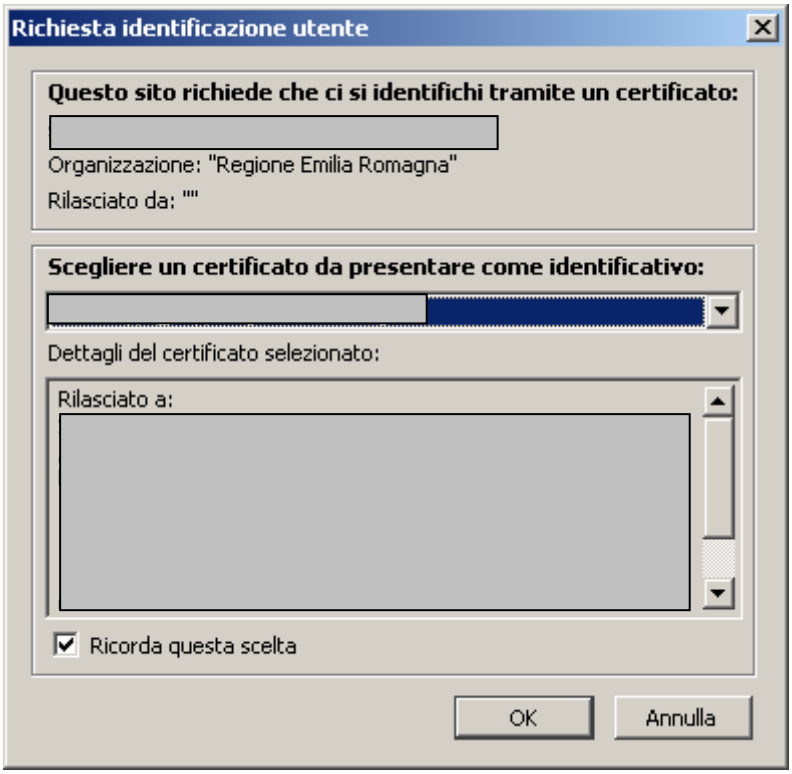


Con **Mozilla** una volta cliccato sul pulsante ENTRA:

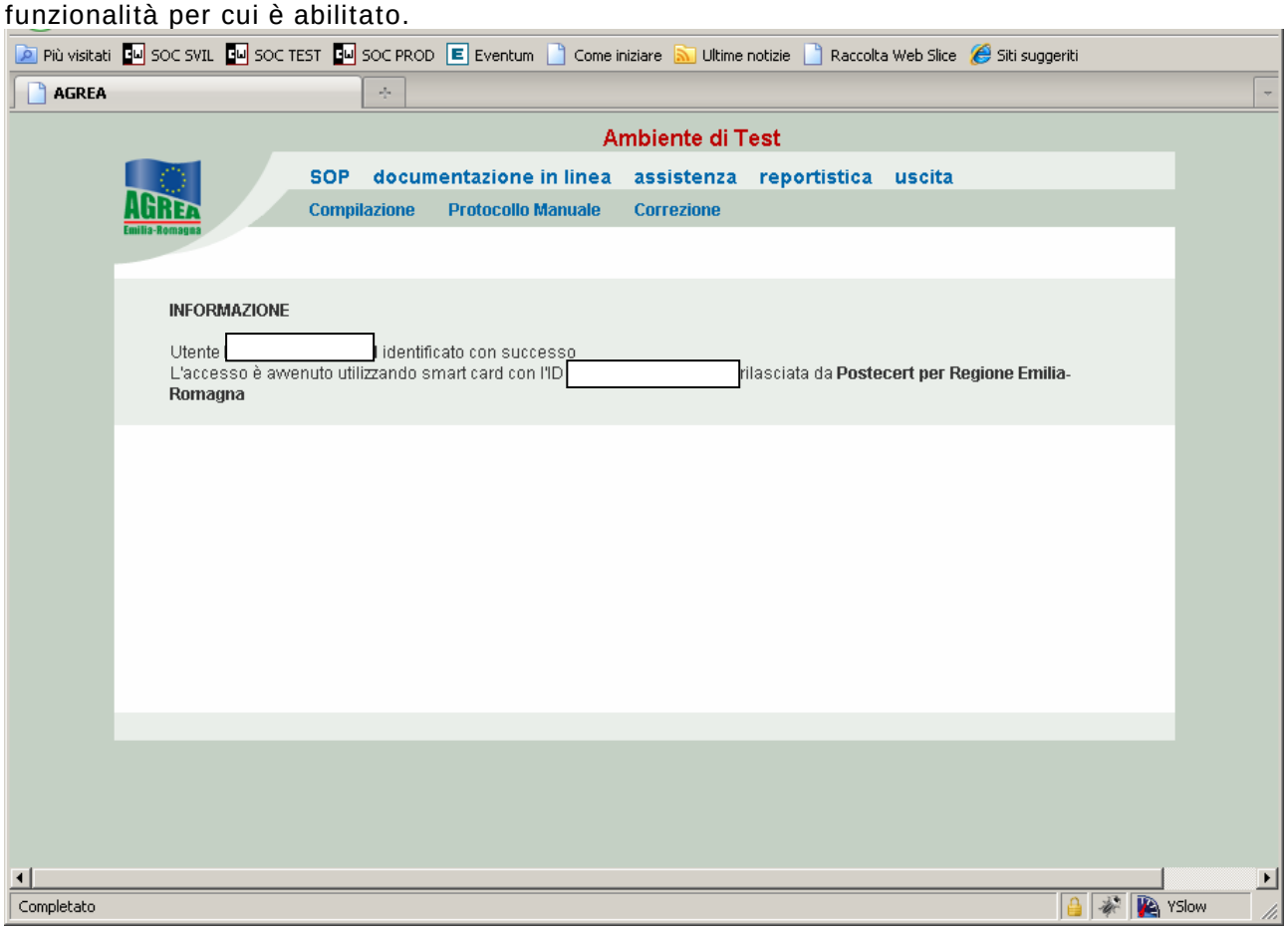
1) viene per primo richiesto il PIN



2) e successivamente la scelta del certificato



Se si tratta di un utente già in precedenza registrato e che è ricorso all'utilizzo della SC, una volta eseguiti questi passaggi si ritroverà direttamente nella maschera che prevede le funzionalità per cui è abilitato.



Se, al contrario, trattasi di un nuovo utente mai registrato prima, ai passaggi sopradescritti seguirà la fase di registrazione (non visibile all'utente) e gli si presenterà (trattandosi di primo ingresso) la maschera riferita all'accettazione *dell'informativa sul trattamento dei dati personali*.