Al fine di favorire la risoluzione dei più comuni problemi che si verificano nell'utilizzo del dispositivo per il riconoscimento digitale, si forniscono alcune semplici informazioni di carattere generale necessarie ad una comprensione di massima dell'argomento, seguite da alcuni semplici suggerimenti tecnici. La trattazione potrà sembrare eccessiva, ma va considerato che si tratta di acquisire la minima conoscenza di una tecnologia che è iniziata non meno di otto anni fa.

Introduzione

Il "Codice dell'Amministrazione Digitale" (CAD), fin dalla sua nascita (*2005*), definisce anche le modalità per l'erogazione di "Servizi in Rete".

In particolare, l'art. 64. "*Modalità di accesso ai servizi erogati in rete dalle pubbliche amministrazioni*" al comma 1, si fissa che "*La carta d'identità elettronica* (CIE) *e la carta nazionale dei servizi* (CNS) *costituiscono strumenti per l'accesso ai servizi erogati in rete dalle pubbliche amministrazioni per i quali sia necessaria l'identificazione informatica*".

Saltando l'aspetto normativo, per il cui approfondimento si rimanda alla lettura dei documenti reperibili nel sito http://www.FunzionePubblica.gov.it e http://www.DigitPA.gov.it, possiamo affermare che il riconoscimento digitale (informatico) dell'identità di una persona, avviene leggendo i dati contenuti nel certificato d'identità elettronico che si trova all'interno di una CNS o di una CIE. Questo certificato d'identità, è noto come "**certificato di autenticazione**".

Ora, è bene considerare che nell'uso comune degli strumenti di "***firma digitale***" si è diffuso in primis il concetto di "***Smart Card***", proprio con questa associazione rigida, come se un termine fosse sinonimo dell'altro, ovvero "Smart Card = Firma Digitale".

Successivamente abbiamo visto l'arrivo del "***Token USB***" come evoluzione della SmartCard, in quanto strumento "portabile" perché non necessita di un lettore di Card installato sul PC.

Infine, sono seguite varie evoluzioni del TokenUSB, note con nomi commerciali tipo *"BusinessKey", "ArubaKey", "PosteKey", "BusinessWay", "ActalisOne", ecc.* rimanendo sostanzialmente dei "Token USB" più evoluti.

Dobbiamo considerare quindi che in senso generale, il termine "***Smart Card***", sintetizza anche se impropriamente, tutto il mondo dei dispositivi di firma digitale.

In realtà, "*SmartCard*" o "*TokenUSB*" sono semplicemente dei supporti fisici necessari per trasportare i certificati digitali rilasciati da un "*Certificatore Qualificato accreditato presso DigitPA*".

I certificati digitali possono essere di vari tipi, in funzione della loro destinazione d'uso. Come esposto all'inizio, per il riconoscimento digitale (informatico) dell'identità di una persona, serve un certificato di "**autenticazione**", mentre per firmare un documento serve un certificato di "**sottoscrizione**".

Queste due tipologie di certificati esistono fin dalla nascita delle prime Smart Card, ma all'inizio le prime applicazioni della Smart Card, erano quasi esclusivamente orientate alla sottoscrizione digitale di documenti, ovvero all'applicazione della firma elettronica. Ancora oggi, moltissimi dispositivi di firma digitale (Card o Token) contengono solo il certificato per la sottoscrizione, e pertanto questi dispositivi non possono essere utilizzati per il riconoscimento elettronico perché prive del certificato di autenticazione.

Solo con l'avvento della CNS (o della CIE), i Certificatori Qualificati hanno iniziato a distribuire regolarmente Smart Card (o Token USB) contenenti entrambi i certificati. Per un discreto periodo prima dell'arrivo della CNS, il certificato di autenticazione veniva rilasciato su richiesta.

Informazioni Tecniche

Per poter utilizzare i certificati digitali contenuti nella Smart card (o nel Token) è necessario che il computer utilizzato sia stato configurato opportunamente.

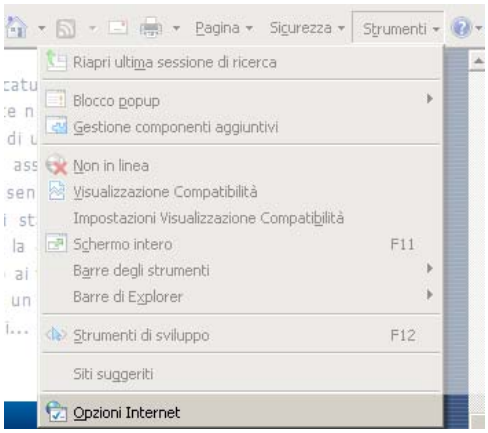
Generalmente, ogni azienda distributrice di questa tecnologia, offre tutto il supporto necessario per il corretto utilizzo/funzionamento dei propri strumenti.

In questo ambito affronteremo principalmente le problematiche connesse all'operazione di autenticazione informatica.

Se si utilizza una Smart Card di tipo classico che per essere utilizzata richiede un lettore collegato stabilmente al computer, allora è necessario aver preventivamente installato e collaudato il corretto funzionamento del lettore seguendo le indicazioni fornite dal costruttore.

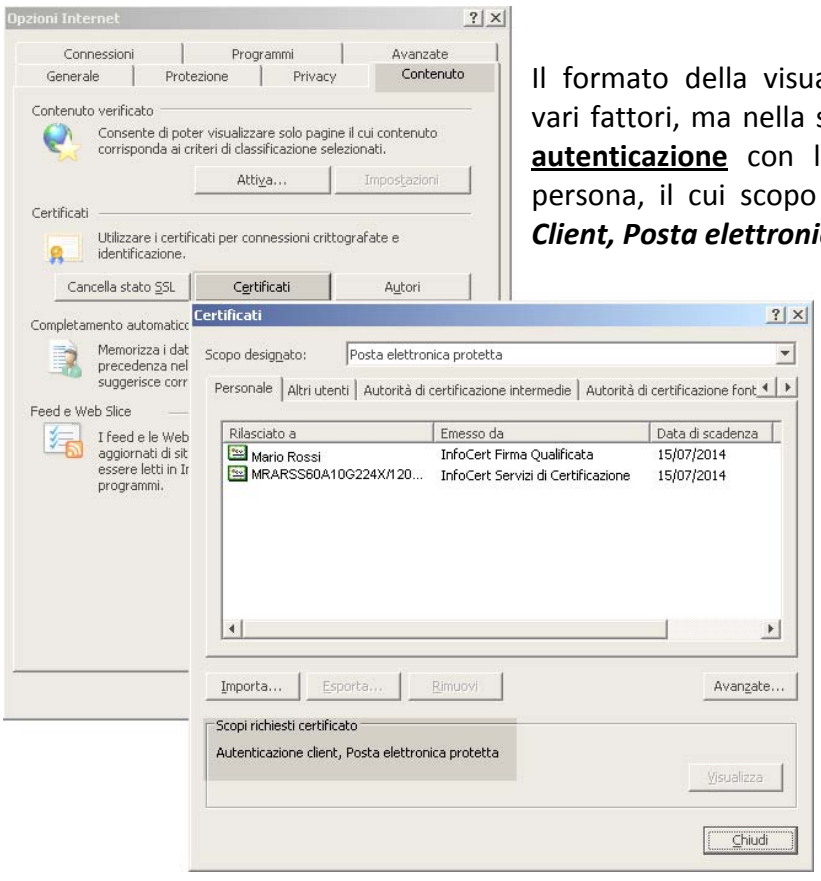
A questo punto, sia per Smart Card che per i Token (*e le varie Keys*) è necessario verificare l'esistenza dei certificati all'interno del dispositivo utilizzato.

Per far questo ci sono vari modi, ad esempio, utilizzando il browser Microsoft Internet Explorer che è certamente presente in un PC dotato di sistema operativo Microsoft Windows, Selezionando la voce "**Strumenti**" e quindi "**Opzioni Internet**"



Dal pannello "Opzioni Internet", selezionare la voce "**Contenuto**" e quindi il pulsante "**Certificati**".

Tra i vari certificati che potranno apparire nell'elenco, dovremmo identificarne almeno due con l'identità del soggetto al quale è stata rilasciata la Smart Card (o il Token).



Il formato della visualizzazione potrebbe dipendere da vari fattori, ma nella sostanza, troveremo il certificato di **autenticazione** con l'evidenza del codice fiscale della persona, il cui scopo designato riporta "***Autenticazione Client, Posta elettronica protetta***"

Tra gli altri certificati visualizzati prestiamo attenzione solo al certificato che si distingue per l'evidenza del Nome e del Cognome del soggetto al quale è stato rilasciato, in quanto si tratta "*normalmente*" del certificato di **sottoscrizione**.

In questo contesto, cogliamo l'occasione per verificare la data di scadenza dei certificati !!!

Questa semplice verifica, effettuata ovviamente con la Smart Card (*o il Token*) inseriti, non richiede la digitazione di alcun PIN e ci consente di appurare (*in modo quasi completo*) il corretto funzionamento del dispositivo e della configurazione del computer.

Per completare la verifica, chiudiamo i pannelli precedentemente aperti, rimuoviamo la Smart card dal lettore, o il Token dalla porta USB e riproviamo ad accedere al pannello "Certificati" nella stessa modalità vista in precedenza.

Nella "quasi" totalità dei casi, i due certificati visti in precedenza dovrebbero essere scomparsi. Questo è un indice di buon funzionamento del sistema, in quanto l'attuale tendenza consiste nel mostrare i certificati solo quando la Smart Card (*o il Token*) sono inseriti.

A questo punto, non rimane che provare l'accesso, con la Smart Card inserita, in un sito web qualsiasi che richieda l'autenticazione mediante certificato digitale. Le Scrivanie telematiche del sito www.Fgas.it richiedono questa modalità di accesso.

Autenticazione mediante Smart Card

L'accesso autenticato avviene in modo abbastanza semplice secondo il seguente protocollo:

1. Il server che ospita il portale web al quale si desidera accedere (https://scrivania.fgas.it nel ns. caso) conosce l'identità di tutti i "*Certificatori Qualificati accreditati presso DigitPA*", in quanto questi soggetti hanno consegnato a DigitPA una copia del certificato digitale che ha dato origine a tutti i certificati emessi in seguito. Solo per intenderci, il padre di tutti i loro certificati.
2. Quindi, il server invia la richiesta al browser con il quale l'utente sta accedendo ad internet, di "esporre" i certificati di identità "utili" per l'autenticazione. I certificati "utili" sono quelli emessi dai "*Certificatori Qualificati accreditati presso DigitPA*" ***non scaduti alla data !***
3. Il Browser interroga il computer chiedendo di mostrare i certificati "utili" (*in modo analogo a quanto fatto in precedenza per la verifica*).
4. L'utente sceglie dall'elenco visualizzato "l'identità desiderata"
5. Il browser accetta il certificato selezionato, e (quando necessario) interagisce attraverso il PC con la Smart card (o con il Token) per eseguire la richiesta del PIN che autorizza la transazione.
6. Il browser per la navigazione in internet risponde al server con i dati del certificato selezionato e si avvia la conversazione su canale sicuro (SSL) e cifrato (con le chiavi digitali scambiate).

Chiaramente stiamo semplificando il processo, ma nella sostanza con questi pochi passaggi si conclude l'autenticazione digitale.

Suggerimenti per la risoluzione di problemi comuni

Se in questi pochi passaggi qualcosa non dovesse funzionare correttamente, l'utente si ritrova con un messaggio di errore generico che richiama tutte le possibile cause, perché il processo di autenticazione non offre molti appigli per favorire una diagnostica di buon livello. Vediamo quindi cosa potrebbe non funzionare e perché.

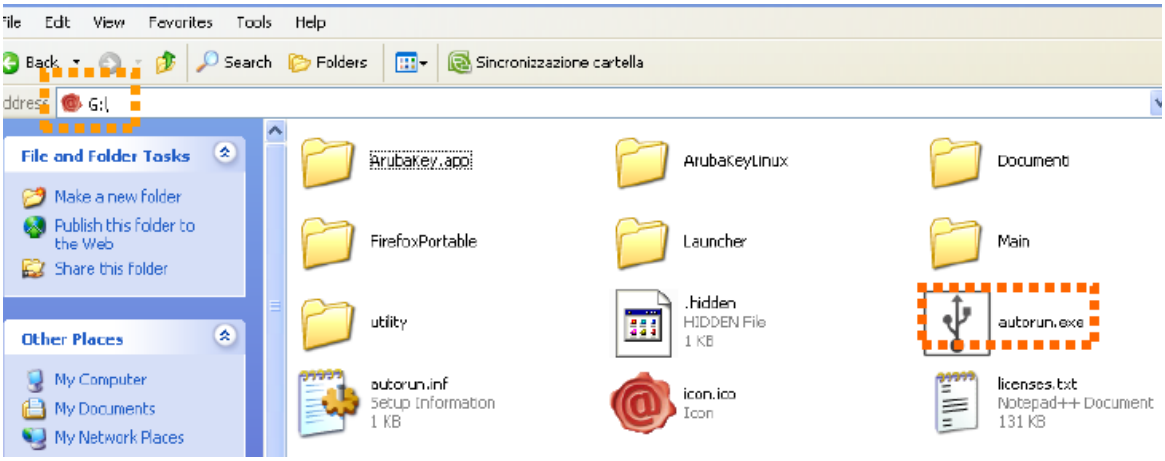
Se il problema inizia già dalla lettura dei certificati secondo le modalità descritte in precedenza, è necessario verificare che il collegamento tra il computer utilizzato e la Smart Card, o il Token USB, avvenga correttamente.

Se si tratta di Smart Card con lettore separato, oppure di di Token USB "semplice" e quindi NON di una "Business Key" evoluta (*generalmente si tratta dei primi Token distribuiti spesso privi della funzione di memory drive*), è necessario verificarne il corretto funzionamento come dichiarato dal costruttore, eventualmente recuperando i driver di sistema forniti dal costruttore, e prestando attenzione alla compatibilità con le nuove generazioni di sistemi operativi a 64 bit.

Se si tratta di un Token USB "evoluto" ovvero di una "Business Key" o simili di nuova generazione, è necessario verificare che il software contenuto sia integro ed aggiornato correttamente, ed inoltre che sia stato "avviato" all'atto dell'inserimento nella porta USB.

Infatti, questi dispositivi si presentano normalmente come delle "Pen Drive" e nella directory principale contengono un programma eseguibile di nome "**autorun.exe**" che il sistema avvia automaticamente quando rileva la presenza del dispositivo.

Poiché molti computer per motivi di sicurezza, bloccano l'avvio automatico dei programmi provenienti da dispositivi esterni, è necessario che l'utente forzi manualmente l'esecuzione di "**autorun.exe**". In tal caso, visualizzare il contenuto del Token ed avviare il file autorun.exe come indicato nella figura seguente.



Quindi, automaticamente dopo l'inserimento del Token USB, oppure dopo l'avvio manuale di "autorun.exe", comparirà una barra comandi del tipo seguente, oppure una finestra o un popup, le cui forme e contenuti dipendono dalle scelte fatte dal fornitore del servizio.

"Non entriamo volutamente nel merito di questi strumenti, in quanto sono sempre accompagnati da ampia documentazione, e di adeguato supporto all'utilizzo".

NOTA **Questi dispositivi di ultima generazione presentano una serie di servizi già configurati per un corretto funzionamento autonomo, senza dover utilizzare il software installato sul PC. Attenzione però che non è possibile utilizzare il browser internet installato sul PC se prima non si eseguono delle opportune operazioni di configurazione** (vedi guide operative).

Nell'ipotesi che l'utente desideri utilizzare il software installato sul proprio computer e non quello disponibile nella chiavetta USB, proseguendo nella risoluzione del problema, se a questo punto ancora non riusciamo a vedere i certificati nella modalità descritta in precedenza, è evidente che abbiamo già individuato un primo problema connesso al non corretto funzionamento o alla

mancanza assoluta della componente denominata **CSP** (*Cryptograpic Service Provider*) che (*grossolanamente*) ha il compito di far comunicare i servizi in esecuzione sul computer con i certificati contenuti nella Smart Card.

Questo problema viene identificato anche come la mancanza dell'importazione dei certificati nello storage del sistema.

La lettura dei certificati dal dispositivo esterno, viene anche identificata come "**importazione**" degli stessi nel computer.

Dobbiamo però precisare che, nonostante vi siano molteplici modalità di esportazione/importazione di chiavi e certificati, **sconsigliamo** di avventurarsi in operazioni "sofisticate" (*delle quali non parleremo*) che all'utente inesperto potrebbero apparire come validi percorsi alternativi.

Raccomandiamo invece di seguire le indicazioni fornite dai rispettivi "*Organismi di certificazione*" ovvero dalle aziende che hanno rilasciato/commercializzato il dispositivo digitale. Pertanto si raccomanda sempre di consultare la specifica guida operativa.

L'importazione dei certificati, ovvero l'installazione del CSP, può avvenire in diverse modalità, dipendenti dal tipo di dispositivo utilizzato oltre che dal sistema operativo del computer.

Ad esempio, i dispositivi digitali distribuiti dalle Camere di Commercio sono distribuiti da ***InfoCamere Scpa*** *la quale si è avvalsa per un lungo periodo della tecnologia fornita da* ***InfoCert****.*

Pertanto, per i dispositivi di recente emissione, è possibile accedere al canale di supporto attraverso il link: http://www.card.infocamere.it/infocamere/pub/installazione_2702

Mentre per i dispositivi rilasciati in precedenza, oppure per quanto distribuito da InfoCert, il supporto necessario si trova al link: https://www.firma.infocert.it/installazione/certificato3.php

Proseguendo con la risoluzione del nostro problema, supponendo che si disponga di una "CNS" rilasciata recentemente da una CCIAA, si deve scegliere la voce "***Utilità***" e quindi la voce "***Importa Certificato***". In realtà, in questo modo il sistema avvierà la procedura per l'installazione del CSP.

1. scegliere la voce "***Utilità***"

2. scegliere la voce "***Importa Certificato***"

In questo caso vedremo avviarsi l'installazione del prodotto "***Bit4Id***" .

Per questa operazione di installazione è fondamentale assicurarsi di disporre dei privilegi amministrativi sul computer, ed assicurarsi che non si generino conflitti con prodotti analoghi precedentemente installati, anche se compatibili con altri tipi di Smart Card o di Token USB.

Per i dettagli vedere a pagina 32 del manuale *TokenUsb_guida_rapida.pdf* reperibile al seguente indirizzo http://www.card.infocamere.it/infocamere/FileDocManager/download?file=/TokenUsb_guida_rapida.pdf

E' necessario tenere presente che il CSP (*quale esso sia*) è sempre necessario per il servizio di autenticazione mediante certificato digitale. Terminata l'installazione del CSP, generalmente è necessario riavviare il computer.

A questo punto, il problema che ci impediva di poter vedere i certificati installati nel nostro computer dovrebbe essere stato risolto. Ciò nonostante, potremmo incontrare ancora delle difficoltà nell'esecuzione della procedura di autenticazione, e vediamo nel seguito come poter diagnosticare/risolvere i vari problemi.

Chiaramente, nella seguente trattazione, si considera correttamente superato il test precedente, e che il programma "autorun.exe" sia stato eseguito (*o in modo automatico o manualmente*) quando si utilizza un Token USB di nuova generazione.

Il server che ospita il portale web al quale dobbiamo accedere **deve** conoscere l'identità di tutti i "*Certificatori Qualificati accreditati presso DigitPA*".

Se per qualche motivo il Certificatore non ha ancora trasmesso a DigitPA la copia del certificato padre (***RootCA***) dal quale sono stati prodotti i nuovi certificati destinati agli utenti, oppure se il server "*FGAS*" non ha ancora prelevato da DigitPA questo nuovo "***RootCA***", si ottiene l'errore di "***CERTIFICATO NON TOVATO***" oppure all'apertura dell'elenco dei certificati "utili" si presenta un box completamente vuoto, oppure si ottiene un messaggio di errore generico nell'accesso con smart card.

Il tipo di segnalazione può dipendere anche dal Browser internet utilizzato e dal CSP installato.

Questo succede generalmente con certificati digitali di recente emissione. Per accertarsene è necessario interagire con l'Ente Certificatore che ha rilasciato il certificato.

Oppure …

"… il problema deriva dalla non corretta installazione o avvio del modulo CSP"

Oppure …

"… il problema deriva dalla data di scadenza del proprio certificato come visto in precedenza"

Oppure …

"… il problema deriva dalla errata impostazione della data del proprio computer, tale da falsare la finestra temporale di validità dei certificati"

Oppure …

"… il problema deriva dalla mancanza di un certificato utile per l'AUTENTICAZIONE"

(sono tutti aspetti che avremmo già dovuto escludere)

1. Il Browser interroga il computer chiedendo di mostrare i certificati "utili".
2. L'utente sceglie dall'elenco visualizzato "l'identità desiderata"

Ma non appare alcuna richiesta di indicazione del PIN, e il sistema ci porta su una pagina di errore generico del tipo "***404 - PAGINA NON TROVATA***".

In questo caso, generalmente si tratta della mancanza o non corretto avviamento del modulo CSP, generalmente coincidente ad una importazione del certificato eseguita in modo "errato"!

Ammesso che la configurazione sia stata testata correttamente come descritto sopra (!?), il problema potrebbe dipendere da un "inceppamento" della sessione SSL, probabilmente dovuto alla chiusura di una precedente sessione che per qualche motivo risulta essere ancora persistente.

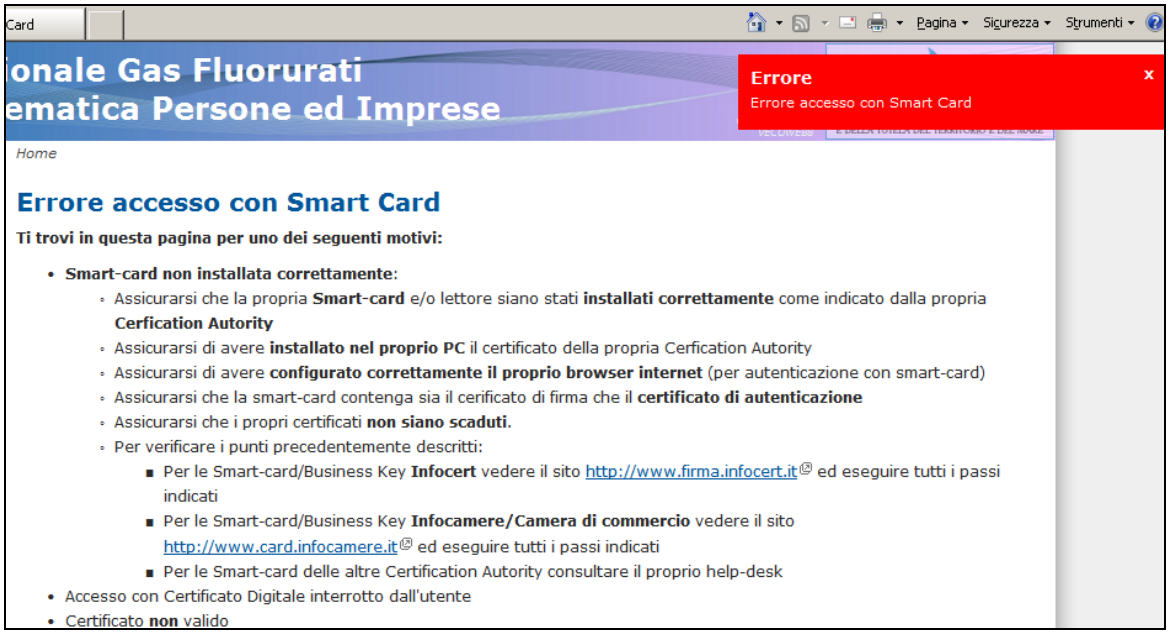
In questo caso sarà sufficiente chiudere tutte le finestre aperte dal browser internet, ma anche eventuali documenti aperti direttamente da link sul web, e possibilmente cancellare i file

temporanei lasciati dalle precedenti navigazioni in internet, ed in ultima analisi, riavviare il computer.

Oppure …

3. Il browser accetta il certificato selezionato ed esegue la richiesta del PIN che autorizza la transazione.

E' abbastanza improbabile che a questo punto si verifichino degli errori, ma se non dovesse apparire la pagina desiderata del portale "*F-GAS*", e il sistema ci dovesse portare su una pagina di errore generico come la seguente, è probabile che il CSP installato non sia esattamente compatibile con il tipo di dispositivo utilizzato.

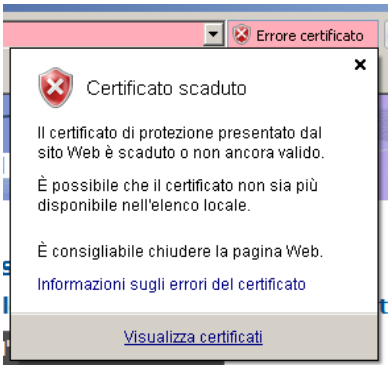


Riepiloghiamo le considerazioni fatte in precedenza, cercando di dare un ordine progressivo agli eventi ed alle soluzioni.

1. Cercando di accedere alla scrivania telematica vengo indirizzato ad una pagina generica dove leggo "Si è verificato un problema con il certificato di protezione del sito Web"

Scegliendo di continuare, appare la pagina FGAS, ma il browser segnala un "**Errore Certificato**" a destra della barra di navigazione, dove "normalmente" dovrei vedere il lucchetto. 

Selezionando "*Errore Certificato*" appare il messaggio di "Certificato scaduto".



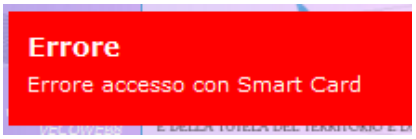
Causa: Il certificato del server è veramente scaduto, oppure la data impostata sul proprio computer è errata.

Soluzione: Correggere l'impostazione della propria data, chiudere il browser internet e ricollegarsi.

2. Riesco ad accedere fino alla pagina di accesso alla Scrivania Telematica FGAS,

ma quando accetto le Informazioni sulla Privacy, vengo indirizzato ad una pagina di errore generico dove leggo:

"Errore accesso con Smart Card"



Cause / Soluzioni possibili

Causa 1: La Smart Card non contiene un certificato utile per l'AUTENTICAZIONE, ma solo per la Sottoscrizione. "*Questa card l'ho sempre utilizzata per firmare documenti, ma non per le operazioni di autenticazione informatica*".

Soluzione 1: Devo richiedere al mio fornitore di servizi, o alla mia CCIAA l'emissione di un certificato utile all'autenticazione, oppure richiedere direttamente una nuova card di tipo CNS. La CNS (Carta Nazionale dei Servizi) contiene "d'ufficio" i due certificati necessari (sottoscrizione & autenticazione) ma si raccomanda comunque di specificare il fabbisogno nella richiesta.

Causa 2: La Smart Card contiene il certificato per l'AUTENTICAZIONE, ma questo risulta essere scaduto (*vedi data validità "fino al"*)

Soluzione 2: Controllo che l'impostazione della data nel mio computer sia esatta. Se la data è corretta, controllo la data di scadenza del certificato di autenticazione (*come ? … vedi sopra !*) Se il certificato è scaduto, devo richiedere al mio fornitore di servizi, o alla mia CCIAA il rinnovo del certificato, oppure l'emissione di un nuovo certificato utile all'autenticazione, oppure richiedere direttamente una nuova card di tipo CNS.

Causa 3: La Smart Card contiene il certificato valido per l'AUTENTICAZIONE, e questo è stato rilasciato recentemente da un "*Certificatore Qualificato accreditato presso DigitPA*" che non ha ancora trasmesso a DigitPA il nuovo certificato "padre o radice" (**RootCA**), oppure DigitPA non lo ha ancora reso pubblico, oppure il Server F-GAS non lo ha ancora recepito. (*Oppure il certificatore che ha prodotto il certificato NON è qualificato presso DigitPA*).

Soluzione 3: Inviare una mail all'indirizzo assitenza@fgas.it chiedendo un ricontatto, possibilmente allegando la copia della parte pubblica del certificato, oppure una stampa delle proprietà dello stesso. E' anche possibile accedere direttamente agli elenchi pubblicati da DigitPA (http://www.digitpa.gov.it/certificatori_firma_digitale o http://www.digitpa.gov.it/carta_nazionale_servizi) e verificare di persona la presenza del Certificatore, ma questa operazione non garantisce il corretto accertamento dell'esistenza del nuovo certificato "***RootCA***" (*serve una discreto livello di conoscenza*)

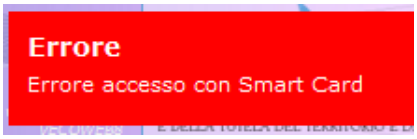
Causa 4: La Smart Card contiene il certificato valido per l'AUTENTICAZIONE, e tutte le casistiche precedenti sono state verificate e validate. Ma il CSP potrebbe non essere stato installato o non funzionare correttamente. Banalmente possiamo dire che "*il browser non è configurato correttamente per l'autenticazione digitale*".

Soluzione 4: Rileggere dall'inizio questo documento, e verificare che tutte le operazioni di controllo siano andate a buon fine. Quindi se il problema persiste, verificare che non ci siano altri prodotti con funzionalità analoghe o versioni precedenti non rimosse correttamente, in conflitto

con il dispositivo utilizzato. (*brevemente: certificati importati; CSP installato; Key attivata con autorun.exe*)

2. Riesco a superare la pagina di accesso alla Scrivania Telematica FGAS, accettare le Informazioni sulla Privacy, e digitare il PIN di identificazione, ma subito dopo vengo indirizzato ad una pagina di errore generico dove leggo:

"Errore accesso con Smart Card"



Causa **:** "quasi certamente" il CSP non è stato installato correttamente, o si tratta di un CSP non idoneo per il tipo di dispositivo utilizzato. Banalmente possiamo dire che "*il browser non è configurato correttamente per l'autenticazione digitale*".

Soluzione : Rileggere dall'inizio questo documento, e verificare che tutte le operazioni di controllo siano andate a buon fine. Quindi se il problema persiste, verificare che non ci siano altri prodotti con funzionalità analoghe o versioni precedenti non rimosse correttamente, in conflitto con il dispositivo utilizzato.

** NOTA IMPORTANTE **

In questo contesto non abbiamo affrontato volutamente alcun aspetto connesso all'utilizzo di browser internet diversi da quanto "naturalmente" già installato su PC dotati di sistema operativo Microsoft Windows, perché l'obiettivo di questo documento consiste nel fornire un supporto all'orientamento dell'utente, nella risoluzione dei problemi connessi all'autenticazione digitale.

Ogni aspetto tecnico peculiare dei vari dispositivi digitali oltre che dei vari browser per la navigazione in internet, sono adeguatamente affrontati e spiegati nei manuali operativi che ciascun fornitore di certificati digitali rende disponibili ai propri utenti, anche con canali diretti di assistenza telefonica competente, ai quali consigliamo di rivolgersi per la risoluzione di questi problemi.