**ALLEGATO E**

# GUIDATECNICA

## PER LA CREAZIONE DI ARCHIVI PROTETTI DA PASSWORD E LA GENERAZIONE DI CODICI HASH

**COME FARE: CREAZIONE DELL'ARCHIVIO CRITTOGRAFATO**

Tutti i singoli file PDF devono essere compressi in un unico archivio protetto da password (è raccomandato *usare una password composta da almeno 12 caratteri, contenente almeno una cifra, e almeno un carattere maiuscolo*).

**> Windows**

Per Windows è richiesta l'installazione del programma **7-Zip**, liberamente scaricabile all'indirizzo: https://www.7-zip.org/

- Selezionare tutti insieme i file da includere nell'archivio.
- Una volta selezionati tutti i file insieme, cliccare con il tasto destro del mouse.
- Dal menù a tendina che si apre (Figura1), selezionare 7-Zip > Aggiungi all'archivio…

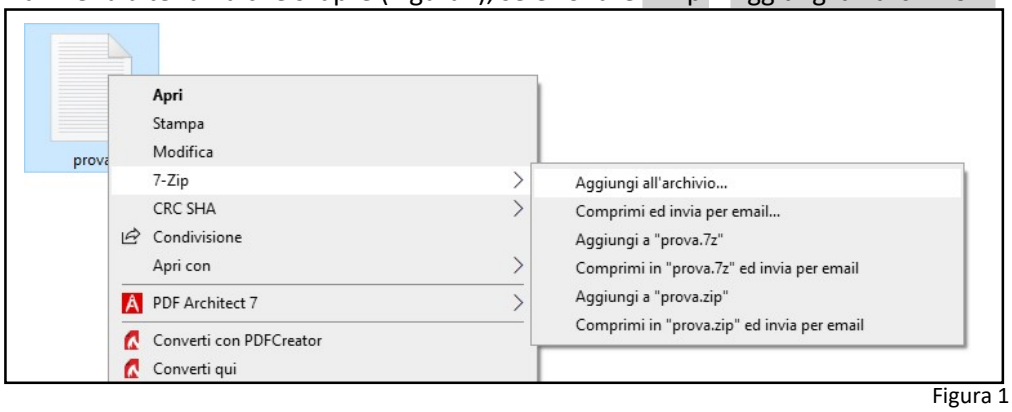



Figura 1

- Si aprirà la finestra seguente (Figura2), nella quale:
  A) INSERIRE LA PASSWORD
  B) SELEZIONARE IL METODO CRITTOGRAFICO AES-256.

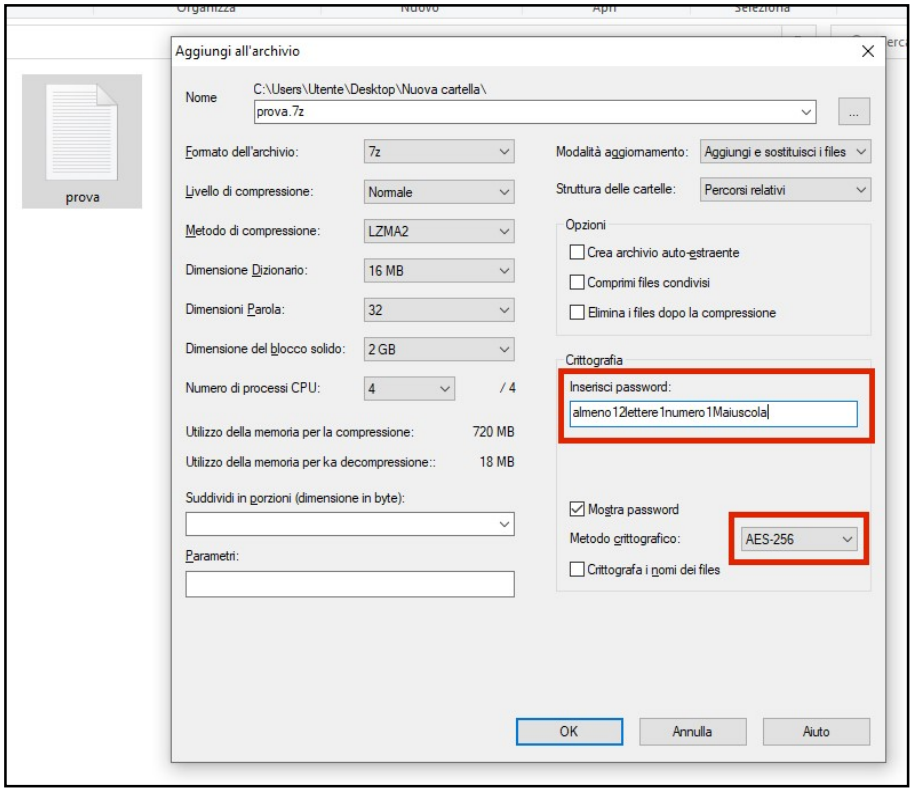



Figura 2

- L'archivio protetto verrà creato nella stessa cartella del/dei file di origine. Questa procedura ha automaticamente creato un codice hash da poter copiare-incollare, dunque non sarà necessario compiere una seconda operazione sull'archivio creato (ma in precedenza ogni singolo file dovrà aver ricevuto un proprio codice hash: vedi pagina 3).

**> MacOs**

Per Mac è richiesta l'installazione del programma **Keka**, liberamente scaricabile all'indirizzo: https://www.keka.io/it/

- Aprire il programma Keka (Figura3)

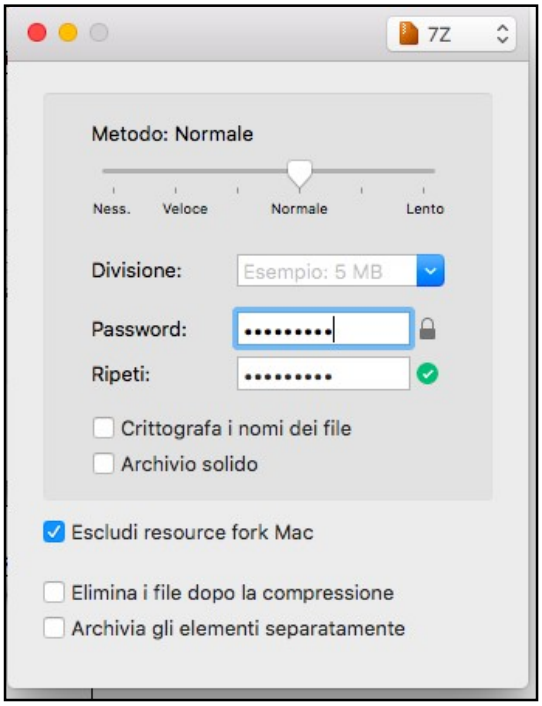



Figura 3

- INSERIRE LA PASSWORD
- assicurarsi che il formato selezionato sia il **7Z** (visibile in alto a destra nella finestra)
- togliere le spunte da "crittografa i nomi dei file" e "archivio solido" (se selezionate)
- Trascinare il/i file che si desidera comprimere sopra la finestra del programma Keka (Figura 4).


figura4

- L'archivio protetto verrà creato nella stessa cartella del/dei file di origine.

## COSA È L'HASH

L'hash è una sorta di "codice fiscale" di un documento elettronico. Esistono degli algoritmi crittografici che generanoHASH a partire da una sequenza di bit, tali per cui per ogni singola sequenza di bit diversa dall'altra si otterrà uno specifico codice HASH. Calcolando due volte, tramite lo stesso algoritmo, l'hash di uno stesso file, si avrà come risultato lo stesso output, ma se il file differisce anche di un solo bit, si avrà un hash totalmente diverso: per questo gli hash vengono usati per verificare l'**integrità dei file**.
Una volta scaricato il file sul PC, per verificare che il file sia integro (privo di errori di trasmissione o di manomissioni volontarie per via di attacchi) basterà ricalcolare l'hash in locale e confrontarlo con la stringa fornita dalla fonte.

## COME FARE: CALCOLO HASH DEI SINGOLI FILE

Per ogni singolo file.PDF e per i lfile.7z da inviare deve essere calcolato il corrispondente codice hash con l'algoritmo **SHA-256**.

**> Windows**
Su Windows è possibile usare il programma **7-Zip** (liberamente scaricabile all'indirizzo: https://www.7-zip.org), utilizzato anche per la compressione e crittografia dei file.

- Selezionare il singolo file per cui calcolare l'HASH e cliccarvi con il tasto destro del mouse.
- Dal menù a tendina che si apre (Figura5), selezionare CRCSHA>SHA-256

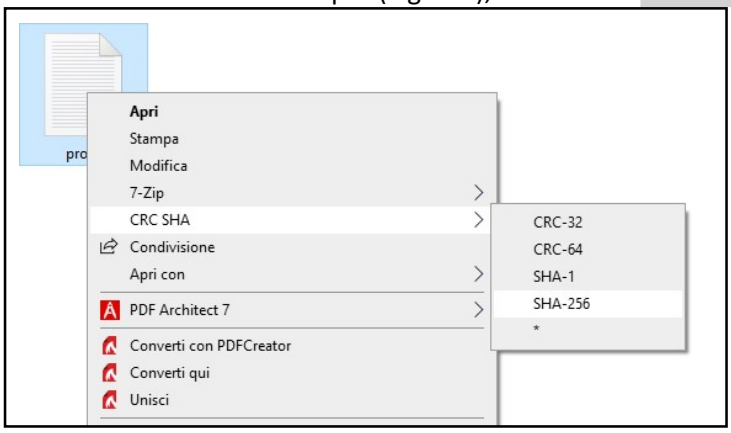


Figura5

- Attendere il completamento dell'operazione automatica (pressoché immediata per file di piccole dimensioni).
- Nella finestra che si apre (Figura 6) copiare il codice alfanumerico SHA256 (riquadro rosso).

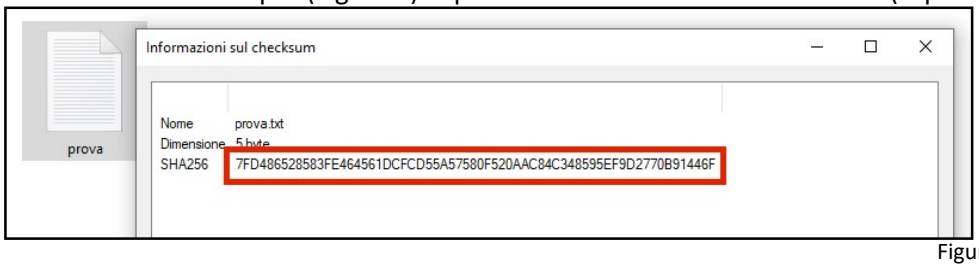


Figura6

- Eseguire la stessa operazione per tutti i file.PDF e per il file.7z crittografato.

**> <u>MacOs</u>**
Su MacOS è possibile sfruttare un'utilità già installata nel sistema operativo, eseguibile da riga di comando del **terminale**: è sufficiente posizionarsi nella cartella contenente i file e digitare **"shasum-a256*.pdf".**

- Per posizionarsi nella cartella è possibile trascinare la cartella sopra l'icona del Terminale (Figura7), se presente nella dashbar del Mac

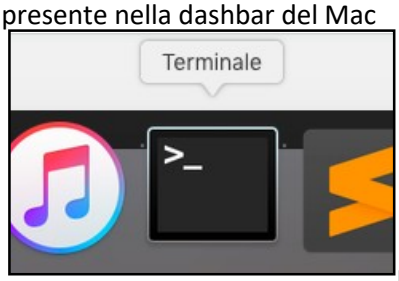
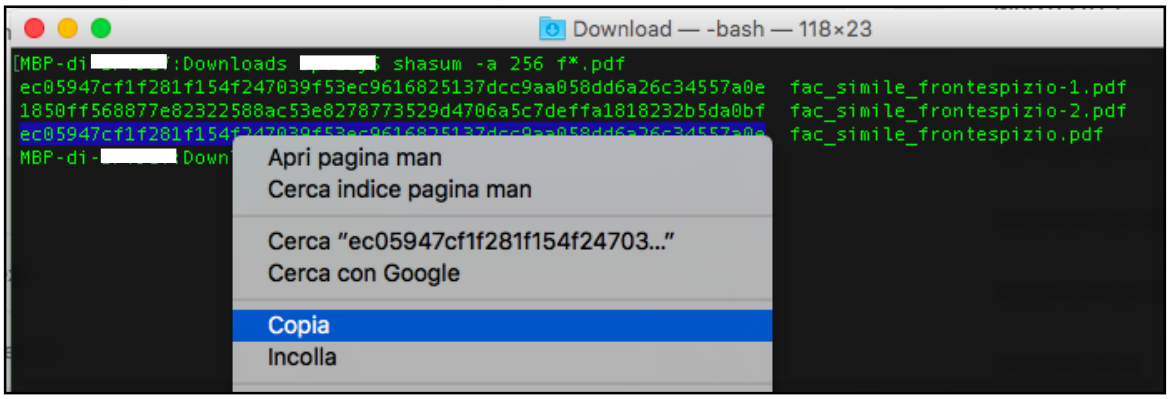


Figura7

In alternativa, è possibile aprire l'applicazione **terminale** e cambiare la cartella digitando il comando **"cd"** seguito da uno spazio e il percorso della cartella (per conoscere l'esatto percorso della cartella, cliccare con il tasto destro sulla cartella stessa, selezionare "Ottieni informazioni" e visualizzare il percorso nella riga "Situatoin:").

- Digitare di seguito il comando shasum – a 256 *.pdf (grazie all'asterisco l'operazione verrà svolta in una sola volta su tutti i file pdf presenti nella cartella).Una volta eseguito il comando, si avrà a video l'elenco degli HASH per ogni file presente e sarà possibile selezionare il testo e copiarlo con la combinazione di tasti "cmd+C" o dal menù contestuale che appare facendo clic con il tasto destro del mouse (o usando 2 dita sull'area touch).




## RIEPILOGO MODALITÀ DI INVIO DELLE OFFERTE

- Entro la data di scadenza inviare la **<u>PRIMA PEC</u>** contenente i TRE ARCHIVI in formato compresso 7z protetti ciascuno da password diversa, contenente i file indicati nella lettera di invito.

Tutti i documenti delle rispettive BUSTE-ARCHIVIO devono essere:

A. Firmati digitalmente
B. Pdf non editabili
C. Associati a un codice hash

**<u>PRIMA PEC ENTRO IL TERMINE DI SCADENZA INDICATO DALLA LETTERA DI INVITO PER LA PRESENTAZIONE DELL'OFFERTA</u>**

- La PRIMA PEC, oltre ai tre archivi protetti da password e contenenti i documenti come indicato nella lettera di invito, dovrà riportare nel corpo del testo nome e cognome del Legale Rappresentante che sottoscrive la domanda, più i codici hash - (**uno per ogni file allegato cui è associato** e **uno per ogni busta-archivio**).
- La PRIMA PEC dovrà riportare come oggetto: ***"Offerta Avviso Piano di Marketing territoriale misura 19.2.20".***
- La PRIMA PEC <u>NON</u> dovrà contenere le password degli ARCHIVI.

**COMUNICAZIONE DELLE PASSWORD SUCCESSIVE ALLA SCADENZA E SU RICHIESTA DELLA STAZIONE APPALTANTE**

**Una volta decorsi i termini di presentazione delle domande, dalle ore 15:00 del giorno 08 novembre 2021 alle ore 10:59 del giorno 09 novembre 2021 dovrà essere inviata** all'indirizzo picenoleader@pec.it **la SOLA password** per poter accedere all'archivio *"BUSTA ARCHIVIO 1 – DOCUMENTAZIONE AMMINISTRATIVA"*.

La PEC dovrà riportare nel corpo del testo unicamente la password dell'archivio 7z "BUSTA ARCHIVIO 1 – DOCUMENTAZIONE AMMINISTRATIVA".
Dovrà riportare come oggetto: "Password Busta Archivio 1 Documentazione Amministrativa – Domanda Piano di marketing territoriale misura 19.20".

**Successivamente dovranno essere inviate le password per accedere agli archivi 2 e 3 A SEGUITO DELLA RICHIESTA DA PARTE DELLA STAZIONE APPALTANTE TRAMITE PEC AL CONCORRENTE.**

*Password per poter accedere all'archivio "BUSTA ARCHIVIO 2 – OFFERTA TECNICA"*

La PEC dovrà riportare nel corpo del testo unicamente la password dell'archivio 7z "BUSTA ARCHIVIO 2 – OFFERTA TECNICA".
Dovrà riportare come oggetto: "Password Busta Archivio 2 Offerta Tecnica – Domanda Piano di marketing territoriale misura 19.20''.

Allo stesso modo la Stazione Appaltante procederà con la richiesta delle password per poter accedere all'archivio "BUSTA ARCHIVIO 3 – OFFERTA ECONOMICA".

*Password per poter accedere all'archivio "BUSTA ARCHIVIO 3 – OFFERTA ECONOMICA"*

La PEC dovrà riportare nel corpo del testo unicamente la password dell'archivio 7z "BUSTA ARCHIVIO 3 – OFFERTA ECONOMICA".
Dovrà riportare come oggetto: "Password Busta Archivio 3 Offerta Economica – Domanda Piano di marketing territoriale misura 19.20".