Regione Umbria

Direzione regionale Governo del territorio, ambiente e protezione civile

Servizio Rischio idrogeologico, idraulico e sismico, Difesa del suolo

Sezione Rischio Sismico, Normativa Antisismica
e Prevenzione Sismica. Genio Civile

Umbria-Sis

Verifica files caricati nel Portale Umbria-Sis mediante l'utilizzo del codice hash indicato nelle ricevute telematiche

INDICE

1 INTRODUZIONE

Per agevolare la verifica della conformità dei files caricati nel portale Umbria-Sis e il duplicato in possesso del professionista o del committente che ha caricato il progetto, il sistema rilascia una ricavuta di presentazione che contiene, oltre al nome dei files presentati, anche il relativo codice hash nel formato HSA-1

Gli utenti potranno pertanto utilizzare uno dei tanti programmi disponibili oppure una delle tante funzionalità disponibili online per la verifica ci congruità tra il file in proprio possesso e il relativo codice hash stampato nella ricevuta telematica rilasciata

RICEVUTA TELEMATICA
DI PRESENTAZIONE

Regione Umbria

La presente ricevuta telematica attesta l'avvenuta presentazione della domanda presso l'Ente e l'avvio del procedimento amministrativo, fatta salva la verifica della completezza dell'istanza

ELENCO DEI DOCUMENTI DIGITALI ALLEGATI

Copie del progetto architettonico	**progetto.p7m**
Hash SHA-1 :	**02003517898a973e287b46d5c938f0f8acef4862**
Copie della relazione tecnica illustrativa	**tecnica.p7m**
Hash SHA-1 :	**02003517898a973e287b46d5c938f0f8acef4862**
Copie della relazione geotecnica	**geotecnica.p7m**
Hash SHA-1 :	**02003517898a973e287b46d5c938f0f8acef4862**
Copie della relazione geologica	**geologica.p7m**
Hash SHA-1 :	**02003517898a973e287b46d5c938f0f8acef4862**
Copie della relazione sulle fondazioni	**fondazioni.p7m**
Hash SHA-1 :	**02003517898a973e287b46d5c938f0f8acef4862**
Copie della relazione di calcoli	**calcoli.p7m**
Hash SHA-1 :	**02003517898a973e287b46d5c938f0f8acef4862**
Copie della Relazione sintetica degli elem	**strutturale.p7m**
Hash SHA-1 :	**02003517898a973e287b46d5c938f0f8acef4862**
Copie della relazione di valutazione di sicu	**sicurezza.p7m**
Hash SHA-1 :	**02003517898a973e287b46d5c938f0f8acef4862**
Copie elaborati grafici esecutivi della struti	**grafici.p7m**
Hash SHA-1 :	**02003517898a973e287b46d5c938f0f8acef4862**
Copie elaborati grafici dei particolari costru	**grafici costruttivi.p7m**
Hash SHA-1 :	**02003517898a973e287b46d5c938f0f8acef4862**
Copie relazione sui materiali impiegati	**materiali.p7m**
Hash SHA-1 :	**02003517898a973e287b46d5c938f0f8acef4862**
Copie piano di manutenzione	**manutenzione.p7m**
Hash SHA-1 :	**02003517898a973e287b46d5c938f0f8acef4862**

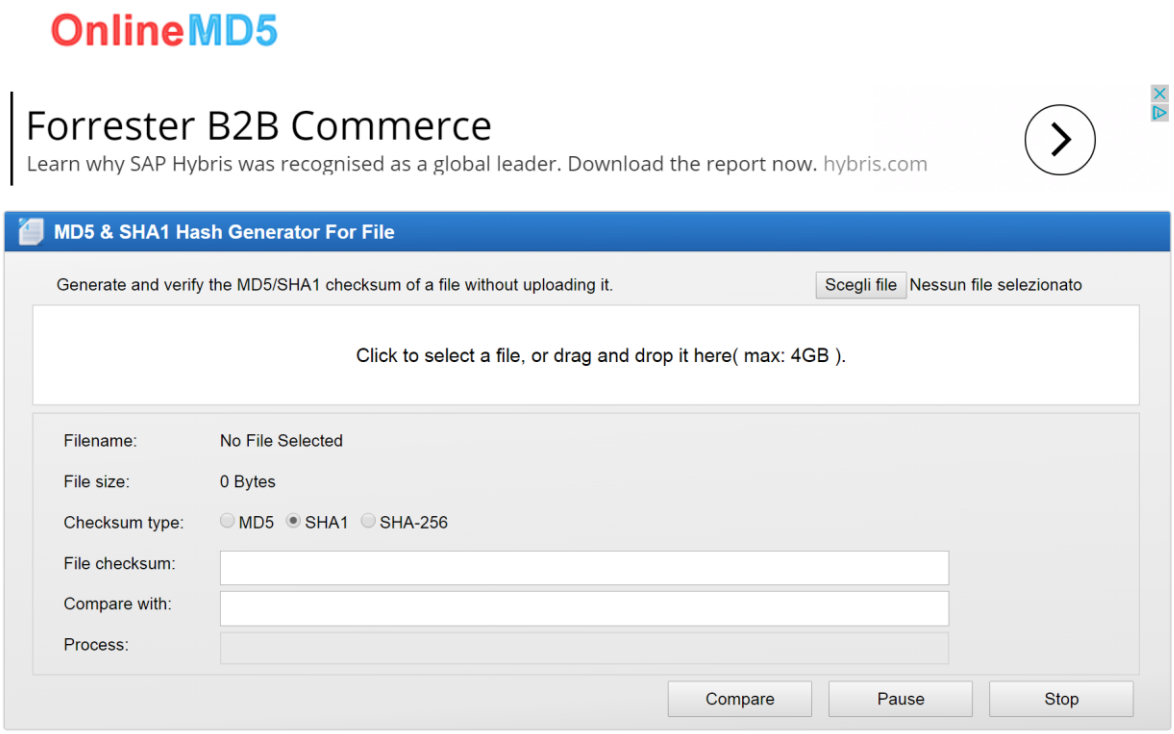
Un soggetto terzo (banca, assicurazione, notaio ecc) che riceve l'autorizzazione firmata digitalmente dal Dirigente del Servizio Regionale, i file che costituiscono il progetto (ed eventuali integrazioni) unitamente alle ricevute telematiche rilasciate dal portale (contenenti i codici hash di tutti i files caricati) può verificare autonomamente, utilizzando le semplici applicazioni online o specifici programmi

2 VERIFICA DEI CODICI HASH

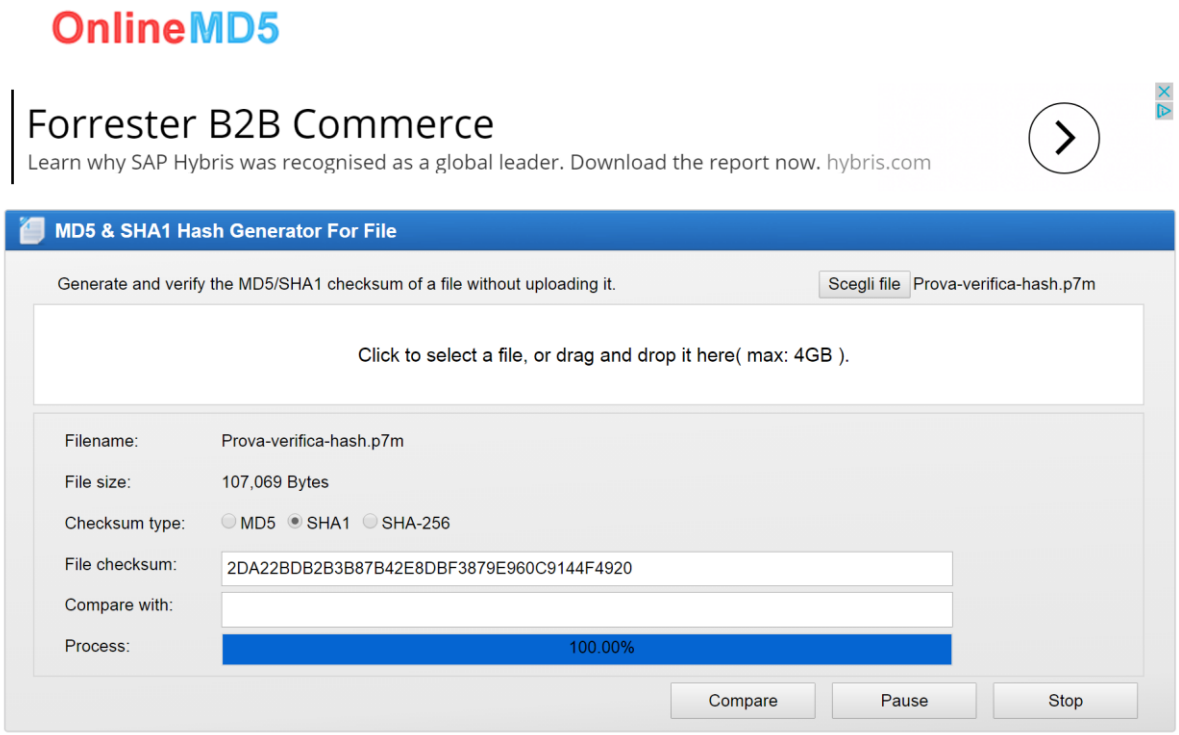
2.1 UTILIZZO APPLICAZIONI ONLINE

Accedere all'applicazione utilizzando il seguente link

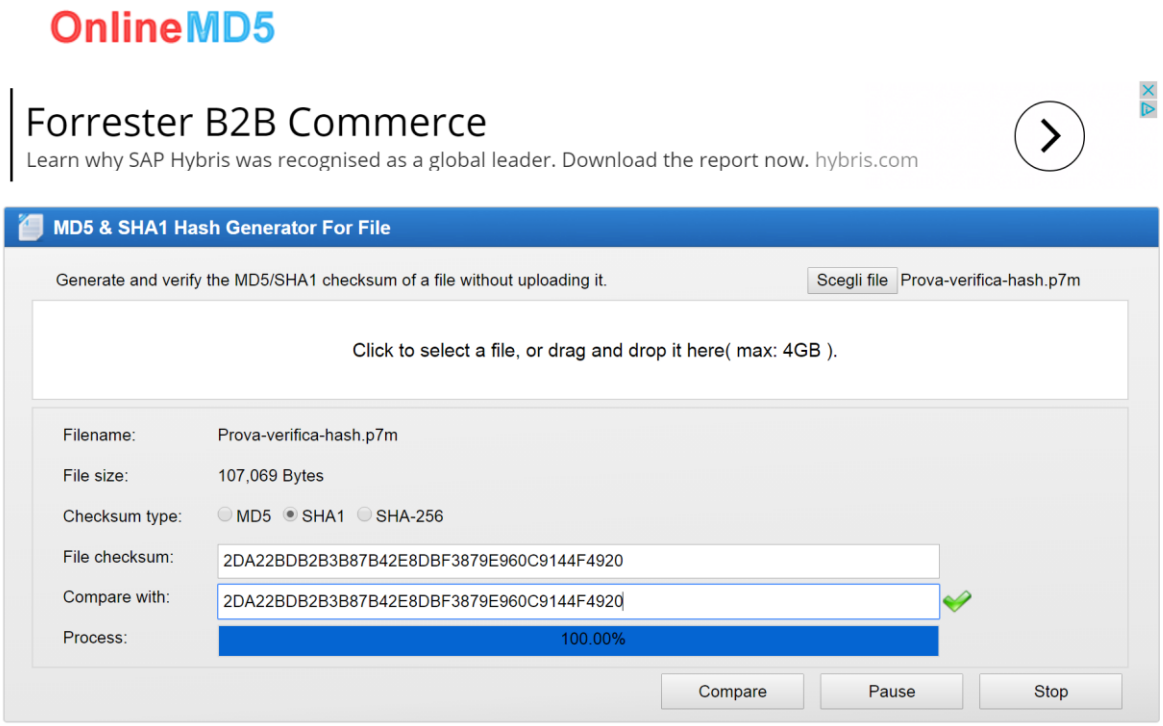
http://onlinemd5.com/



selezionare il tipo di codifica (SHA-1) quindi sceglere il file da verificare (oppure trascinarlo all'interno della finestra)



Verrà automaticamente calcolato il File checksum del file, copiare ora il File checksum SHA-256 riportato nella ricevuta telematica accanto al nome del file e incollarlo nella finestra “Compare with”



Il segno di spunta verde attesta la congruenza del file con il codice hash riportato nella ricevuta garantendo pertanto la conformità del file con quello acquisito dal portale Umbria-Sis

3 Per chi volesse approfondire l'argomento : Mini Guida sull'Impronta Hash

In internet si trovano molte informazioni relative a questo argomento ad esempio qui potrete trovare una sintetica descrizione del funzionamento dei codici hash

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

3.1 *FILE E DOCUMENTI INFORMATICI*

*Tutti i documenti che creiamo, le immagini che otteniamo dallo scanner, i contenuti multimediali (fotografie, audio, video ecc.), le pagine web ed ogni altra informazione visualizzabile su un computer, sono **file di dati** costituiti da **sequenze di byte**.*
*Ogni byte è composto da **8 bit**, dove il bit è l'**unità elementare** di informazione che può assumere valori **0** (zero) o **1** (uno), secondo quella che viene chiamata **codifica binaria**.*
*Anche i caratteri di testo sono rappresentati da sequenze di bit contenute in un byte: la lettera "a" è 01100001, la lettera "b" è 01100010, la lettera "c" è 01100011 e così via. Ad esempio, la parola "giustizia" è codificata in 01100111 01101001 01110101 01110011 01110100 01101001 01111010 01101001 01100001. (se desideri puoi divertirti con questo **convertitore binario**).*
Allo stesso modo, semplificando, una foto digitale è composta da una sequenza di byte che rappresentano i punti colorati nello schermo (pixel), così come un brano musicale è una sequenza di bit che può essere elaborata da un apposito lettore per riprodurre l'audio o un qualsiasi programma software è una sequenza di byte interpretati come istruzioni per il computer.
*Ogni byte può essere inoltre visto come un **numero** intero che va da zero a 255, poiché con 8 bit a disposizione si possono ottenere al massimo 256 combinazioni diverse per ogni singolo byte.*

*In altre parole tutti i contenuti informatici sono costituiti da sequenze di **numeri** (digit in inglese, da cui il termine **digitale**) che, presi singolarmente non hanno ovviamente alcun significato, ma se elaborati da appositi programmi software, vengono convertiti in documenti di testo, fotografie, video, musica, pagine web e tutto ciò che possiamo visualizzare e usare sul nostro computer; per questo motivo, da un punto di vista strutturale, non vi è differenza tra documenti di testo ed altre informazioni: sono tutti **sequenze di bit**.*

Senza dilungarci sul perché in informatica sia stata adottata la codifica binaria, è necessario sapere che questa rappresentazione digitale delle informazioni è universale

e con questa bisogna confrontarci per comprendere meglio come funziona l'impronta hash.

3.2 *COS'È L'IMPRONTA HASH*

*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.*
*Questo algoritmo non fa altro che **scandire sequenzialmente** tutti i byte che costituiscono un testo o un file e ricavare, passo dopo passo, una serie di "impronte intermedie", ciascuna dipendente dalla precedente, per ottenere, al termine della scansione, quella che sarà l'impronta hash definitiva; ogni passo della scansione influisce quindi su quelli successivi e per questo motivo è sufficiente modificare anche **un solo bit** di tutto il file per ottenere un'impronta finale **diversa**.*
*L'impronta hash è indicata spesso anche con il termine **"evidenza informatica"** oppure semplicemente **"impronta"**.*

*Una prima caratteristica dell'algoritmo di hash è quindi quella di generare **impronte diverse** a fronte di **contenuti diversi**.*

*Ad esempio, l'impronta hash della parola "**applicazione**" è:*

07ae8b27c7596b3314601736f32d5f0
ed17fc8c0e27a0475e8ea2d8b2c788436

*L' hash della parola "**applicazioni**" è invece:*

9377d36b72f4f1455cace0b386b7242
d95525832668d02a6cd805556d8306d19

Come si vede quindi, basta cambiare una sola vocale per ottenere un'impronta completamente diversa.

*In altri termini, non esistono file diversi tra loro che abbiano la stessa impronta hash. Naturalmente, resta inteso che due file identici (ovvero costituiti dalla stessa sequenza di bit) hanno impronte hash uguali, ma in questo caso si parla di "duplicati informatici", peraltro disciplinati anche dal CAD, per i quali non serve alcuna dichiarazione di conformità (per approfondire l'argomento leggi l' **articolo pubblicato**).*

Per completezza, anche se può sembrare ovvio, è bene precisare che applicando lo stesso algoritmo allo stesso contenuto si ottiene sempre la stessa impronta hash e sul calcolo non influisce il decorso del tempo.

*Un'altra caratteristica dell'impronta hash è quella di **non permettere di risalire al testo originario** (o al contenuto del file).*
L'algoritmo di hash infatti è congeniato in modo da non permettere a nessuno di capire

*cosa abbia generato una determinata impronta. Non esiste infatti alcun algoritmo di **decodifca** che possa "svelare", ad esempio, che dietro alle impronte hash del nostro esempio si nascondono le parole "applicazione" e "applicazioni".*

*Infine, è bene evidenziare che l'impronta hash può essere calcolata per **qualsiasi contenuto digitale**, sia che si tratti di un documento Word, OpenOffice o PDF, sia che si tratti di un contenuto multimediale (immagine/audio/video), in quanto, come detto, si tratta sempre di file informatici costituiti da **sequenze di bit**.*

3.3 *A COSA SERVE L'IMPRONTA HASH*

*L'algoritmo di hash nasce innanzitutto per la necessità di '**nascondere**' determinate informazioni (ad esempio le password degli utenti inserite in un database) in modo che nessuno, leggendo la rappresentazione hash, possa risalire al dato originario. Per questo motivo l'hash non può essere considerato una vera e propria "cifratura" in quanto, come noto, per ogni algoritmo di cifratura esiste sempre la possibilità di "decifrare" mentre, come detto, l'hash non lo permette (non posso risalire al testo originario).*

*Un altro utilizzo dell'impronta hash è quello di **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; gli basta infatti ricalcolare l'hash del file ricevuto e confrontarlo con quello che gli è stato inviato per essere sicuro dell'integrità del documento. Se infatti viene alterato anche **un solo bit** di un solo byte del documento, l'algoritmo produrrà un'impronta hash **diversa**, rivelando quindi che il documento è diverso da quello originale.*

3.4 *LA CONFORMITÀ*

Nell'ambito del Codice dell'Amministrazione Digitale e del PCT l'impronta hash ha generalmente un duplice scopo:
*- garantire l' **integrità** dei documenti (come avviene ad esempio nella firma digitale),*
*- permettere di **certificare la conformità** di un documento.*

*Quando si certifica la conformità di un file rispetto all'originale, è necessario che nella dichiarazione firmata vi sia un **"elemento"** che consenta a chiunque di **identificare univocamente il file che stiamo certificando come "conforme all'originale"**.*

Ebbene, per le caratteristiche sopra descritte, l'impronta hash può essere proprio l' "elemento" di cui abbiamo bisogno.

*Infatti, per la sua peculiarità di essere **unica** per ogni file, l'impronta hash ci permette di affermare con certezza che stiamo certificando proprio **quel determinato documento**, e non un altro.*

*Naturalmente è bene precisare che l'impronta hash entra in gioco quando la certificazione di conformità viene redatta in un **documento separato**, mentre non è assolutamente necessaria se inserita all'interno del documento stesso (che poi viene firmato digitalmente).*

Aggiornamento:
*La Direzione Generale dei Sistemi Informativi Automatizzati (DGSIA), con le ultime specifiche contenute nel **DM 28 dicembre 2015**, pubblicato sulla G.U. n.4 del 7/1/2016, e in vigore dal 9 gennaio 2016, ha inteso semplificare il processo di certificazione di conformità rendendo obbligatorio l'utilizzo dell'impronta hash solo in determinate circostanze.*

*Quando si "copia" un documento cartaceo, o più in generale analogico, producendo il corrispondente documento informatico, (ad esempio quando si scannerizza un documento in PDF o in jpeg) è naturale attendersi che sia richiesta per legge una certificazione di conformità tra l'**originale cartaceo** e la **copia informatica**. Tuttavia è più difficile giustificare tale necessità quando anche l'originale è un documento informatico, ma in realtà c'è una motivazione ben precisa. Per comprenderla è bene distinguere tra "**copia informatica**" e "**duplicato informatico**" e per approfondire l'argomento leggi **questo articolo**.*

*A questo proposito ci limitamo a ricordare che l'**art. 23 bis** del Codice dell'Amministrazione Digitale ha equiparato i "duplicati informatici" agli originali (se prodotti secondo le regole tecniche del Capo VII del CAD) conferendo loro il "medesimo valore giuridico, ad ogni effetti di legge, del documento informatico da cui sono tratti". E' sufficiente in questo caso dichiarare sotto la propria responsabilità che si tratta di "duplicato informatico".*

Per contro, sempre lo stesso art. 23 bis, prevede la necessità di certificare la conformità per le "copie informatiche" di documenti informatici, ottenute attraverso procedimenti diversi dalla duplicazione esatta. Ed è qui che può entrare in gioco l'impronta hash.

3.5 *LA FIRMA DIGITALE*

L'impronta hash di un file è utilizzata anche nella "firma digitale" per la quale esistono due formati: CADES e PADES.
Con il formato CADES (CMS Advanced Electronic Signatures), quando si firma digitalmente un documento tramite uno dei tanti programmi in commercio, viene

*creato un nuovo documento di estensione "**.p7m**" che sostanzialmente può essere visto come una sorta di contenitore (la cosiddetta "busta crittografica") che racchiude in sé varie informazioni tra cui il documento originario, l'identità di chi ha lo firmato, l'ente certificatore, una marca temporale e l'impronta hash del documento stesso.*

I file ".p7m" non possono essere aperti dai normali programmi di gestione documenti ma hanno bisogno dei software utilizzati per la firma. Quando un qualsiasi file ".p7m" viene aperto, il software controlla automaticamente, tra le altre informazioni, la corrispondenza tra l'impronta hash del documento e quella memorizzata nel contenitore, impedendo l'apertura del documento stesso nel caso in cui non vi sia corrispondenza, o avvisando l'utente della presenza di un'alterazione delle informazioni.

Il formato PADES (PDF Advanced Electronic Signatures) produce invece un file in formato PDF e consente di gestire versioni successive dello stesso documento, con la possibilità di apporre firme multiple anche in tempi diversi e senza necessità di utilizzare software particolari per la lettura dei documenti.

Nell'ambito del PCT è bene sapere che, con il provvedimento del 16/04/2014, il Ministero della Giustizia ha introdotto la possibilià di utilizzare anche il formato PADES per la formazione dei documenti informatici.