UNIVERSITAT POLITÈCNICA
DE CATALUNYA
BARCELONATECH

Memoria tecnica del progetto

Versione del documento

Versione:	Modifiche:	Realizzato da:
V1.0	Creazione del documento	UPC
V2.0	Definizione tecnica	UPC

Indice

1. Requisiti e contesto del progetto

Questo progetto consiste nell'analisi e nella convalida del Blockchain Legalization Engine (BLE) di Certifydoc, una soluzione progettata per la notarizzazione dei dati archiviati nella blockchain con rilevanza legale. La piattaforma BLE funge da intermediario tra i dati della blockchain e i fornitori di servizi fiduciari qualificati dell'UE.

Nel corso del progetto è stata inoltre svolta l'analisi e la convalida della certificazione dei file di Certifydoc.

Il servizio è accessibile on-demand e viene offerto in modalità Software as a Service, potendo interagire con il sistema tramite un modulo web o tramite una REST API. A sua volta, i risultati della notarizzazione possono essere disponibili tramite e-mail o tramite la REST API.

Requisiti del progetto

Il progetto richiede l'esecuzione di diverse fasi per garantirne la fattibilità tecnica e commerciale:

- **Test e sperimentazione:** convalidare la proposta tecnica tramite test concettuali, sia tecnologici che con gli utenti finali, per verificare la funzionalità e l'usabilità del servizio.
- **Consulenza tecnica e di processo:** consulenza per migliorare i processi e gli aspetti tecnologici in base ai risultati dei test iniziali.
- **Valutazione della sicurezza e delle prestazioni:** test specifici per garantire l'integrità e la protezione dei dati, nonché la stabilità e le prestazioni del sistema in scenari di utilizzo reale.
- **Rapporto di fattibilità:** sviluppo di un rapporto dettagliato che concluda i risultati dei test e convalidi la proposta di progetto.

Contesto del progetto

Questo progetto si inquadra all'interno della Proposta di Servizi del Programma di Aiuti Digital Innovation Hubs, cercando di esplorare ed espandere le funzionalità di notarizzazione elettronica di documenti con rilevanza legale alle tecnologie blockchain. La soluzione BLE non solo propone un'innovazione tecnologica ma è anche in linea con le attuali necessità di digitalizzazione e sicurezza documentale nell'Unione Europea, offrendo un approccio pratico e scalabile che può essere adottato in diversi settori e applicazioni.

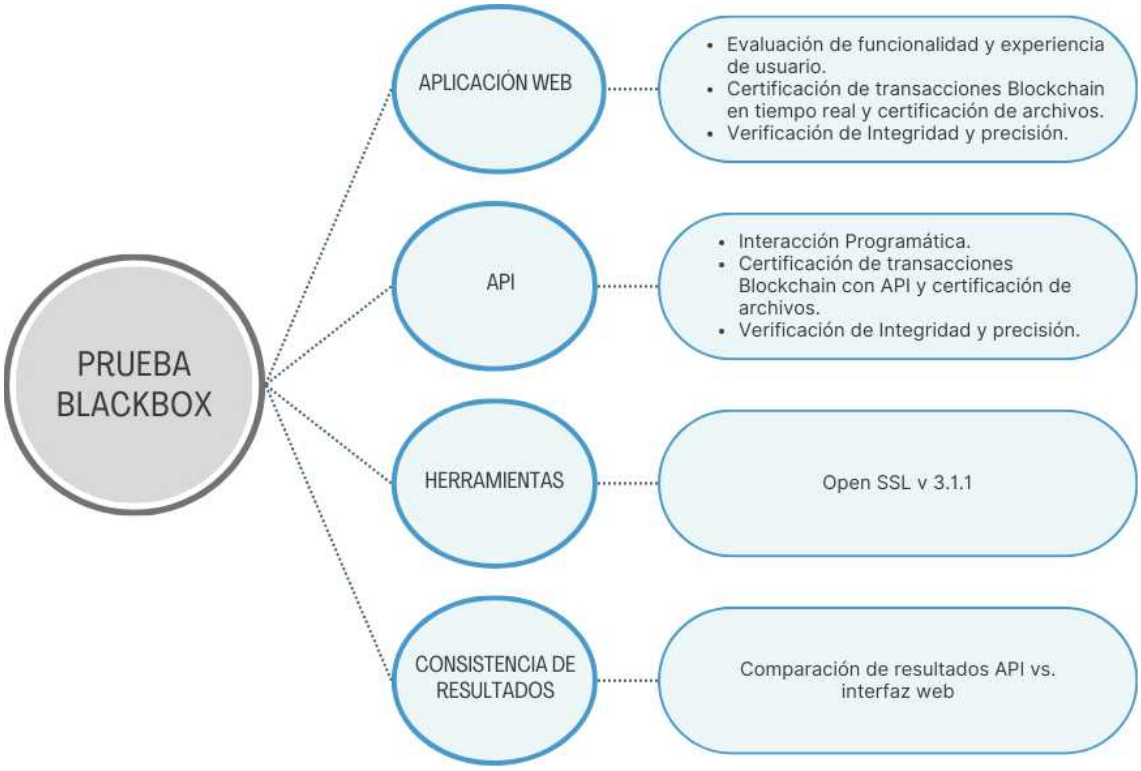
2. Definizione tecnica del problema

Consulenza e valutazione dei servizi di certificazione di Certifydoc; piattaforma di certificazione dei file e piattaforma Blockchain Legalization Engine che offre servizi di certificazione delle transazioni Blockchain mediante la creazione di marcatura temporale con l'hash della transazione e la sua successiva certificazione attraverso un certificatore europeo. L'analisi è stata portata a termine utilizzando la metodologia Black Box.

D'ora in avanti si considerano intercambiabili le parole ""timestamp" con "marcatura temporale"

3. Metodologia di analisi di Certifydoc

L'analisi del Blockchain Legalization Engine (BLE) e della certificazione dei file di Certifydoc è stata effettuata utilizzando un approccio black box, valutando l'applicazione da una prospettiva esterna senza accedere al codice sorgente o alla struttura interna del sistema.



Questa analisi è stata realizzata da due interfacce distinte per fornire una valutazione completa:

1. **Dall'applicazione web di Certifydoc:**

a. Accesso come utente tipico: l'applicazione web Certifydoc è stata utilizzata come utente tipico per valutare sia le funzionalità generali che l'esperienza utente. Ciò includeva la navigazione nell'interfaccia, la gestione degli account e l'esecuzione di funzioni di base.
b. Certificazione dei file e delle transazioni blockchain: il test di certificazione delle transazioni è stato eseguito tramite l'interfaccia utente per osservare il processo di certificazione in tempo reale e valutare l'usabilità e l'accessibilità del sistema. Oltre ai test di certificazione dei file.
c. Verifica dell'integrità e dell'accuratezza: le informazioni fornite durante il processo di certificazione sono state verificate per integrità e accuratezza, assicurando che i dati e i risultati visualizzati fossero coerenti e affidabili.

2. Utilizzo delle API di Certifydoc:
a. Interazione programmatica: l'API fornita da Certifydoc è stata utilizzata per interagire con la piattaforma a livello di programmatico, il che ha consentito di valutare la flessibilità e la capacità di integrazione del servizio.
b. Certificazione di file di transazioni blockchain: le certificazioni delle transazioni blockchain sono state eseguite utilizzando le varie funzioni disponibili nell'API, con l'obiettivo di testare la robustezza e l'efficienza di queste interfacce programmatiche. Oltre ai test di certificazione dei file.
c. Verifica dell'integrità e dell'accuratezza: le informazioni fornite durante il processo di certificazione sono state controllate per integrità e accuratezza, assicurando che i dati e i risultati visualizzati fossero coerenti e affidabili.
d. Coerenza dei risultati: è stata verificata la coerenza dei risultati ottenuti tramite l'API rispetto a quelli generati tramite l'interfaccia web, assicurando che entrambe le piattaforme fornissero risultati equivalenti.

Strumenti di verifica:

Per verificare la validità delle certificazioni è stato utilizzato OpenSSL (versione 3.1.1), una libreria crittografica open source che facilita l'implementazione di protocolli di sicurezza. Questo software ha permesso di confermare l'autenticità e la sicurezza delle certificazioni generate da BLE, assicurando che il sistema sia conforme agli standard di sicurezza correnti.

4. Processo di certificazione di Certifydoc

Certifydoc utilizza una tecnologia avanzata per certificare sia le transazioni blockchain che i file digitali, garantendo l'autenticità e l'integrità dei dati tramite la creazione di marcature temporali verificabili.

Processo tecnico comune

Per tutti i tipi di certificazione, Certifydoc utilizza tecniche di crittografia sicure per garantire che timestamp e certificazioni siano inconfutabili e legalmente validi. Inoltre, utilizza lo standard RFC 3161 per garantire la compatibilità globale e il riconoscimento delle certificazioni. Ogni certificazione rilasciata da Certifydoc può essere verificata in modo indipendente utilizzando strumenti come OpenSSL, garantendo trasparenza e affidabilità.

Vantaggi del processo

- Sicurezza: l'uso dell'hashing SHA256 e del protocollo RFC 3161 garantisce una solida sicurezza contro manomissioni e falsificazioni.
- Flessibilità: capacità di gestire sia singole transazioni che più file, offrendo soluzioni adattate a diverse esigenze.
- Verificabilità: ogni certificazione può essere verificata in modo indipendente, offrendo un elevato livello di trasparenza e fiducia per gli utenti.

Di seguito è riportato un dettaglio di come viene eseguito ogni tipo di certificazione:

Tipo A) Certificazione di un singolo file. Questo processo prevede:

- **Calcolo hash:** l'utente carica il file sulla piattaforma Certifydoc, che calcola automaticamente l'hash SHA256 del file.
- **Richiesta timestamp:** come per le transazioni blockchain, viene generata una query timestamp per l'hash del file.
- **Risposta timestamp:** un certificatore autorizzato emette una risposta di marcatura di tempo qualificata che verifica l'integrità e l'autenticità del file all'ora specificata.

Tipo B) Certificazioni di file multipli con e senza crittografia sorgente avanzata (fino a 17 MB). Questo processo prevede:

- **Creazione del file .zip:** l'utente seleziona diversi file, che Certifydoc comprime in un singolo file .zip.
- **Hash .zip:** viene calcolato l'hash SHA256 dell'intero file .zip.
- **Processo timestamp:** viene seguito lo stesso processo di richiesta e risposta timestamp, certificando il set di file come un'unica entità.

Tipo C) Certificazioni hash file di dimensioni illimitate. Questo processo prevede:

- **Ottenere l'hash SHA256 di file, partizioni, dischi, aree di memoria con uno strumento di terze parti.** In genere solo gli utenti esperti utilizzano questo tipo di processo, ottimizzato per creare copie di backup certificate delle memorie dei dispositivi per indagini giudiziarie da parte di informatici forensi.
- **Processo di marcatura temporale:** viene seguito lo stesso processo di richiesta e risposta di marcatura temporale qualificata, certificando il set di file come un'unica entità.

Tipo D) Certificazione di transazioni blockchain in cui Certifydoc certifica l'hash della transazione blockchain. Questo processo prevede:

- **Ricezione dell'hash**: l'utente fornisce l'hash della transazione blockchain che desidera certificare.
- **Generazione di marcatura temporale**: Certifydoc genera una query di marcatura temporale (.tsq) per l'hash specificato.
- **Certificazione da parte di un'entità autorizzata**: l'hash viene inviato a un servizio di certificazione temporale qualificato, che restituisce una risposta di marcatura temporale (.tsr) che certifica l'ora esatta della transazione.

Il vero obiettivo del progetto è l'analisi del processo di certificazione delle transazioni blockchain (Tipo D), a cui è stata aggiunta anche l'analisi della certificazione dei file (Tipi A, B e C).

4.1. Protocollo Timestamp

Il protocollo Timestamp utilizzato in Certifydoc si basa sullo standard RFC 3161, noto come "Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)." Questo protocollo è fondamentale per l'emissione di timestamp digitali ed è ampiamente riconosciuto e utilizzato nel settore per garantire l'integrità e l'autenticità dei documenti elettronici.

Funzionamento del protocollo Timestamp

- **Definizione e scopo:** il servizio di marcatura temporale consente alle agenzie di fornire documenti elettronici da timbrare. Una marca temporale è una firma elettronica eseguita da una Time Stamping Authority (TSA), che dimostra che i dati sono esistiti e non sono stati alterati da un momento specifico, in base a una fonte di tempo affidabile.

- **Processo tecnico:** il motore Legalization Blockchain genera una query Timestamp (.tsq) che verrà successivamente certificata da un certificatore europeo, che genererà una risposta Timestamp (.tsr).

    - Query Timestamp: è una richiesta inviata a un servizio di certificazione temporale per ottenere una marca temporale associata a dati o eventi specifici. Questa richiesta include generalmente l'hash crittografico di un

documento o di una transazione e richiede un timestamp che certifichi l'ora di occorrenza di tali dati.

- Risposta timestamp: è la risposta del servizio di certificazione temporale che include il timestamp generato, un timestamp digitale che verifica quando i dati specificati nella query sono stati certificati.

Specifiche tecniche RFC 3161

- **Formato messaggio:** RFC 3161 specifica come devono essere strutturati i messaggi di richiesta e risposta, inclusi i campi obbligatori e facoltativi.
- **Algoritmi crittografici:** dettaglia gli algoritmi consigliati per la firma e la verifica dei timestamp, insieme a considerazioni sulla sicurezza per preservare l'integrità e l'autenticità dei timestamp emessi.

Integrazione e applicazione

- **OpenSSL TS (Timestamping)**: questo è un sottoinsieme di OpenSSL specificamente progettato per generare e verificare i timestamp in conformità con lo standard RFC 3161. Offre sia un'interfaccia a riga di comando che un'API programmatica, facilitando l'integrazione in una varietà di applicazioni e sistemi. OpenSSL TS supporta più formati di input e output, rendendolo estremamente versatile e adatto a numerose applicazioni industriali.

Questo standard fornisce una solida base per l'implementazione di servizi di timestamping interoperabili e sicuri ed è fondamentale per il funzionamento efficiente e affidabile del Blockchain Legalization Engine di Certifydoc.

4.2. Regolamento europeo: eIDAS

Nella nostra analisi del Blockchain Legalization Engine e della sua capacità di offrire un'esperienza utente efficiente e sicura, è fondamentale considerare il quadro normativo in cui operano queste tecnologie. Il Regolamento (UE) n. 910/2014, meglio noto come eIDAS, è il quadro normativo che supporta i servizi di certificazione e di timbratura temporanea offerti da piattaforme come Certifydoc.

Solido quadro normativo eIDAS

Il Regolamento eIDAS stabilisce un solido quadro normativo per le transazioni elettroniche all'interno del Mercato unico digitale dell'Unione europea, affrontando specificamente l'identificazione elettronica e i servizi fiduciari come la marcatura temporale elettronica. Questo quadro non solo promuove l'uso di identità elettroniche sicure e affidabili per le transazioni transfrontaliere, ma garantisce anche l'interoperabilità delle marche temporali elettroniche in tutta l'UE.

Impatto e vantaggi di eIDAS

- **Interoperabilità migliorata:** eIDAS garantisce che i sistemi di identificazione elettronica di un paese siano riconosciuti da tutti gli altri Stati membri, promuovendo così efficienza e sicurezza nelle transazioni transfrontaliere.
- **Sicurezza delle transazioni:** questo regolamento aumenta il livello di sicurezza per le transazioni commerciali, riducendo al minimo l'onere amministrativo e i costi, con conseguenti processi aziendali più efficienti e un aumento dei profitti.
- **Fiducia e accettazione legale:** i servizi fiduciari conformi a eIDAS possono essere utilizzati come prova nei procedimenti giudiziari, il che è fondamentale per l'accettazione legale e la validità delle transazioni e delle certificazioni digitali.

Rilevanza di eIDAS per Certifydoc

- **Standard di sicurezza e autenticità:** eIDAS definisce gli standard di sicurezza che servizi come Blockchain Legalization Engine devono soddisfare per garantire l'autenticità e l'integrità delle certificazioni digitali. Ciò è particolarmente pertinente dato che le nostre analisi hanno confermato la robustezza e l'affidabilità della piattaforma Certifydoc nell'emissione di marcature temporali verificate.
- **Interoperabilità nell'UE:** il regolamento semplifica il riconoscimento e l'accettazione dei timestamp emessi da Certifydoc in tutti gli Stati membri dell'UE, il che è fondamentale per le operazioni transfrontaliere e per le aziende che operano su scala europea.
- **Quadro giuridico per i servizi fiduciari:** stabilendo un quadro giuridico per i servizi di timestamp, eIDAS contribuisce a garantire che questi servizi mantengano la loro validità e affidabilità, rafforzando la fiducia nelle soluzioni fornite da Certifydoc ai suoi utenti.

Impatto di eIDAS sull'adozione della tecnologia blockchain

L'inclusione di requisiti per i servizi di marcatura temporale in eIDAS è un passo significativo verso l'integrazione delle tecnologie blockchain nell'ecosistema digitale europeo. Garantendo che i documenti e le transazioni siano sicuri e legalmente convalidati, eIDAS non solo supporta l'adozione della tecnologia, ma promuove anche la fiducia e la sicurezza sulle piattaforme digitali in tutta Europa.

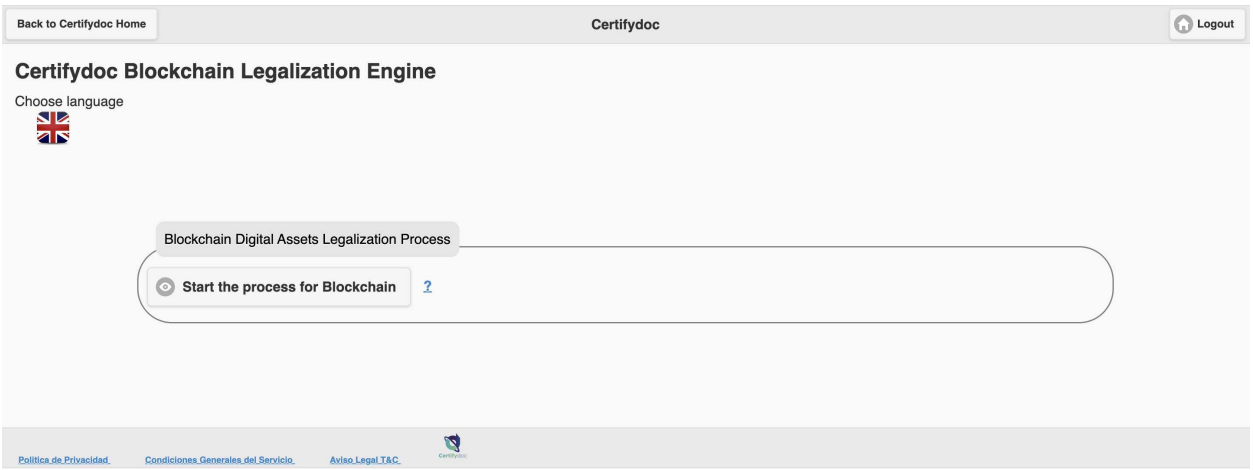
Il quadro fornito da eIDAS è essenziale per il funzionamento e l'espansione di servizi come quelli offerti da Certifydoc. Inoltre, stabilisce le basi legali e tecniche necessarie per un'adozione più ampia di soluzioni di certificazione basate su blockchain, assicurando che queste tecnologie siano armoniosamente integrate nel quadro legale e commerciale dell'Unione europea.

5. Analisi del Blockchain Legalization Engine

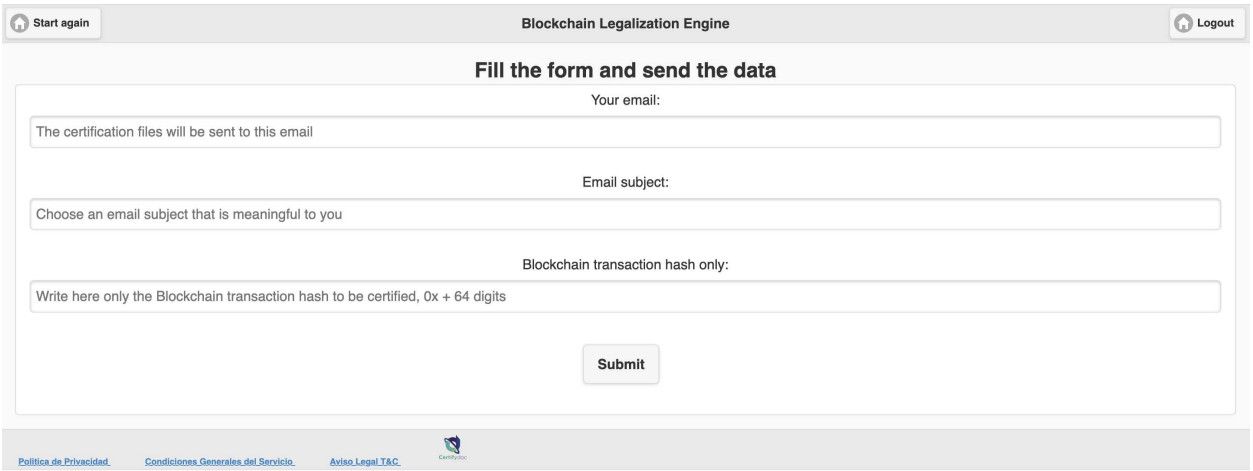
Questa sezione descrive il funzionamento del Blockchain Legalization Engine, descrivendo i protocolli e le procedure utilizzati per la generazione e la certificazione del timestamp, nonché i metodi di interazione tramite l'applicazione web e l'API.

5.1. Certificazione delle transazioni Blockchain tramite applicazione web

Il Blockchain Certification Engine di Certifydoc ha un'applicazione web (https://www.certifydoc.eu/blockchain-legalization-engine/) da cui i clienti possono generare certificati utilizzando un'interfaccia grafica.



Esiste un unico processo per generare certificati di transazione Blockchain:

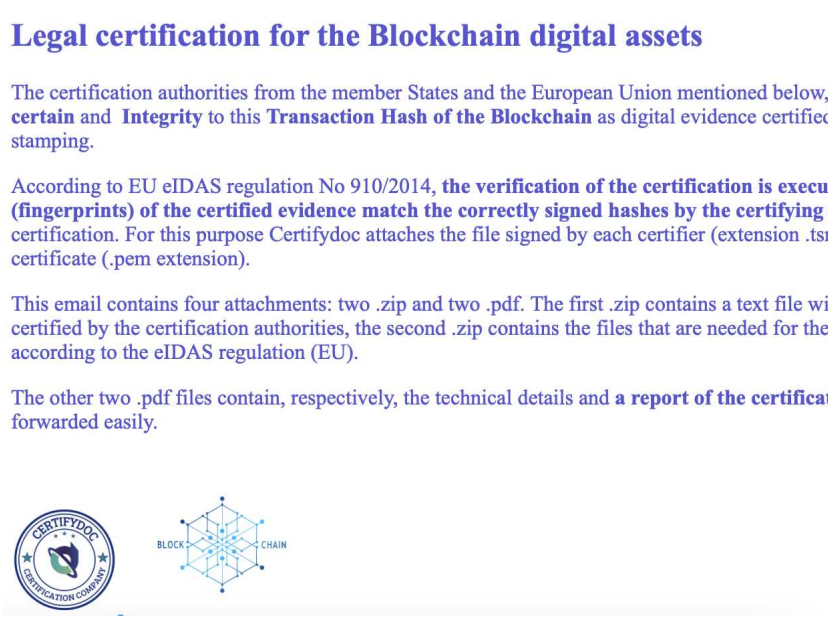


In questo menu l'utente deve completare le seguenti informazioni:

1. **Email:** Email a cui arriverà la certificazione.
2. **Oggetto email:** Oggetto dell'email con la certificazione.
3. **Hash transazione Blockchain:** Hash esadecimale della transazione Blockchain da certificare.

Una volta inviato il modulo, l'utente consuma una certificazione.

L'utente riceverà un'email con informazioni e una serie di documenti relativi alla certificazione:



Legal certification for the Blockchain digital assets

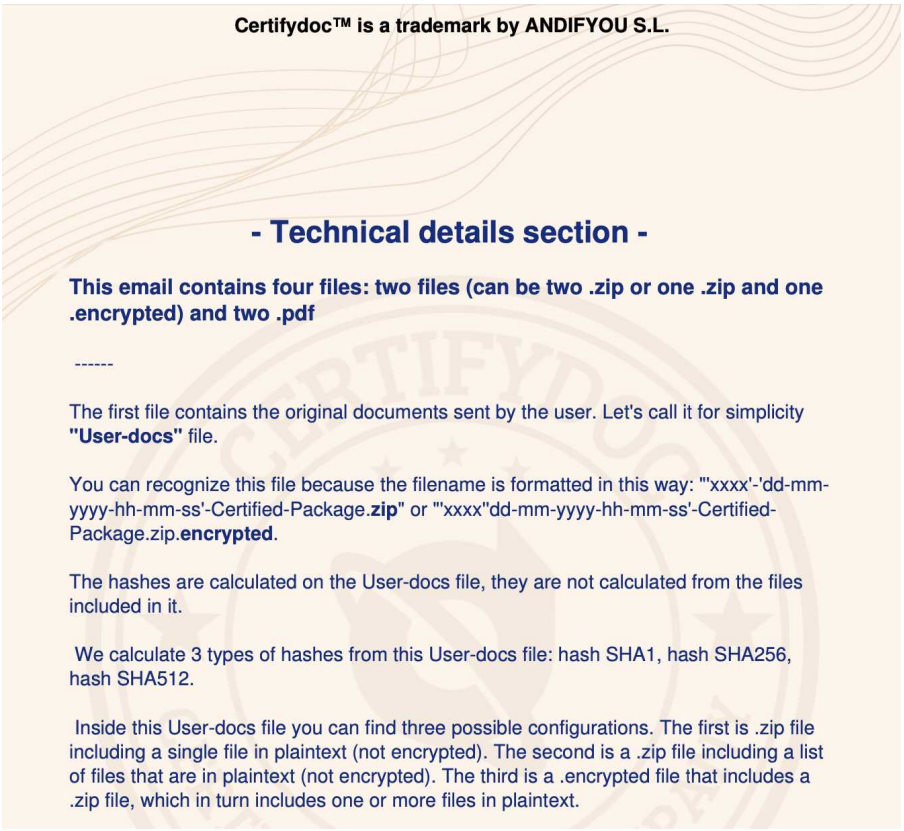
The certification authorities from the member States and the European Union mentioned below, grant **Jurisdiction**, **Date certain** and **Integrity** to this **Transaction Hash of the Blockchain** as digital evidence certified through qualified time stamping.

According to EU eIDAS regulation No 910/2014, **the verification of the certification is executed checking that the hashes (fingerprints) of the certified evidence match the correctly signed hashes by the certifying authority** at the time of certification. For this purpose Certifydoc attaches the file signed by each certifier (extension .tsr) and its relative public certificate (.pem extension).

This email contains four attachments: two .zip and two .pdf. The first .zip contains a text file with the transaction hash certified by the certification authorities, the second .zip contains the files that are needed for the verification operation according to the eIDAS regulation (EU).

The other two .pdf files contain, respectively, the technical details and **a report of the certification to be printed** or forwarded easily.

1. **Dettagli tecnici:** file PDF che spiega i dettagli tecnici degli altri file nell'e-mail.



Certifydoc™ is a trademark by ANDIFYOU S.L.

- Technical details section -

This email contains four files: two files (can be two .zip or one .zip and one .encrypted) and two .pdf

---

The first file contains the original documents sent by the user. Let's call it for simplicity **"User-docs"** file.

You can recognize this file because the filename is formatted in this way: "'xxxx'-'dd-mm-yyyy-hh-mm-ss'-Certified-Package.**zip**" or "'xxxx"dd-mm-yyyy-hh-mm-ss'-Certified-Package.zip.**encrypted**.

The hashes are calculated on the User-docs file, they are not calculated from the files included in it.

We calculate 3 types of hashes from this User-docs file: hash SHA1, hash SHA256, hash SHA512.

Inside this User-docs file you can find three possible configurations. The first is .zip file including a single file in plaintext (not encrypted). The second is a .zip file including a list of files that are in plaintext (not encrypted). The third is a .encrypted file that includes a .zip file, which in turn includes one or more files in plaintext.

2. **Report di certificazione**: il file PDF è una spiegazione della certificazione. È importante notare che questo file rappresenta solo un report esplicativo della certificazione. Nel caso di un esperto forense, il valore legale del certificato è costituito dai file di risposta .tsr e dal certificato pubblico .pem dell'autorità di certificazione.

Certifydoc™ is a trademark by ANDIFYOU S.L.

Report of Legal certification for the digital files

The certification authorities from the member States and the European Union mentioned below, grant **Jurisdiction**, **Date certain** and **Integrity** to digital evidence certified through qualified time stamping.

According to EU eIDAS regulation No 910/2014, **the verification of the certification is executed checking that the hashes (fingerprints) of the certified evidence match the correctly signed hashes by the certifying authority** at the time of certification. For this purpose Certifydoc attaches the file signed by each certifier (extension .tsr) and its relative public certificate (.pem extension).

Date certain: 19

Certified

3. **Dati utente**: file ZIP contenente un .txt con l'hash della transazione Blockchain certificata.

```
→  Downloads cat 7168-19-04-2024-07-38-57--hash256-uploaded.txt
You uploadad to Certifydoc, for its certification, the following transaction hash, you can
copy and paste it in the blockchain portal to validate it exists in the Blockchain: 0x5febc
690cf8f9d884c91909f6f5179bb7ec4e9a53346c83c7f339f827f000eef%
```

4. **Certificazione**: file ZIP contenente la certificazione e i file necessari per verificarla.

```
1519807286XJTlEf-Namirial.tsr                2078436848b5fOwW-customer.txt
1519807286XJTlEf-Namirial.tsr-readable.txt   547857767dhS2MS-Izenpe.tsq
1541346359uvbg1C-Namirial.tsq                98130948697UKkK-hash-sha256.txt
1713096163gmX1Kc-Izenpe.tsr                  Izenpe-RAIZQC_cert_signing_0.pem
1713096163gmX1Kc-Izenpe.tsr-readable.txt     NamirialCATSA.pem
```

5.2. Certificazione delle transazioni Blockchain tramite API

Il Blockchain Legalization Engine di Certifydoc ha un'API che ci consente di generare certificazioni in modo programmatico. L'API ha 4 diversi possibili processi:

1. **Email Response**: l'API ci invierà un'e-mail con i file. Questo processo ha lo stesso risultato della certificazione tramite Web.

   https://www.certifydoc.eu/wp-json/certifydocapi/v1/sdbx-notarization-api/

   ?submitethereum=submitethereum

   &hashethereum=0x9c820dc62b09fcb517ff22d4888d06c8cc858d59cbeff8830865814a852e1a3

   &response_type=email_response

   &emailsubjectethereum=Test API sandbox Blockchain to email En 230508

   &emailethereum=email@dominio.es

   &language=en

2. **API response complete:** riceviamo gli stessi file dell'e-mail ma come risposta dall'API. I file sono codificati in base64.

   https://www.certifydoc.eu/wp-json/certifydocapi/v1/sdbx-notarization-api/

   ?submitethereum=submitethereum

   &hashethereum=0x9c820dc62b09fcb517ff22d4888d06c8cc858d59cbeff8830865814a852e1a3

   &response_type=api_response

   &api_response_options=complete

   &language=en

3. **API response reduced:** riceviamo la risposta tramite l'API. Ci invia la risposta Timestamp (.tsr), il certificato CA (.pem) e il report di certificazione (.pdf). I file sono codificati in base64.

   https://www.certifydoc.eu/wp-json/certifydocapi/v1/sdbx-notarization-api/

   ?submitethereum=submitethereum

   &hashethereum=0xa85c41d8ffd5212a7537b4556eb8c748b723fbb51a56f67b7961e830087adb6b

   &response_type=api_response

   &api_response_options=reduced

&language=en

4. **API response minimized:** riceviamo la risposta tramite l'API. Ci invia la risposta Timestamp (.tsr) e il certificato CA (.pem). I file sono codificati in base64.

   https://www.certifydoc.eu/wp-json/certifydocapi/v1/sdbx-notarization-api/

   ?submitethereum=submitethereum

   &hashethereum=0xea586e91e71a09e9fb27fa1cfbfdeea582269f2bc30da37d8ed75b6facc6bea7

   &response_type=api_response

   &api_response_options=minimized

   &language=en

5.3. Processo di verifica

Possiamo verificare le informazioni contenute nei diversi file:

1. El **Timestam Query** (.tsq) contiene informazioni utili come l'hash da certificare. Puoi verificarne i dati eseguendo il comando:

   ```
   openssl ts -query -in <tsq_filename>.tsq -text
   ```

   ```
   Version: 1
   Hash Algorithm: sha256
   Message data:
       0000 - 72 aa 7f 8b 4c 04 b3 e2-cf d8 41 c0 aa 90 dc fe   r...L.....A.....
       0010 - 80 7f 38 12 46 44 76 78-74 d3 27 e7 2d 7b 4b f2   ..8.FDvxt.'.-{K.
   Policy OID: unspecified
   Nonce: 0xFD1C6DF7F100FF79
   Certificate required: yes
   Extensions:
   ```

2. La **Timestamp Response** (.tsr) contiene informazioni utili come l'hash del certificato e il timestamp del certificato. Puoi verificarne i dati eseguendo il comando:

   ```
   openssl ts -reply -in <tsr_filename>.tsr -text
   ```

```
Version: 1
Policy OID: 0.4.0.2023.1.1
Hash Algorithm: sha256
Message data:
    0000 - 72 aa 7f 8b 4c 04 b3 e2-cf d8 41 c0 aa 90 dc fe   r...L.....A.....
    0010 - 80 7f 38 12 46 44 76 78-74 d3 27 e7 2d 7b 4b f2   ..8.FDvxt.'.-{K.
Serial number: 0x3DD0A8286AE7A1EF
Time stamp: Apr 30 12:53:38 2024 GMT
Accuracy: 0x01 seconds, unspecified millis, unspecified micros
Ordering: no
Nonce: 0xFD1C6DF7F100FF79
TSA: unspecified
Extensions:
```

3. El **CA certificate** (.pem) contiene informazioni utili come il CN del certificatore. Puoi verificare i tuoi dati eseguendo il comando:

```
openssl x509 -in <pem_filename>.pem -text -noout
```

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 2362980985481067158 (0x20cafeafca99fa96)
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = IT, O = Namirial S.p.A./02046570426, OU = Certification Authority, CN = Namirial CA TSA
        Validity
            Not Before: Nov 24 15:01:35 2010 GMT
            Not After : Nov 24 15:01:35 2030 GMT
        Subject: C = IT, O = Namirial S.p.A./02046570426, OU = Certification Authority, CN = Namirial CA TSA
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:ab:3e:a2:79:55:77:ee:a1:b3:a9:dc:2c:02:30:
                    e4:74:7a:36:a9:f2:92:39:db:fb:50:26:b0:90:9b:
                    a3:d5:09:74:e5:7d:ff:57:80:79:23:1e:9a:50:71:
                    4c:c3:bb:71:7e:9e:01:c2:11:cb:70:51:2d:ab:d4:
                    37:77:84:11:86:ab:c3:b3:f4:63:0d:dc:da:ce:44:
                    84:3f:c1:4f:9a:04:d4:ec:7a:62:82:79:cc:62:a2:
                    33:c8:c1:e2:f8:aa:77:0f:69:7e:93:fd:34:3d:10:
                    7c:75:4b:2c:5c:fd:17:e2:15:45:ee:74:be:78:95:
                    21:02:5b:6a:73:71:cc:d5:da:4f:69:9a:46:11:9c:
                    8c:6f:73:07:c0:69:96:d6:6f:b5:0e:09:e1:dd:ed:
                    bc:98:e7:15:1f:3e:15:b7:fe:92:da:11:76:95:f9:
                    da:ec:dd:a9:55:80:3e:9d:62:3d:cf:58:77:b9:b4:
                    a5:c6:1f:67:19:11:74:6e:55:72:f1:1b:8c:89:54:
                    8e:99:26:af:99:06:bd:70:55:52:2e:85:cb:a9:6f:
                    67:f4:bf:bf:ad:87:f5:4b:9c:0f:30:ef:73:b5:ee:
                    af:62:d7:97:58:58:2c:e1:1f:a7:29:15:22:47:1e:
                    7b:0a:cc:2d:89:b4:8d:6e:4f:59:b3:4b:05:ab:b8:
                    af:87
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            Authority Information Access:
                OCSP - URI:http://ocsp.firmacerta.it/ocsp/certstatus
            X509v3 Subject Key Identifier:
                96:BE:FC:C7:A7:57:72:AD:82:5A:61:AE:E6:AF:90:98:9D:A1:11:5D
            X509v3 Basic Constraints: critical
```

Una volta verificato che i file hanno il contenuto previsto, possiamo verificare il certificato eseguendo il seguente comando:

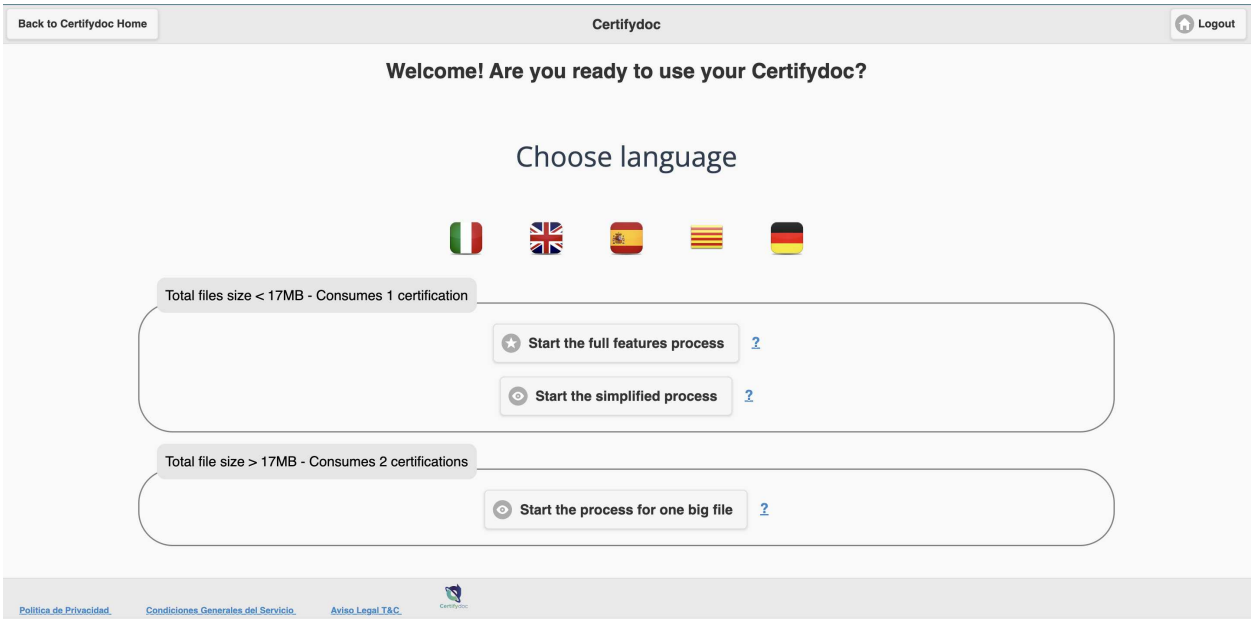
```
openssl ts -verify -in <tsr_filename>.tsr -CAfile <pem_filename>.pem -digest $(cat <trasaction_to_verify>.txt)
```

6. Certificazione dei file

Questa sezione descrive in dettaglio il funzionamento della certificazione dei file, descrivendo i protocolli e le procedure utilizzati per la generazione e la certificazione del timestamp, nonché i metodi di interazione tramite l'applicazione web e l'API.

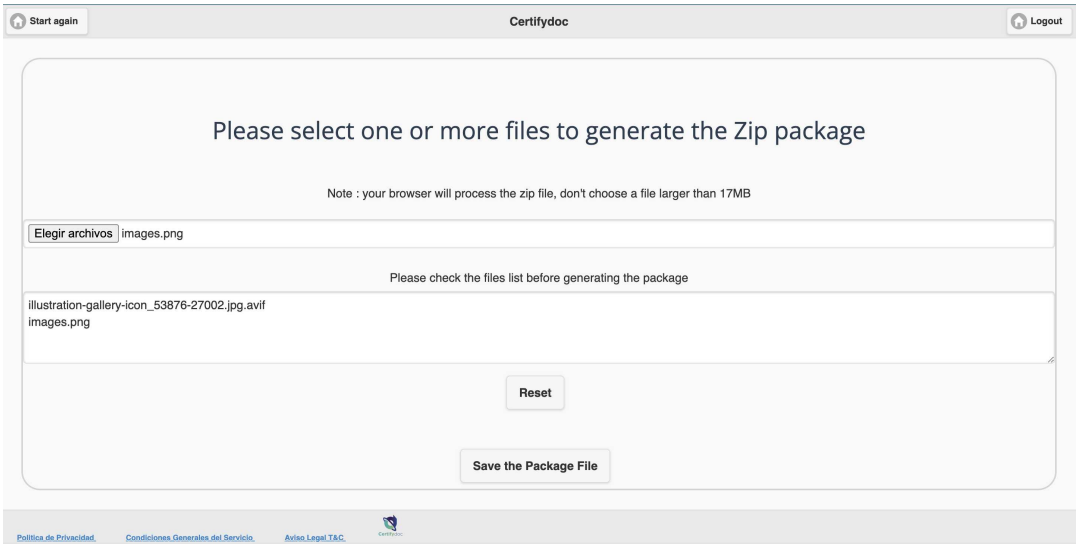
6.1. Certificazione dei file tramite applicazione web

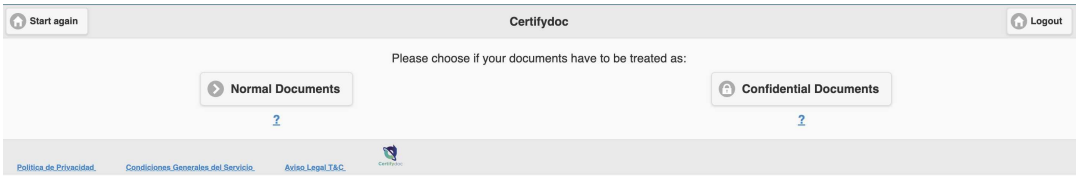
La certificazione dei file Certifydoc ha un'applicazione web (https://www.certifydoc.eu/certification/) da cui i client possono generare certificati utilizzando un'interfaccia grafica.

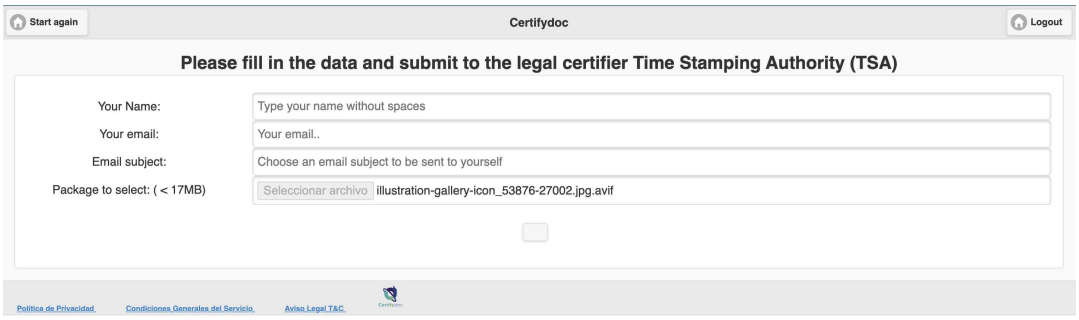


L'applicazione web ha 3 processi diversi:

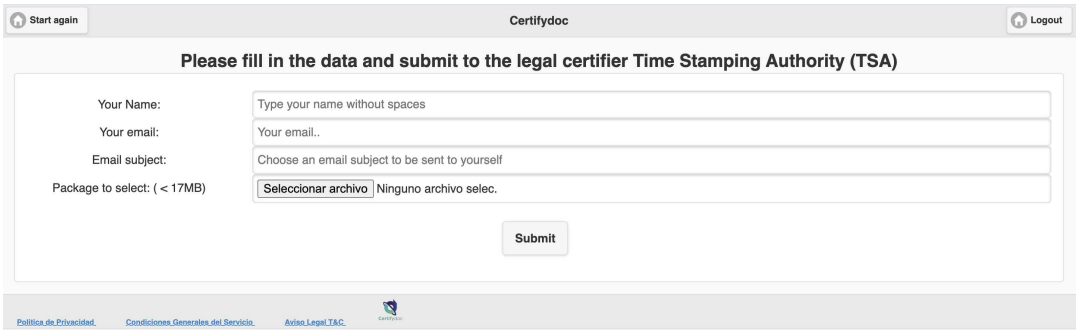
1. **Processo completo**: puoi caricare più file, che verranno salvati in uno ZIP. Puoi anche crittografare il contenuto. Ha una limitazione di 17 MB.



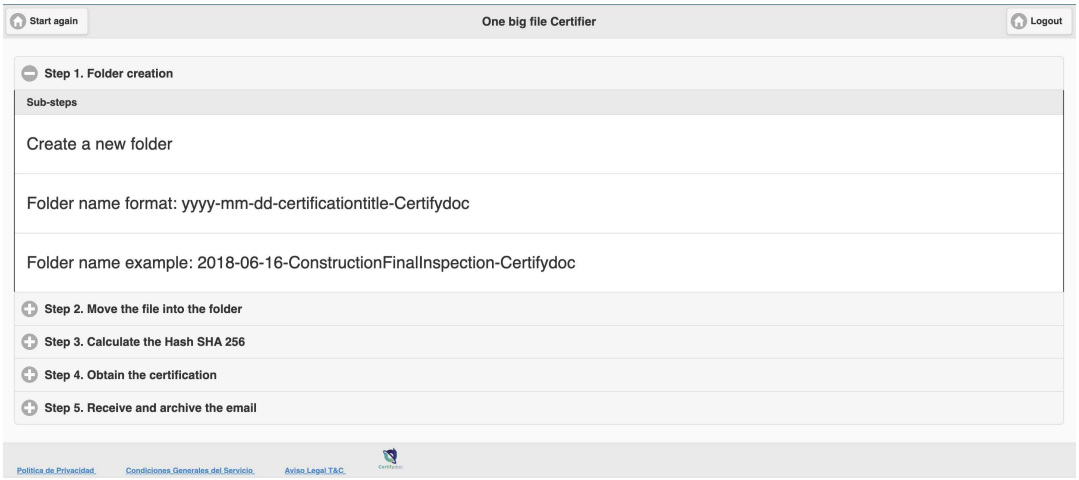


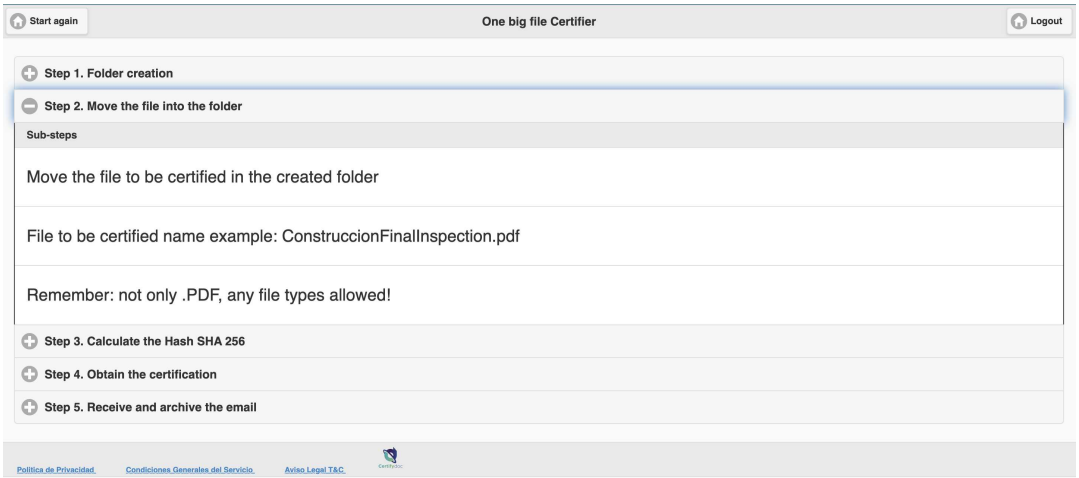


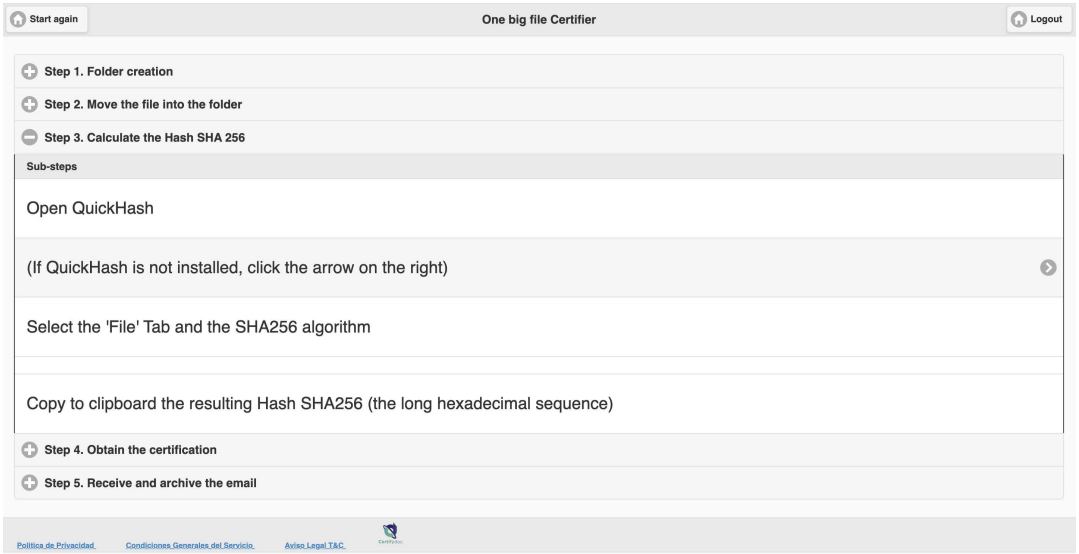
2. **Processo semplificato**: puoi caricare solo un singolo file. Ha una limitazione di 17 MB.

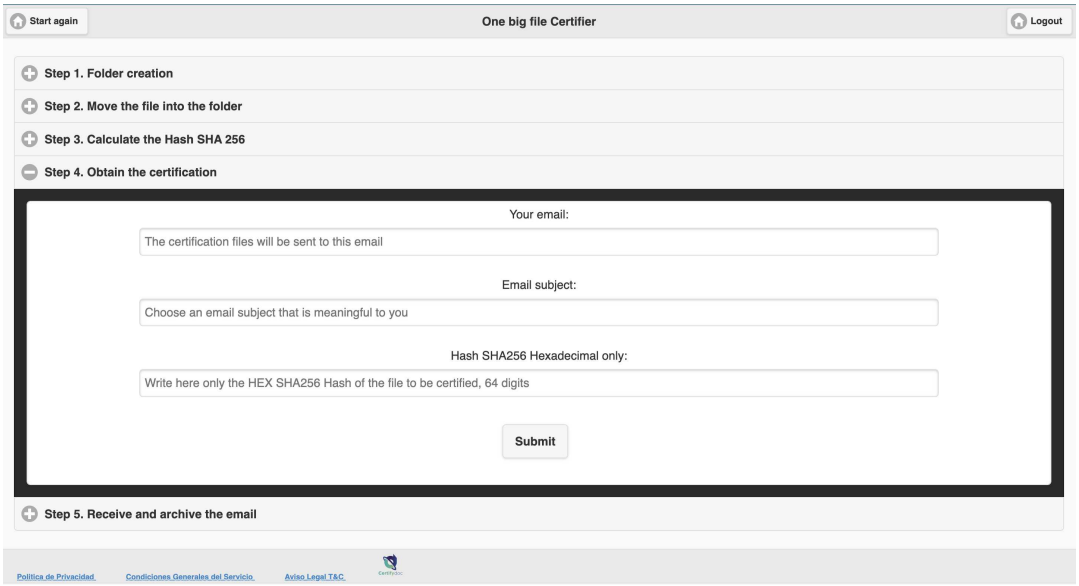


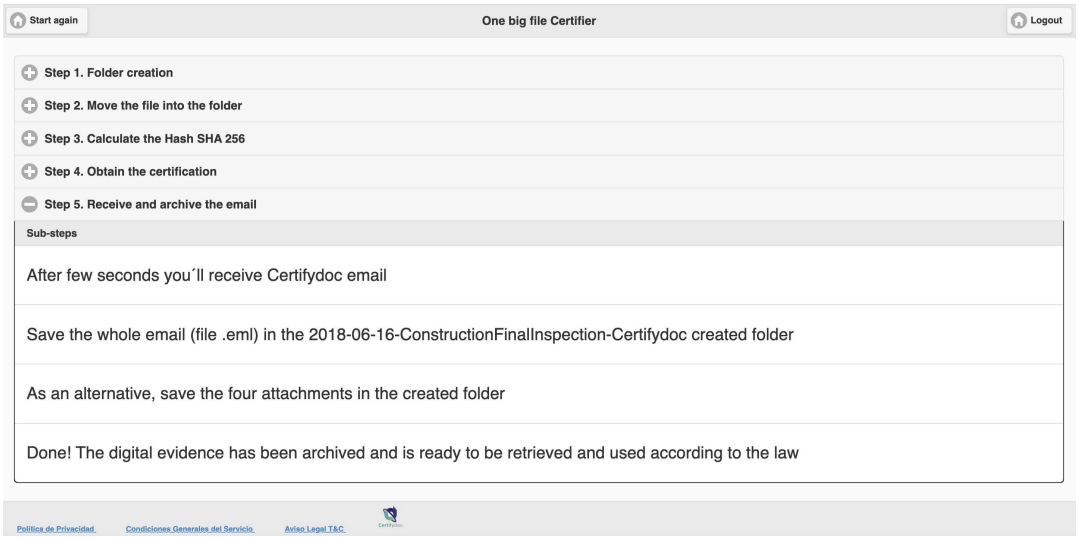
3. **Processo per un singolo file di grandi dimensioni**: puoi caricare l'hash sha256 di un singolo file o di una porzione del file system senza limitazioni di dimensione. Questo file può essere uno ZIP o un intero disco rigido, quindi per scopi pratici puoi certificare più file.


Start again
One big file Certifier
Logout
Step 1. Folder creation
Sub-steps
Create a new folder
Folder name format: yyyy-mm-dd-certificationtitle-Certifydoc
Folder name example: 2018-06-16-ConstructionFinalInspection-Certifydoc
Step 2. Move the file into the folder
Step 3. Calculate the Hash SHA 256
Step 4. Obtain the certification
Step 5. Receive and archive the email
Política de Privacidad
Condiciones Generales del Servicio
Aviso Legal T&C


Start again
One big file Certifier
Logout
Step 1. Folder creation
Step 2. Move the file into the folder
Sub-steps
Move the file to be certified in the created folder
File to be certified name example: ConstruccionFinalInspection.pdf
Remember: not only .PDF, any file types allowed!
Step 3. Calculate the Hash SHA 256
Step 4. Obtain the certification
Step 5. Receive and archive the email
Política de Privacidad
Condiciones Generales del Servicio
Aviso Legal T&C


Start again
One big file Certifier
Logout
Step 1. Folder creation
Step 2. Move the file into the folder
Step 3. Calculate the Hash SHA 256
Sub-steps
Open QuickHash
(If QuickHash is not installed, click the arrow on the right)
Select the 'File' Tab and the SHA256 algorithm
Copy to clipboard the resulting Hash SHA256 (the long hexadecimal sequence)
Step 4. Obtain the certification
Step 5. Receive and archive the email
Política de Privacidad
Condiciones Generales del Servicio
Aviso Legal T&C





6.2. Certificazione dei file tramite API

Possiamo anche certificare i file tramite API. Ci sono 4 possibili processi (sono gli stessi di Blockchain Legalization Engine):

1. **Email response:** l'API ci invierà un'email con i file. Questo processo ha lo stesso risultato della certificazione tramite web.
2. **API response complete:** riceviamo gli stessi file dell'email ma come risposta dall'API. I file sono codificati in base64.
3. **API response reduced:** riceviamo la risposta tramite API. Ci invia la risposta Timestamp (.tsr), il certificato CA (.pem) e il report di certificazione (.pdf). I file sono codificati in base64.
4. **API response minimized:** riceviamo la risposta tramite API. Ci invia la risposta Timestamp (.tsr) e il certificato CA (.pem). I file sono codificati in base64.

6.3. Verifica certificazione dei file

Quando verifichiamo la certificazione dei file, ciò che stiamo verificando è se la Timestamp Response (.tsr) contiene l'hash SHA256 del file da verificare e se è stato firmato da un'autorità di certificazione. Abbiamo due possibilità:

1. Se abbiamo certificato un solo file, la Timestamp Response contiene l'hash SHA256 del file.

   ```
   openssl ts -verify -in <tsr_filename>.tsr -CAfile <pem_filename>.pem -data
   <file_to_verify>
   ```

2. Se abbiamo certificato più file, la Timestamp Response contiene l'hash SHA256 dello ZIP dei file.

```
penssl ts -verify -in <tsr_filename>.tsr -CAfile <pem_filename>.pem -data <zip_to_verify>.zip
```

7. Conclusioni

Dopo un'analisi esaustiva che ha comportato l'uso ripetuto sia dell'applicazione Web che dell'API della certificazione dei file e del Blockchain Legalization Engine di Certifydoc utilizzando un approccio di test Black Box, sono stati ottenuti risultati coerenti e soddisfacenti in tutte le certificazioni eseguite.

Attraverso molteplici interazioni con la piattaforma, tutte le certificazioni emesse sono state verificate senza riscontrare alcun inconveniente significativo. Questo processo di verifica ha comportato la creazione di marcature temporali qualificate con l'hash delle transazioni Ethereum, e di tutte le transazioni da altre blockchain con lo stesso formato esadecimale, successivamente la loro certificazione usando il servizio di Certifydoc. Oltre alla stessa verifica per il processo di certificazione dei file.

Sia l'applicazione Web Certifydoc che l'API hanno dimostrato di offrire un'esperienza utente fluida ed efficiente. L'interfaccia utente dell'applicazione Web è intuitiva e facile da usare, facilitando il processo di certificazione delle transazioni. Allo stesso modo, l'API ha dimostrato di essere robusta e affidabile, consentendo un'interazione programmatica con la piattaforma in modo efficace.

Durante il processo di verifica della certificazione tramite OpenSSL, è stata confermata l'autenticità e la validità di tutte le certificazioni emesse da Certifydoc. Lo strumento OpenSSL ha convalidato con successo i timestamp generati, supportando l'integrità del processo di certificazione temporale implementato dalla piattaforma.

In sintesi, i risultati ottenuti indicano che lo strumento Certifydoc Blockchain Certification Engine (BLM) e il processo di certificazione dei file funzionano correttamente e soddisfano il loro scopo di certificare le transazioni Blockchain e file in modo affidabile e accurato.

Questi risultati sono incoraggianti e supportano l'efficacia della piattaforma come soluzione praticabile per la certificazione temporale e di integrità nel contesto delle transazioni Ethereum e delle transazioni su altre blockchain che presentano lo stesso formato esadecimale. Anche la certificazione dei file è stata verificata funzionare correttamente.