# **CERTIFICATI DIGITALI Explorer**

I Certificati Digitali sono preinstallati nella maggior parte dei browser, il loro riconoscimento ed i conseguenti messaggi che vengono mandati a video dipendono dal tipo di browser che viene utilizzato. È utile per l'utente conoscere alcune informazioni sul funzionamento del proprio browser per poter valutare con maggiore chiarezza le situazioni che gli si presentano.

È consigliato non utilizzare versioni di explorer inferiori alla 5.00.29, inoltre è opportuno tenere presente che dalla versione 5.5 il livello di sicurezza è maggiore in quanto la cifratura dei dati nel protocollo SSL è a 128bit.

Explorer 5.0, 5.5 e 6.0 hanno una sezione in cui è possibile verificare il tipo di certificati installati: cliccare su "STRUMENTI" nella barra di menù e scegliere "OPZIONI INTERNET", cliccare su "CONTENUTO".

Vi appare una finestra come questa:

Restriz	ioni d'accesso	
8	Permettono di controllare il contenuto delle pagine Internet che possono essere visualizzate sul computer.	
	Attiva Impostazioni	
- Certific	ati	
	Usare i certificati per identificare in modo univoco se stessi, autorità di certificazione e autori.	
	Certificati Autori	
– Informa	azioni personali	
¢	Completamento automatico memorizza i dati immessi in precedenza e suggerisce corrispondenze.	
	Microsoft Profile Assistant memorizza le <u>Profilo</u> informazioni personali.	

A questo punto cliccare sul pulsante "CERTIFICATI...", vi appare una finestra con diverse sezioni dove sono elencati tutti i certificati installati sul vostro browser.

**Explorer 4.0** è leggermente diverso, le informazioni sui certificati si trovano cliccando su "VISUALIZZA" nella barra di menù e scegliendo "OPZIONI INTERNET"

È opportuno impostare alcune opzioni perché il browser si comporti correttamente: sempre nella sezione "OPZIONI INTERNET" cliccare questa volta su "AVANZATE", scorrere con la barra fino a "PROTEZIONE", appare una finestra come questa:

pzioni Internet
Generale Protezione Contenuto Connessioni Programmi Avanzate
Impostazioni:
Protezione
Avvisa in caso di certificati di siti non validi
Avvisa se la sottoscrizione delle schede viene reindirizzata
Non salvale pagine chilografiate su disco
Verifica revoca dei certificati del server (sarà necessario riavviare il computer)
Verifica revoca dei certificati dell'autore
Ricerca dalla barra degli indirizzi
Q Durante la ricerca
<u>R</u> ipristina predefinite
OK Annulla <u>Applica</u>

Nell'immagine sono indicate le opzioni minime da spuntare: Attiva Profile Assistant, Avvisa in caso di certificati di siti non validi, Avvisa se la sottoscrizione delle schede viene reindirizzata, Usa Fortezza, Usa SSL 2.0, Usa SSL 3.0, Verifica revoca dei certificati del server (sarà necessario riavviare il computer), Verifica revoca dei certificati dell'autore. Ognuno può, a propria discrezione, aggiungere le altre opzioni aumentando il livello di protezione.

Anche in questo caso **Explorer 4.0** presenta delle opzioni leggermente diverse.

€indietro

## **CERTIFICATI DIGITALI Explorer**

Continuo della pagina precedente

Una volta effettuate le operazioni indicate nella pagina precedente si pone il problema di verificare i certificati digitali che si trovano nei diversi siti:

- quando il browser è in modalità normale, cioè non ci troviamo su un sito protetto da certificati, sulla barra di stato in basso a destra appare un'icona contenete una chiave rotta, un lucchetto aperto o niente.
- quando la sessione SSL è attiva e il browser trasmette su un canale sicuro, la chiave diventa intera e il lucchetto si chiude.

Utilizzando **Explorer 5.0, 5.5 e 6.0** e supponendo di essere sul sito <u>http://www.so-ri.it/pagamenti/multe/</u> (sito per il pagamento online delle contravvenzioni elevate dalla Polizia Municipale), una volta inseriti i dati della multa richiesti, si entra nel sito protetto da certificato: per la verifica del certificato cliccare sul lucchetto o sulla chiave; appare una finestra come questa:

ficato		
nerale	Dettagli Percorso certificazione	
	Informazioni sul certificato	
Scope	o certificato:	
•	Assicura che il contenuto della posta elettronica non possa ssere visto da altri	
•	Protegge il software dalle alterazioni dopo la pubblicazione	
	Assicula crie la provenienza del sottware sia il sub editore Garantisce la propria identità ad un computer remoto	_
• × Paru	u arantisce l'identita di un computer remoto Iteriori dettadi consultare la dichiarazione dell'autorità	•
Rilasc	i <b>ato a:</b> pagamenti.comune.prato.it	
Rilasc	i <b>ato da:</b> Server CA PO-NET	
Vəlid	lo dal. 22/07/2004 al. 22/07/2007	
Tanc		
	Installa certificato Dichiarazione emittent	e
		ЭК

### Controllare:

**1.** la prima parte dell'indirizzo internet del sito deve essere uguale a quello che è scritto nella parte del certificato dove c'è scritto "Rilasciato a:". Il controllo è positivo, infatti l'indirizzo del sito è https://pagamenti.comune.prato.it/ e sul certificato c'è scritto pagamenti.comune.prato.it.

Cliccare su "DETTAGLI", appare una finestra come questa:

	<u> </u>
Campo Versione Numero di serie Algoritmo della firma elettronic Emittente Valido dal Valido fino al Soggetto Chiave pubblica	Valore V3 07 a sha1RSA Server CA PO-NET, CED, Com giovedi 22 luglio 2004 11.44.23 domenica 22 luglio 2007 11.44 w3master@comune.prato.it, p RSA (1024 Bits)

#### Controllare:

1. la validità della data di rilascio e di scadenza del certificato

Cliccare su "PERCORSO CERTIFICAZIONE", appare una finestra come questa:

Certificato	? ×
Generale Dettagli Percorso certificazione	
Percorso certificazione Root CA PO-NET Degementi.comune.prato.it	
⊻isualizza certificato	
Stato certificato:	
Il certificato specificato è valido.	
OK	

#### Controllare:

Sulle icone del 1. certificato NON devono esserci croci rosse 2. L'indirizzo indicato nell'ultimo certificato deve essere uguale alla prima parte dell'indirizzo internet del sito. Il controllo è positivo perché sulle icone NON ci sono croci rosse, quindi i certificati sono validi, e l'indirizzo indicato sul certificato (pagamenti.comune.prato.it/) corrisponde all'indirizzo del sito internet (https://pagamenti.comune.prato.it/)

Se si utilizza **Explorer 4.0** il certificato che appare una volta cliccato sul lucchetto è diverso, ma le informazioni che fornisce ed i controlli da effettuare sono gli stessi delle altre versioni del browser. Il certificato che appare è il seguente:

Proprietà		×						
Propriet	à del certificato							
	<u>Campo:</u> Argomento Rilasciato da Data di validità Data di scadenza Fingerprint Protocollo di protezione Tipo di codifica Tipo di hash Scambio chiave	Dettagli: Certificato emesso da un'agenzia di protezio						
		Chiudi						
Il browser ci avvisa anche quando stiamo entrando o uscendo da un sito protetto inviando a video i seguenti messaggi:								
Messaggio di ENTRATA								
	Avviso di protezione Si stanno per visuali connessione protetta Le informazioni scarr essere visualizzate d Non mostrare l'ar	zzare delle pagine su una a. Ibiate con questo sito non possono la altri utenti del Web. Ivviso in futuro						
Messaggio di USCITA								
	Avviso di protezione Si sta per abbandor Internet. Altre persor informazioni inviate. Continuare? Non <u>m</u> ostrare l'a	Imare una connessione protetta ne potrebbero visualizzare le   vviso in futuro   No Ulterjori informazioni						