ISTRUZIONI PER CIFRARE DI UN FILE

CON IL SOFTWARE FIRMA 4NG

Cifratura di un documento

La crittografia asimmetrica è un tipo di cifratura che consente lo scambio di informazioni in modo sicuro, evitando i rischi della tradizionale crittografia simmetrica connessi allo scambio di un'unica chiave (es. una password o un PIN) necessaria per la codifica/decodifica delle informazioni. La crittografia asimmetrica è basata su una duplice chiave:

- la chiave pubblica, che può essere distribuita a chiunque, serve a cifrare un documento destinato a chi possiede la relativa chiave privata (rende illeggibile il messaggio a chiunque non sia in possesso della chiave privata);
- la chiave privata, personale e segreta, utilizzata dal destinatario per decifrare un documento cifrato con la chiave pubblica.

In tal modo il documento cifrato con una chiave pubblica, potrà essere decifrato solo con la corrispondente chiave privata.

Dopo aver predisposto gli elenchi degli associati in formato elettronico (csv) e in formato PDF/A ed aver provveduto all'apposizione della firma digitale sugli stessi, si può procedere con l'eventuale crittografia di entrambi i documenti. (Tale modalità è alternativa all'utilizzo della busta chiusa sigillata).

Prerequisiti:

- Token USB DIGITAL DNA FIRMA4NG (o altro software di firma digitale rilasciato dai certificatori accreditati AGID)
- Certificato chiave pubblica del Segretario Generale della Camera di Commercio scaricato dal sito www.vr.camcom.it
- File da cifrare

Procedura per cifrare un file

1) Inserire il token di firma digitale su una porta USB del proprio computer



Figura 1: esempio di token di firma digitale

2) Avviare il software di firma all'interno del token se quest'ultimo non si avvia automaticamente all'inserimento del dispositivo nella porta USB



3) Selezionare la voce Applicazioni e successivamente la voce Cifra:

🐴 id			firma	a4ng	() O _ X
e, seregifrar il mesegio a cl	Cifra	nt Si Decifra	Storico	province Impostazioni	 4) Selezionare il file da firmare sul proprio

4) Selezionare il file da firmare sul proprio computer e premere il bottone "Apri":

gence Renera	relia dian				10 • 18
🗑 orde Complete 💆	Alterna Contra C	(Here resided)	100	Sectors	
inity r	The constant of the				
A freedom of	Contraction of the second				
There are a local division of the local divi	The second second			10.000	
	 Concercing 				
a second a	- autorgan				
Stoppene /	Contraction and a state former contradigations			1000	
Realition	State and a set of the second second second	State States and			
and in case of the local division of the loc					
	Elenco.pdf	10/05/2021 11:42	Documento Adob	27 KB	
A COMPANY OF A	autopenacity of	127-027-022-02-086-04	Decomposite Adult .	142, 153	
Marco Carlos	an internation (2) and	(Bene) / Bally (Be)?	Decomposite match.	10.00	
🖉 Ganadia PC	in monotoner125.pdf	(Berld) /Bally (Berl)	Decompting Adults -	10.40	
a faccolla	preserve cite	partie (2021 10-38	Fogle d'avore d.,	12.43	
C 10400 (2) (7) (9)	M uffile.pdf	111000-0000-000-000	Decuments Adult	176-63	
d here	Schule per bando pror 1-6-6 identità dig	second costs on our	Decamanity # 19k.	00.02	
	(g) in concorning	10103-0018-00-0	154,825	3.48	
Nome	file: Elenco ndf				ilec (* *)

5) Se è la prima volta che si cifra il documento occorre preventivamente importare il certificato (chiave pubblica) del destinatario. Selezionare la label "file" e importare il certificato da file selezionandolo dal proprio computer dopo averlo scaricato dal sito della Camera di Commercio come mostrato in figura:

G Cifra			- 🗆 X
Cifra Scegli i contatti per cui cifrare			firma
	Contatti File Elenco in linea	Cifra per	
	BRGRCR68M01L781S/7420100700153633	3.Qa	
$\langle \rangle$			
firma	<	>	
	Importa da fil	e	
			<u>A</u> vanti > Annulla

Selezionare il certificato e spostarlo nella sezione a destra (riquadro "Cifra per...") e cliccare su Avanti

6) Procedere con la procedura guidata eventualmente modificando il percorso del file cifrato. L'estensione del file sarà .p7e

🔒 Cifra		- 🗆 X
Cifra Scegli le opzioni di cifratura		firma
firma	Salva come: C: \Users\marco.carlini\Documents\CAMCOMVR_1 (2).pdf.p7e Algoritmo di offratura: DES-EDE3-CBC \v Salva in formato PEM Distruggi il documento originale	
	< Indietro	<u>A</u> vanti > Annulla

Cliccare su Avanti per avvivare la cifratura del file e terminare la procedura:

🔒 Cifra		- 🗆 X
Cifra in corso Attendere che il file venga cifrat	0	firma
firmad	Ofra del file in corso	
		Avanti > Annulla

🔒 Cifra		_		×
Cifratura conclusa		f	irma	24.
	Operazione conclusa			
	Il file C: /Users/marco.carlini/Documents/CAMCOMVR_1 (2).pdf è stato cifrato correttamente Salvato in: C: /Users/marco.carlini/Documents/CAMCOMVR_1 (2).pdf.p7e			
			<u>T</u> ermir	na