ALLEGATO

Procedura di convalida indirizzo mail, zippatura e policy password: istruzioni operative.

La convalida dell'indirizzo mail è una operazione necessaria per avere la certezza che la comunicazione avvenga con il soggetto effettivamente destinatario della missiva.
L'indirizzo mail sarà quindi rilevato nel contatto con l'utente in presenza, per esempio nella fase della prenotazione, oppure della visita, o anche nel contatto telefonico.

Altre modalità che forniscono certezza sono relative a procedure che consentono il riconoscimento sicuro dell'utente, per esempio su servizi o app in cui l'identificazione avvenga tramite CNS (quale la Tessera sanitaria): sarebbe quindi da considerarsi verificato per esempio il numero di telefono inserito nel Fascicolo Sanitario da parte dell'utente nei "numeri utili" della sezione "Il mio taccuino", in quanto compilabile solo dall'interessato.

L'indirizzo mail potrà essere verificato, con ragionevole affidabilità mediante l'incrocio con altro strumento di contatto dell'utente, per esempio inviandogli un codice via sms sul numero di cellulare fornito come proprio e chiedendo di rispondere alla mail inviata all'indirizzo dichiarato, riportando quel codice.

La criptazione del documento allegato serve a mantenere riservato il contenuto della comunicazione anche dopo che la mail è stata ricevuta dal destinatario, rimandando alla esclusiva responsabilità di quest'ultimo la eventualità che il documento rimanga in chiaro sulla postazione di lavoro dopo che è stata effettuata l'operazione di decriptazione.
Per sicurezza, chi riceve e decripta l'allegato, può mantenere sullo strumento in uso (e che collega in internet) solo la copia criptata dell'allegato, o effettuare una successiva criptazione della stessa con propria password; oppure può scaricare il documento in chiaro su supporto fuori linea (chiavetta usb, hd esterno) per la sua conservazione confidenziale.

La comunicazione di un documento criptato necessita di due requisiti:

1) la password di criptazione utilizzata dall'inviante deve essere conosciuta dal soggetto che riceve il documento (procedura simmetrica)
2) lo strumento (software) utilizzato per effettuare la criptazione deve essere disponibile anche al soggetto che vuole decriptare.

In questo caso avere la disponibilità di un software liberamente scaricabile dal web rappresenta una ottima opportunità.
La procedura seguente illustra come procedere per l'invio di documenti compressi e crittografati utilizzando il prodotto 7-Zip scaricabile liberamente dal sito www.7-zip.org.
La procedura che segue illustra l'utilizzo di questo prodotto per la criptazione.
La procedura è da intendersi esemplificativa dei parametri e delle fasi operative che devono essere normalmente eseguite.
Nella scelta del prodotto è da preferirsi la semplicità di acquisizione (e la gratuità) da parte del ricevente; la disponibilità del prodotto multipiattaforma (Windows, Linux, MAC, IOS, Android, ecc.) la semplicità dello svolgimento della fase di criptazione/decriptazione.
In particolare il prodotto utilizzato in queste istruzioni da una parte offre l'opportunità di poter essere decriptato anche mediante altre app o software (winzip, winrar, ecc.), ma potrebbe non essere garantito il funzionamento in alcune piattaforme MAC).

Per utilizzare il software occorre scaricarlo installarlo sul proprio pc (se non si posseggono i diritti di amministratore del pc, rivolgersi all'help desk per il supporto).

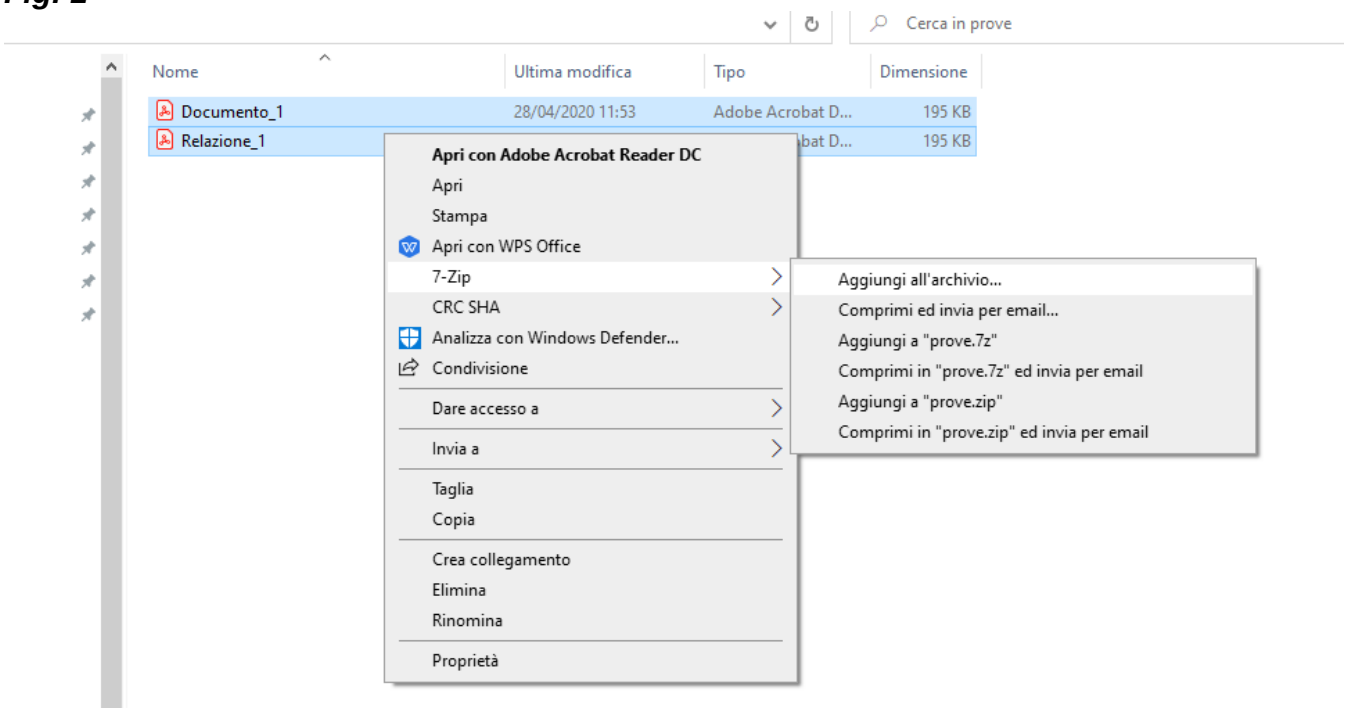
Per effettuare la cifratura procedere come segue:

1) scrivere su un proprio documento la password che si utilizzerà per la criptazione, in modo da poterla riportare correttamente in fase di criptazione del documento e essere sicuri di comunicarla in modo corretto al destinatario.

   Questo consente di costruire la password della complessità desiderata che si raccomanda avere le seguenti caratteristiche minime:
   - lunghezza almeno 10 caratteri
   - la password deve contenere numeri, caratteri sia maiuscoli che minuscoli, e simboli, combinati fra loro: almeno uno per ogni insieme, quindi almeno un carattere maiuscolo, almeno un carattere minuscolo, almeno un numero, almeno un carattere speciale fra quelli ammessi, esempio: "@nTr0poL0g1a";
   - non deve avere più di tre caratteri consecutivi che si ripetono;
   - non deve riportare facilmente ad analogie sull'utente (es. combinazione di caratteri del nome e numeri della data di nascita);

2) **Fig. 1**. Selezionare il/i file da proteggere (es. dall'interfaccia di windows tenendo premuto <ctrl> +tasto sx del mouse su ciascun file); cliccare quindi con il tasto dx del mouse, selezionare 7-Zip e quindi "Aggiungi all'archivio"

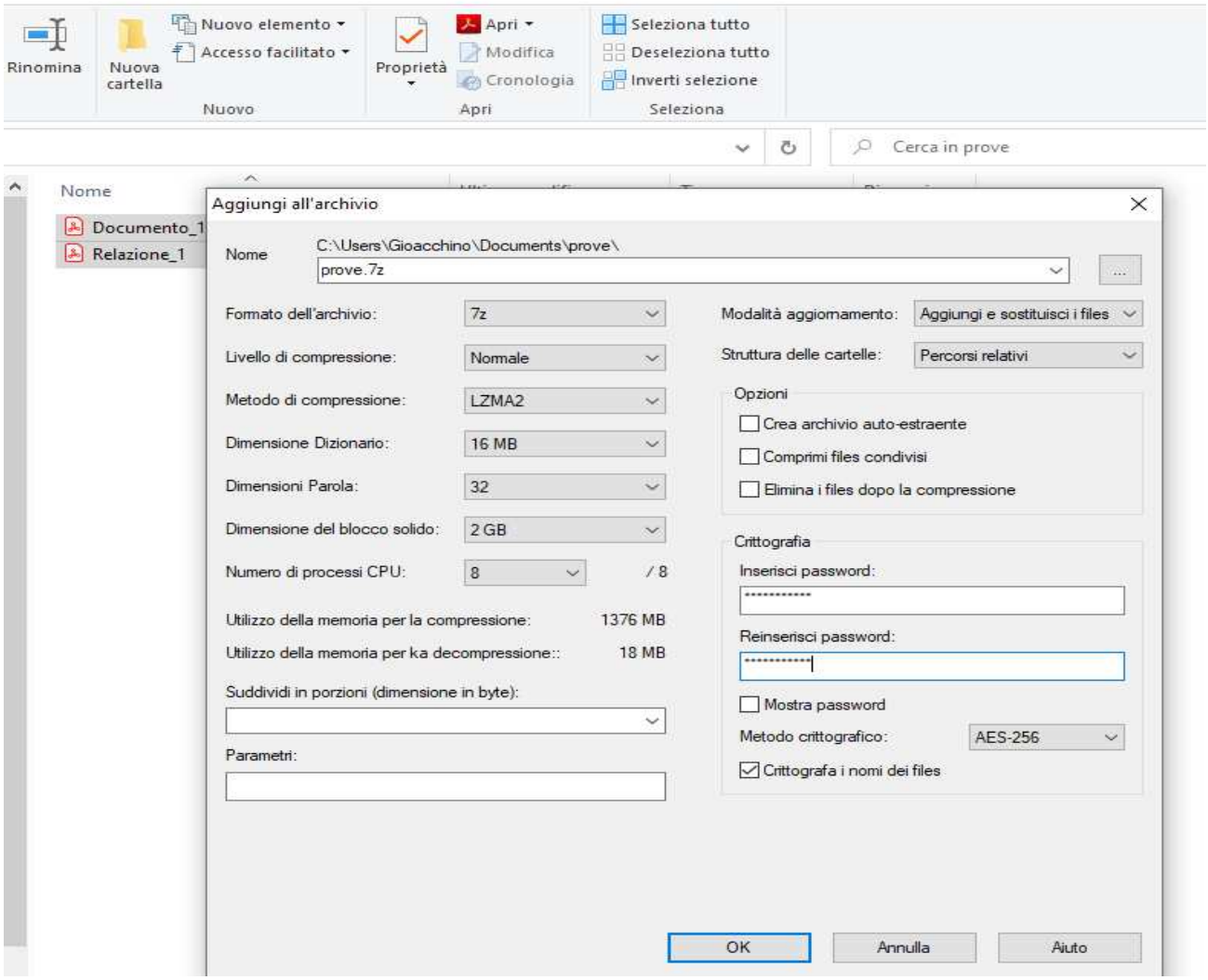
Fig. 1

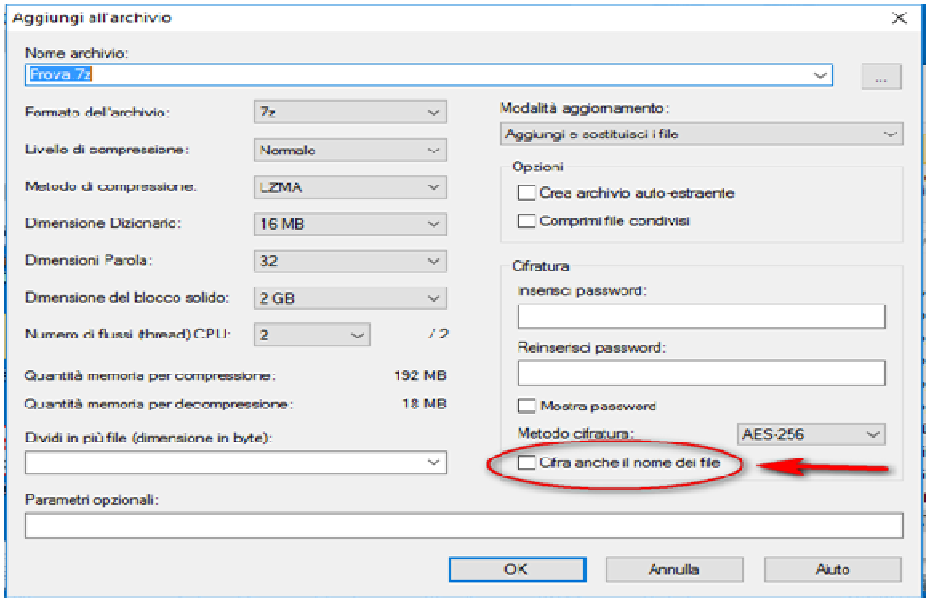


3) **Fig. 2**. Sulla videata che si apre:
   - Selezionare <Formato Archivio>: 7z
   - Assegnare un nome al file criptato (es. prove.7z)

- Selezionare <Metodo Crittografico>: AES-256
- Inserire la password scelta nelle due posizioni indicate (o copia/incolla dal documento su cui si è trascritta al punto 1
- **Togliere o non mettere il check su <Crittografa i nomi dei file>** (l'opzione non deve essere spuntata perché alcuni indirizzi di posta elettronica possono, per motivi di controllo di sicurezza dei files, non consentire la ricezione della mail e conseguentemente nemmeno dell'allegato).

Fig. 2





4) Inviare tramite mail il file criptato ottenuto;

5) Comunicare per altro canale la password di criptazione/decriptazione, per esempio tramite telefono, o tramite sms o strumenti social quali whatsapp, o Telegram

Con 7-Zip si possono produrre anche degli allegati con criptazione più debole ma sempre protetti da password, con estensione ".zip" da selezionare nel "Formato dell'archivio" e "Metodo crittografico" selezionato come ZipChripto (disponibile per l'estensione .zip).

Documenti zippati con l'estensione ".zip" possono essere prodotti anche con altri strumenti free o a pagamento (winzip, winrar) con procedure pressochè identiche a quelle illustrate per 7-Zip, veicolando archivi che possono essere sicuramente decriptati con i prodotti disponibili nelle varie piattaforme.