



PRESIDENZA

DIREZIONE GENERALE AGENZIA DEL DISTRETTO IDROGRAFICO DELLA SARDEGNA

Impronta HASH: procedure di utilizzo

Scopo del presente documento è quello di individuare delle procedure codificate finalizzate al calcolo e alla verifica della suddetta impronta hash al fine di verificare la corrispondenza tra il contenuto di un documento inviato e quello ricevuto per posta elettronica o attraverso un download da un servizio di trasferimento o condivisione di files.

A tale proposito, l'Allegato A alla delibera del Comitato Istituzionale n. 1 del 04.12.2020 recante «*Directive applicative della L. n. 120/2020 ai procedimenti di variante dei piani per l'assetto idrogeologico dell'Autorità di Bacino della Sardegna*» contempla, al paragrafo **3.a** «*Fase di verifica delle condizioni di procedibilità*», la possibilità di ricevere files attraverso un servizio pubblico di trasferimento o condivisione di files o cloud, purché siano inviati i codici univoci di riconoscibilità (impronte crittografiche basate su funzioni di hash) di ciascun documento trasmesso, a garanzia dell'immutabilità, autenticità ed integrità dei documenti trasmessi.

2 - Premessa

L'impronta hash di un testo o di un file informatico è una sequenza di lettere (a,b,c,d,e,f) e cifre (da zero a 9), lunga solitamente 64 caratteri, ottenuta applicando un particolare algoritmo di calcolo alla sequenza di bit che formano il testo o il file.

L'impronta hash è indicata spesso anche con il termine «*evidenza informatica*» oppure semplicemente «*impronta*», in quanto una delle caratteristiche dell'algoritmo di creazione è quindi quella di generare impronte diverse a fronte di contenuti diversi o modificati.

Grazie all'impronta hash è possibile quindi verificare la corrispondenza tra il contenuto di un documento inviato e quello ricevuto (ad esempio per posta elettronica oppure tramite download). Se il mittente calcola l'hash del documento e lo invia assieme al documento stesso, il destinatario è in grado di verificare che durante la trasmissione il documento non abbia subito alterazioni. Basterà infatti ricalcolare l'hash del file ricevuto e confrontarlo con quello che gli è stato inviato per essere sicuro dell'integrità del documento.

Questo sistema è riconosciuto anche in ambito giuridico in materia di attestazione di conformità di un documento.

Le procedure di generazione e verifica dell'impronta hash di seguito descritte fanno riferimento a uno dei più diffusi sistemi attualmente disponibili che prevedono l'utilizzo di portali in rete, in mancanza, al momento, di servizi web ufficiali gestiti da Enti Pubblici.



3 - Calcolo dell'impronta Hash

Per il calcolo dell'impronta hash di uno o più file, è possibile utilizzare, tra quelli attualmente disponibili, il servizio disponibile online al seguente indirizzo:

<https://www.avvocatoandreani.it/servizi/calcolo-verifica-impronta-hash.php>

Questa applicazione consente di calcolare rapidamente, in un unico passaggio, l'**impronta hash** di uno o più file in base all'algoritmo SHA256, da utilizzare ovunque vi sia necessità di identificare univocamente un file.

L'applicativo è caratterizzato da un'interfaccia semplice, illustrata nell'immagine a fianco.

The screenshot shows a web interface for calculating and verifying file hashes. At the top, it says "CALCOLO e VERIFICA dell'IMPRONTA HASH". Below this, there are two radio buttons: "CALCOLO" (selected) and "VERIFICA". A large dashed box in the center contains the instruction: "Trascina i file nell'area tratteggiata o clicca per selezionarli." Below this is a "NOTA:" section with a red information icon, stating that files are not transferred to the server but processed locally using the sha256 algorithm from the Asmcrypto library. A rating bar shows "Valuta il servizio: 4.56 / 5 (406 voti)" with five stars. At the bottom, there is a "Segnala questa Applicazione" button and social media icons for Facebook, LinkedIn, and Twitter.



3 - Calcolo dell'impronta Hash

Per calcolare l'impronta di un file sarà sufficiente seguire la seguente procedura:

1) Selezionare (opzione di default) la voce «**CALCOLO**»;

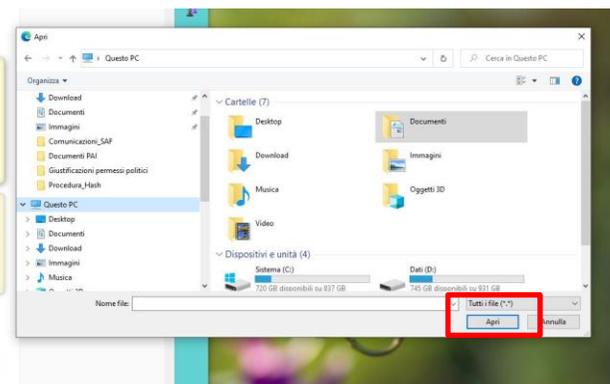
CALCOLO e VERIFICA dell'IMPRONTA HASH

CALCOLO VERIFICA

2) Cliccare nello spazio di caricamento dei files;

Trascina i file nell'area tratteggiata o clicca per selezionarli.

3) Navigare nelle risorse del computer e selezionare il file di cui si desidera calcolare l'impronta. Per confermare la selezione fare click su «**Apri**»;



3 - Calcolo dell'impronta Hash

4) Il software calcola l'impronta e la annota nel riquadro inferiore dell'applicativo;

Come si osserva, l'applicativo annota non solo l'impronta hash, ma anche la denominazione, la dimensione e la marcatura temporale del file.

CALCOLO e VERIFICA dell'IMPRONTA HASH

CALCOLO VERIFICA

Trascina i file nell'area tratteggiata o clicca per selezionarli.

Elaborazione terminata (1/1 file elaborato)

File: 2023.01.10_PP.pdf ✕

Dimensioni: 80674 byte

Riferimento temporale: Mer, 25 Gen 2023 08:55:56 UTC

Impronta Hash SHA256:
3ef3c3bc63eeec1c4c9b1e9da958dd8e4eae8d8611cdfae12a47
32e21d0de449

Nuovo Calcolo

↑

NOTA:
Durante l'elaborazione i file **NON** sono trasferiti sul server del sito ma sono elaborati direttamente sul tuo computer da un'apposita routine *javascript* (algoritmo *sha256* della libreria *Asmcrypto*). Questo a garanzia della **riservatezza** dei tuoi documenti ed anche per **velocizzare** l'elaborazione in caso di file di grosse dimensioni che impiegherebbero troppo tempo per essere caricati sul server.

4 - Invio della documentazione completa dell'impronta Hash

L'invio della documentazione ad ADIS sarà comunicata via *pec* con una nota di trasmissione nella quale saranno indicati:

1. Elenco della documentazione trasmessa;
2. Link al servizio di condivisione pubblica o cloud che contiene gli elaborati trasmessi che consenta il download degli stessi con indicazione della eventuale scadenza dello stesso;
3. Impronta hash relativa a ciascuno dei files trasmessi;



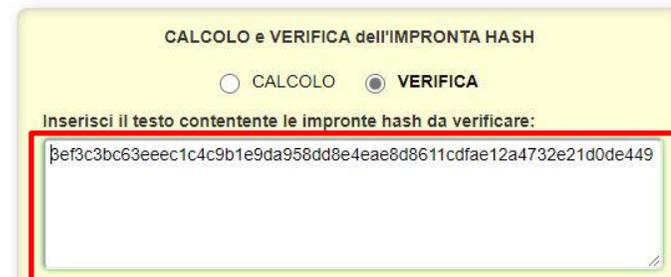
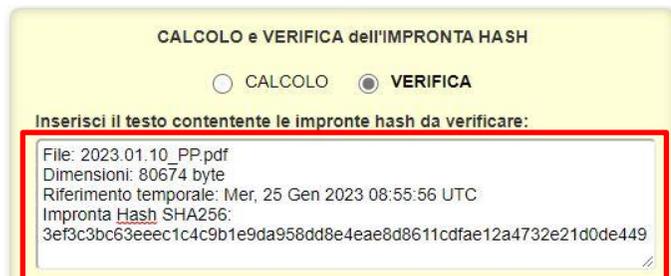
5 - Verifica dell'impronta Hash (a carico di ADIS)

ADIS, ottenuta la documentazione nelle modalità descritte nel precedente punto 4, provvederà alla verifica di un'impronta hash di un file ricevuto utilizzando il medesimo strumento, secondo la seguente procedura:

1) Aprire l'applicativo e selezionare la voce «**VERIFICA**» presente in alto a destra;

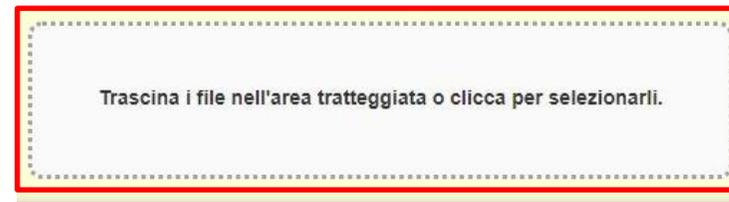


2) Incollare il codice nell'apposito spazio. Il codice può essere riportato nella forma completa di dettagli e marcatura temporale (immagine a sinistra), come quello rilasciato dall'applicativo e descritto nel paragrafo precedente, oppure nella sola una sequenza di lettere e cifre (immagine a destra)

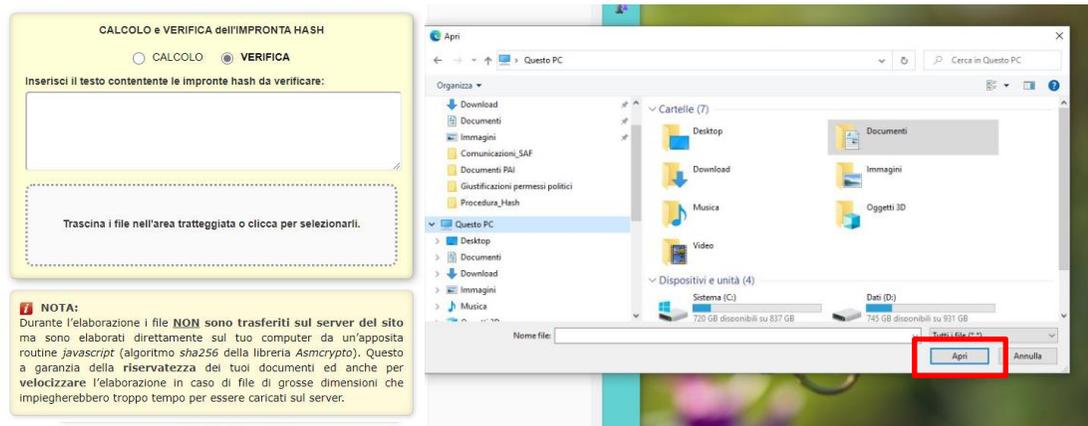


5 - Verifica dell'impronta Hash (a carico di ADIS)

3) Cliccare nello spazio di caricamento dei files;



4) Navigare nelle risorse del computer e selezionare il file di cui si desidera verificare l'impronta. Per confermare la selezione fare click su «**Apri**»;



5 - Verifica dell'impronta Hash (a carico di ADIS)

5) In caso di esito positivo della verifica nel riquadro inferiore apparirà il messaggio:

«Perfetto! Il file corrisponde.»

