## PROCEDURA DI VERIFICA DELLA VALIDITÀ DEI CERTIFICATI CONTENUTI NEL DISPOSITIVO DI FIRMA DIGITALE

## Programma FirmaCerta



Aprire il programma FirmaCerta dall'icona sul desktop

Cliccare su Strumenti e poi su Visualizza certificati contenuti nel dispositivo di firma:

	Firma Certa [4.2.9.5]			$\times$
File	Strumenti Modulistica Help			
	Attiva dispositivo di firma	ED	1	
ph.p	Visualizza certificati contenuti nel dispositivo di firma	1		
Eirr	Verifica dispositivo di firma	afor	etrica	
	Cambio PIN			
	Sblocca dispositivo di firma			
	Rinnovo certificati			
	Firma Certa Protect			
	Firma grafometrica	>		
	Opzioni			

## Cliccare su Verifica

🙀 Certificati contenuti nella smart card —		×
BINIMILT22558H199T/2444024000000882.IGn9RKDyRl4AYzauYjmVqyl Esito Dettagli		
Certificato di autenticazione non verificato		
ė		
< >>		
Verifica 18/08/2017 V 13:41:42 🔁 Data di verifica	Chi	udi

Attendere che la verifica sia conclusa: compariranno due spunte verdi e sulla destra sarà possibile verificare il periodo di validità di ogni certificato.



Aprire il programma Dike6 dall'icona sul desktop



Cliccare su Impostazioni



Cliccare su Dispositivi: se compare il messaggio "Nessun lettore" cliccare sul tasto aggiorna

(	S) Configurazione personalizzata	
	🏟 Generale	Sono stati rilevati Odispositivi. Scegliere il dispositivo da gestire:
	🧭 Marcatura Temporale	
	( ) Firma Remota	
	Connessione	
	ψ Dispositivi	
	Cronologia Certificati	
	R Licenza PRO ed Estensioni	
	Torna alla homo	

verificare che compaiano i dati dell'intestatario della chiavetta: cliccando su uno dei due certificati si aprira il dettaglio con il periodo di validità.

8 Configurazione personalizzata		×
🍫 Generale	Sono stati rilevati 1 dispositivi. Scegliere il dispositivo da gestire:	0.8
🧭 Marcatura Temporale	Attivazione dispositivo	VU
🕒 Firma Remota	Cambio PIN	
Connessione	Imposta doppio PIN	
∲ Dispositivi	Mostra certificati sul dispositivo	
Cronologia Certificati	BNNMLI72S58H199T/244402400000882.IGn9RKDyRl4AYzauYjmVqyN0OrY=	
R Licenza PRO ed Estensioni	Certificato	<
Torna alla home	Generale Dettagli Percorso certificazione  Informazioni sul certificato  Scopo certificato:  Dimostra la propria identità ad un computer remoto Protegge i messaggi di posta elettronica 1.3.6.1.4.1.36203.4.1.2 Accesso smart card  * Per ulteriori dettagli consultare l'informativa dell'Autorità di ce Rilasciato a: BNNMLI72558H199T/244402400000882.IGn9 RKDyRI4AYzauYjmVqyN0CrY= Rilasciato da: Namirial CA Autenticazione Valido dal 06/10/2015 al 11/10/2018 Installa certificato Dichiarazione emittente OK	

## Programma Consolle Avvocato®

Aprire Consolle Avvocato e cliccare sulla voce di Menù in basso a sinistra UTILITA' – Configurazione:



Cliccare su Sicurezza e poi su Verifica PIN

Dati Anagrafici	Java Runtime in uso: 1.8.0_121 ( Firma digitale / Autenticazione
Deleghe	Selezionare il driver PKCS#11 della smart card tra quelli presenti nel sistema:
Pagamenti Telematici	Autenticazione : Smart Card / Token
Documenti	
Sicurezza	Directory extra:
Certificati U.G.	asepkcs Cryptovision(B)
Proxy	bit4xPKI
Notificazioni	Incard-PKCS CardOS-M4
Database	Siemens-CardOS Bit4id_Incard
Accesso Agenda	Verifica PIN Verifica Firma
U Prodotti	
	Utilizza la firma digitale in formato PAdES

Verrà richiesto l'inserimento del PIN e al messaggio PIN corretto cliccare su Ok.

Apparirà la seguente finestra di Verifica Smartcard ove è possibile verificare la validità dei certificati contenuti nella chiavetta Usb.

