



1 RISOLUZIONE DEI PROBLEMI ALL'ACCESSO

Prima di procedere l'utente deve verificare

- A. di aver scaricato i certificati root della CA InfoCert Servizi di certificazione
- B. di aver installato il lettore di smart-card
- C. di aver installato il programma Dike

Se al momento dell'autenticazione si riceve il messaggio "Certificato utente non trovato" i possibili errori sono i seguenti:

- 1) *La smart card non è una CNS e non contiene il certificato di autenticazione:* è necessario dotarsi di CNS con certificato di autenticazione. In particolare le smart card che hanno un codice che inizia per 1202 oppure per 1203 sono smart card che, presumibilmente, non dispongono di certificato di autenticazione.
- 2) *Il browser non legge le pagine più aggiornate di internet:* svuotare la cache del proprio browser ed impostarlo in modo da aggiornare le pagine al primo accesso (le opzioni si trovano in "Strumenti – Opzioni internet" di Internet Explorer o in "Strumenti – Elimina dati personali" di Firefox)
- 3) *E' stato digitato un pin errato o la smart card non è correttamente inserita nel lettore:* Inserire la smart card nel lettore prima di aprire il browser (Internet Explorer o Firefox)
- 4) *Il pin della smart card è bloccato:* sbloccare il pin della smart card. Per le smart card rilasciate dalle Camere di Commercio, da Infocamere o da Infocert lo sblocco del pin si effettua utilizzando il programma "Dike Util" disponibile sul sito www.firma.infocert.it nella sezione "Installazione->Software". Per le Business Key lo sblocco si effettua con la funzione "Sblocco pin" presente nel menu "Gestione pin" del "Business Key Manager"
- 5) *Il lettore non viene letto correttamente dal PC:* installare i driver più aggiornati del lettore di smart card
- 6) *Non si è configurato il proprio browser con i driver per l'utilizzo della smart card o business key:* per capire se questo è il problema bisogna verificare se tra i programmi installati sul proprio PC è presente Bit4id->Universal Middleware for Incard -> Bit4id Smart Card Manager . In questo caso è necessario seguire le istruzioni di seguito riportate e riprese dal sito <https://www.firma.infocert.it/installazione/certificato3.php> al quale si rimanda per maggiori dettagli.



La procedura di configurazione è diversa a seconda del programma utilizzato:



Internet Explorer 6.0

Per utilizzare il browser di Microsoft per la navigazione SSL è necessario installare il modulo CSP (Cryptographic Service Provider, il software indispensabile per l'importazione del certificato di autenticazione nello store Microsoft).

I moduli CSP sono diversi, a seconda del **dispositivo di firma** utilizzato, i software sono disponibili sul sito :

- per la **Business Key** fare clic su "Utilizza la BUSINESS KEY con le applicazioni del tuo PC" della voce "IMPOSTAZIONI" del menu del BK Manager
- per Smart Card con numero di serie **1202.., 1203.., 7420.., 1204.., 6090.., 1205..**, scaricare il file [KIT_CSP_1.1.15.1.zip](https://www.firma.infocert.it/software/Kit%20CSP%201.1.15.1.zip) (<https://www.firma.infocert.it/software/Kit%20CSP%201.1.15.1.zip>)
- per Smart Card con numero di serie **1601..**, scaricare il file [KIT_INSTALL_CSP_CV.zip](https://www.firma.infocert.it/installazione/zip/KIT_INSTALL_CSP_CV.zip) (https://www.firma.infocert.it/installazione/zip/KIT_INSTALL_CSP_CV.zip) e seguire le indicazioni illustrate nel file leggimi.pdf
- per Smart Card o Token USB con numero di serie **1401.., 1402.., 1501..**, il CSP viene installato con il CARDOS API 2.2.



Firefox 1.5.0.1

Per utilizzare il browser Firefox per la navigazione SSL è sufficiente configurare opportunamente il browser (vedere le istruzioni disponibili all'indirizzo

https://www.firma.infocert.it/installazione/pdf/configura_FF_1.5.0.1_SSL.pdf .



Mozilla 1.7.12

Per utilizzare il pacchetto Mozilla per la navigazione SSL e la firma della posta è sufficiente configurare opportunamente il programma vedere le istruzioni disponibili sul sito https://www.firma.infocert.it/installazione/pdf/configura_MZ_1.7.12_SSL.pdf .