



**UNIVERSITAT POLITÈCNICA
DE CATALUNYA
BARCELONATECH**

Memoria técnica del proyecto

Versiones del documento

Versión:	Modificaciones:	Realizado por:
V1.0	Creación del documento	UPC
V2.0	Definición técnica	UPC

Índice

1. Requisitos y contexto del proyecto.....	4
2. Definición técnica del problema.....	5
3. Metodología de análisis de Certifydoc.....	5
4. Proceso de certificación de Certifydoc.....	7
4.1. Timestamp Protocol.....	8
4.2. Regulación Europea: eIDAS.....	9
5. Análisis Blockchain Legalization Engine.....	11
5.1. Certificación de transacciones Blockchain vía aplicación web.....	11
5.2. Certificación de transacciones Blockchain vía API.....	14
5.3. Proceso de verificación.....	15
6. Certificación de archivos.....	17
7. Conclusiones.....	22

1. Requisitos y contexto del proyecto

Este proyecto consiste en el análisis y validación del Blockchain Legalization Engine (BLE) de Certifydoc, una solución diseñada para notarizar con relevancia legal los datos almacenados en blockchain. La plataforma BLE actúa como un intermediario entre los datos en blockchain y los prestadores de servicio de confianza cualificados de la UE.

Durante el transcurso del proyecto también se ha realizado el análisis y validación de la certificación de ficheros de Certifydoc.

El servicio es accesible on-demand y se ofrece en modalidad de Software as a Service, pudiendo interactuar con el sistema a través de formulario web o mediante una API REST. A su vez, los resultados de la notarización pueden estar disponibles vía email o mediante la API REST.

Requisitos del proyecto

El proyecto requiere la ejecución de varias fases para garantizar su viabilidad técnica y comercial:

- **Ensayos y experimentación:** Validar la propuesta técnica mediante pruebas de concepto, tanto tecnológicas como con usuarios finales, para verificar la funcionalidad y usabilidad del servicio.
- **Asesoramiento técnico y de proceso:** Consultoría para mejorar procesos y aspectos tecnológicos basados en los resultados de las pruebas iniciales.
- **Evaluación de seguridad y rendimiento:** Pruebas específicas para asegurar la integridad y protección de los datos, así como la estabilidad y rendimiento del sistema en escenarios de uso real.
- **Informe de viabilidad:** Desarrollo de un informe detallado que concluya los hallazgos de las pruebas y valide la propuesta del proyecto.

Contexto del proyecto

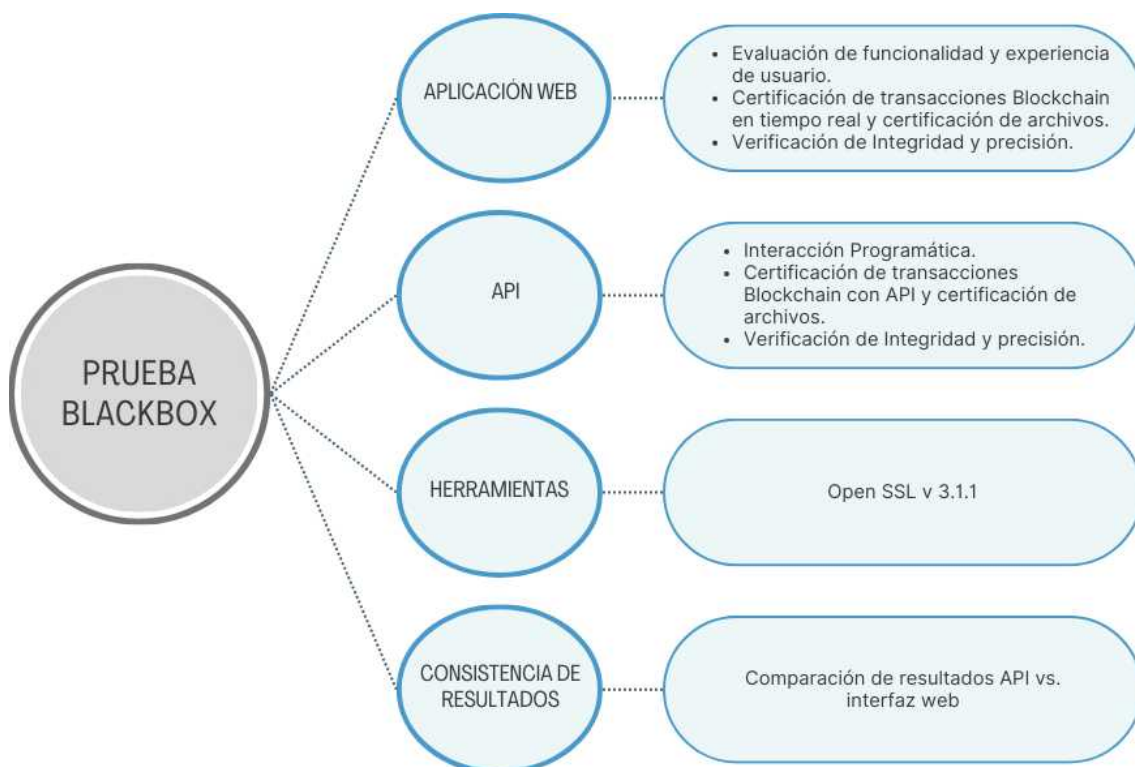
Este proyecto se enmarca dentro de la Propuesta de Servicios del Programa de Apoyo a Digital Innovation Hubs, buscando explorar y expandir las posibilidades de la notarización de documentos con relevancia legal a las tecnologías blockchain. La solución BLE no solo propone una innovación tecnológica sino que también se alinea con las necesidades actuales de digitalización y seguridad documental en la Unión Europea, ofreciendo un enfoque práctico y escalable que puede ser adoptado en diversos sectores y aplicaciones.

2. Definición técnica del problema

Asesoramiento y evaluación sobre los servicios de certificación de Certifydoc; plataforma Blockchain Legalization Engine que ofrece servicios de certificación de transacciones de Blockchain mediante la creación de timestamps con el hash de la transacción y su posterior certificación a través de un certificador europeo, y plataforma de certificación de ficheros. El análisis se ha llevado a cabo utilizando una metodología Black Box.

3. Metodología de análisis de Certifydoc

El análisis del Blockchain Legalization Engine (BLE) y certificación de ficheros de Certifydoc se ha llevado a cabo utilizando un enfoque de caja negra (Black Box), evaluando la aplicación desde una perspectiva externa sin acceder al código fuente o a la estructura interna del sistema.



Este análisis se realizó desde dos interfaces distintas para proporcionar una evaluación integral:

1. Desde la aplicación web de Certifydoc:

- a. Acceso como usuario normal: Se accedió a la aplicación web de Certifydoc como un usuario típico para evaluar tanto la funcionalidad general como la experiencia de usuario. Esto incluyó la navegación por la interfaz, la gestión de cuentas y la ejecución de funciones básicas.

- b. Certificación de transacciones blockchain y archivos: Se realizaron pruebas de certificación de transacciones a través de la interfaz de usuario para observar el proceso de certificación en tiempo real y evaluar la facilidad de uso y la accesibilidad del sistema. Así como pruebas de certificación de archivos.
- c. Verificación de integridad y precisión: Se comprobó la integridad y la precisión de la información proporcionada durante el proceso de certificación, asegurando que los datos mostrados y los resultados fueran consistentes y confiables.

2. Utilizando la API de Certifydoc:

- a. Interacción programática: Se utilizó la API proporcionada por Certifydoc para interactuar con la plataforma de manera programática, lo que permitió evaluar la flexibilidad y la capacidad de integración del servicio.
- b. Certificación de transacciones blockchain y archivos: Se ejecutaron certificaciones de transacciones de blockchain utilizando las diversas funciones disponibles en la API, con el objetivo de probar la robustez y la eficiencia de estas interfaces programáticas. Así como pruebas de certificación de archivos.
- c. Verificación de integridad y precisión: Se comprobó la integridad y la precisión de la información proporcionada durante el proceso de certificación, asegurando que los datos mostrados y los resultados fueran consistentes y confiables.
- d. Consistencia de resultados: Se verificó la consistencia de los resultados obtenidos a través de la API en comparación con los generados a través de la interfaz web, asegurando que ambas plataformas proporcionaran resultados equivalentes.

Herramientas de verificación:

Para la verificación de la validez de las certificaciones, se utilizó OpenSSL (versión 3.1.1), una biblioteca criptográfica de código abierto que facilita la implementación de protocolos de seguridad. Este software permitió confirmar la autenticidad y la seguridad de las certificaciones generadas por BLE, asegurando que el sistema cumple con los estándares de seguridad actuales.

4. Proceso de certificación de Certifydoc

Certifydoc emplea tecnología avanzada para certificar tanto transacciones en blockchain como archivos digitales, asegurando la autenticidad e integridad de los datos mediante la creación de timestamp verificable.

Proceso técnico común

Para todos los tipos de certificación, Certifydoc utiliza técnicas de criptografía segura para garantizar que los timestamps y las certificaciones sean irrefutables y legalmente válidas. Además, utiliza el estándar RFC 3161 para garantizar la compatibilidad y reconocimiento global de las certificaciones. Cada certificación emitida por Certifydoc puede ser verificada de manera independiente mediante herramientas como OpenSSL, proporcionando transparencia y confiabilidad.

Ventajas del proceso

- **Seguridad:** El uso de hash SHA256 y el protocolo RFC 3161 garantiza una seguridad robusta contra alteraciones y falsificaciones.
- **Flexibilidad:** Capacidad para manejar tanto transacciones individuales como múltiples archivos, ofreciendo soluciones adaptadas a diversas necesidades.
- **Verificabilidad:** Cada certificación puede ser verificada de forma independiente, ofreciendo un alto nivel de transparencia y confianza para los usuarios.

A continuación, se detalla cómo se realizan cada tipo de certificación:

Tipo A) Certificación de un archivo único. Este proceso implica:

- **Cálculo del hash:** El usuario sube el archivo a la plataforma de Certifydoc, que automáticamente calcula el hash SHA256 del archivo.
- **Solicitud de timestamp:** Al igual que con las transacciones blockchain, se genera una consulta de timestamp para el hash del archivo.
- **Respuesta de timestamp:** Un certificador autorizado emite una respuesta de timestamp que verifica la integridad y autenticidad del archivo en el momento especificado.

Tipo B) Certificaciones de múltiples archivos con y sin cifrado fuerte a la fuente (hasta 17 MB). Este proceso implica:

- **Creación del archivo .zip:** El usuario selecciona varios archivos, que Certifydoc comprime en un único archivo .zip.
- **Hash del .zip:** Se calcula el hash SHA256 del archivo .zip completo.
- **Proceso de timestamp:** Se sigue el mismo proceso de solicitud y respuesta de timestamp, certificando el conjunto de archivos como una única entidad.

Tipo C) Certificaciones del hash de ficheros ilimitados. Este proceso implica:

- **Obtener con herramienta de terceros el Hash SHA256 de ficheros, particiones, discos, areas de memoria.** Normalmente solo los usuarios expertos usan este tipo de proceso, optimizado para crear copias de seguridad certificadas de memorias de dispositivos para investigaciones judiciales de los informáticos forenses.
- **Proceso de timestamp:** Se sigue el mismo proceso de solicitud y respuesta de timestamp, certificando el conjunto de archivos como una única entidad.

Tipo D) Certificación de transacciones blockchain en las que Certifydoc certifica el hash de la transacción de blockchain. Este proceso implica:

- **Recepción del hash:** El usuario proporciona el hash de la transacción de blockchain que desea certificar.
- **Generación de timestamp:** Certifydoc genera una consulta de timestamp (.tsq) para el hash proporcionado.
- **Certificación por entidad autorizada:** El hash se envía a un servicio de certificación de tiempo cualificado, que devuelve una respuesta de timestamp (.tsr) certificando el momento exacto de la transacción.

El objetivo real del proyecto es el análisis del proceso de certificación de transacciones blockchain (Tipo D), adicionalmente se ha añadido el análisis de certificación de archivos (Tipos A, B y C).

4.1. Timestamp Protocol

El Timestamp Protocol que se utiliza en Certifydoc se basa en el estándar RFC 3161, conocido como "Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)". Este protocolo es fundamental para la emisión de sellos de tiempo digitales, y es ampliamente reconocido y utilizado en la industria para garantizar la integridad y autenticidad de los documentos electrónicos.

Funcionamiento del timestamp protocol

- **Definición y propósito:** El servicio de sellado de tiempo permite a los organismos suministrar documentos electrónicos para ser sellados. Un sello de tiempo es una firma electrónica realizada por una Autoridad de Sellado de Tiempo (TSA), demostrando que los datos han existido y no han sido alterados desde un momento específico, basado en una fuente fiable de tiempo.
- **Proceso técnico:** El Legalization Blockchain Engine genera una Timestamp Query (.tsq) que, posteriormente, será certificada por un certificador europeo, el cual generará una Timestamp Response (.tsr).
 - **Timestamp query:** Es una solicitud enviada a un servicio de certificación de tiempo para obtener un timestamp asociado a un dato o evento específico. Esta solicitud generalmente incluye el hash criptográfico de un documento o transacción, y pide un timestamp que certifique el momento de ocurrencia de ese dato.

- **Timestamp response:** Es la respuesta del servicio de certificación de tiempo que incluye el timestamp generado, una marca de tiempo digital que verifica cuándo se certificó el dato especificado en la consulta.

Especificaciones técnicas del RFC 3161

- **Formato de mensajes:** El RFC 3161 especifica cómo deben estructurarse los mensajes de solicitud y respuesta, incluyendo los campos obligatorios y opcionales.
- **Algoritmos criptográficos:** Detalla los algoritmos recomendados para firmar y verificar los timestamps, junto con las consideraciones de seguridad para preservar la integridad y autenticidad de los timestamps emitidos.

Integración y aplicación

- **OpenSSL TS (Timestamping):** Este es un subconjunto de OpenSSL específicamente diseñado para generar y verificar sellos de tiempo de acuerdo con el estándar RFC 3161. Ofrece tanto una interfaz de línea de comandos como una API programática, facilitando la integración en una variedad de aplicaciones y sistemas. OpenSSL TS es compatible con múltiples formatos de entrada y salida, lo que lo hace extremadamente versátil y adecuado para numerosas aplicaciones industriales.

Este estándar proporciona una base sólida para la implementación de servicios de estampado de tiempo interoperables y seguros, y es crucial para el funcionamiento eficaz y confiable del Blockchain Legalization Engine de Certifydoc.

4.2. Regulación Europea: eIDAS

A lo largo de nuestro análisis del Blockchain Legalization Engine y su capacidad para ofrecer una experiencia de usuario eficiente y segura, es crucial considerar el marco regulatorio en el que estas tecnologías operan. La regulación (UE) N° 910/2014, más conocida como eIDAS, es el marco legal que respalda los servicios de certificación y sellado temporal ofrecidos por plataformas como Certifydoc.

Marco legal sólido de eIDAS

El Reglamento eIDAS establece un marco legal sólido para las transacciones electrónicas dentro del mercado único digital de la Unión Europea, abordando específicamente los servicios de identificación electrónica y de confianza como el sellado temporal electrónico. Este marco no solo promueve el uso de identidades electrónicas seguras y confiables para transacciones interfronterizas, sino que también asegura la interoperabilidad de los sellos de tiempo electrónicos en toda la UE.

Impacto y Beneficios de eIDAS

- **Interoperabilidad mejorada:** eIDAS garantiza que los sistemas de identificación electrónica de un país sean reconocidos por todos los demás

Estados miembros, promoviendo así la eficiencia y la seguridad en las transacciones transfronterizas.

- **Seguridad en las Transacciones:** Este reglamento eleva el nivel de seguridad para las transacciones empresariales, minimizando la carga administrativa y reduciendo los costos, lo que resulta en procesos empresariales más eficientes y un incremento en los beneficios.
- **Confianza y Aceptación Legal:** Los servicios de confianza que cumplen con eIDAS pueden ser utilizados como prueba en procedimientos judiciales, lo cual es crucial para la aceptación y validez legal de las transacciones y certificaciones digitales.

Relevancia de eIDAS para Certifydoc

- **Estándares de seguridad y autenticidad:** eIDAS define los estándares de seguridad que los servicios como el Blockchain Legalization Engine deben cumplir para garantizar la autenticidad e integridad de las certificaciones digitales. Esto es especialmente pertinente dado que nuestros análisis han confirmado la robustez y confiabilidad de la plataforma Certifydoc en la emisión de sellos de tiempo verificados.
- **Interoperabilidad en la UE:** La regulación facilita que los sellos de tiempo emitidos por Certifydoc sean reconocidos y aceptados en todos los Estados miembros de la UE, lo que es vital para operaciones transfronterizas y para empresas que operan a escala europea.
- **Marco legal para servicios de confianza:** Al establecer un marco legal para los servicios de sellado temporal, eIDAS ayuda a garantizar que estos servicios mantengan su validez y fiabilidad, fortaleciendo la confianza en las soluciones proporcionadas por Certifydoc a sus usuarios.

Impacto de eIDAS en la adopción de tecnología blockchain

La inclusión de requisitos para servicios de sellado temporal bajo eIDAS es un paso significativo hacia la integración de tecnologías de blockchain en el ecosistema digital europeo. Al garantizar que los documentos y transacciones sean seguros y estén legalmente validados, eIDAS no solo soporta la adopción tecnológica sino que también promueve la confianza y la seguridad en las plataformas digitales a lo largo de Europa.

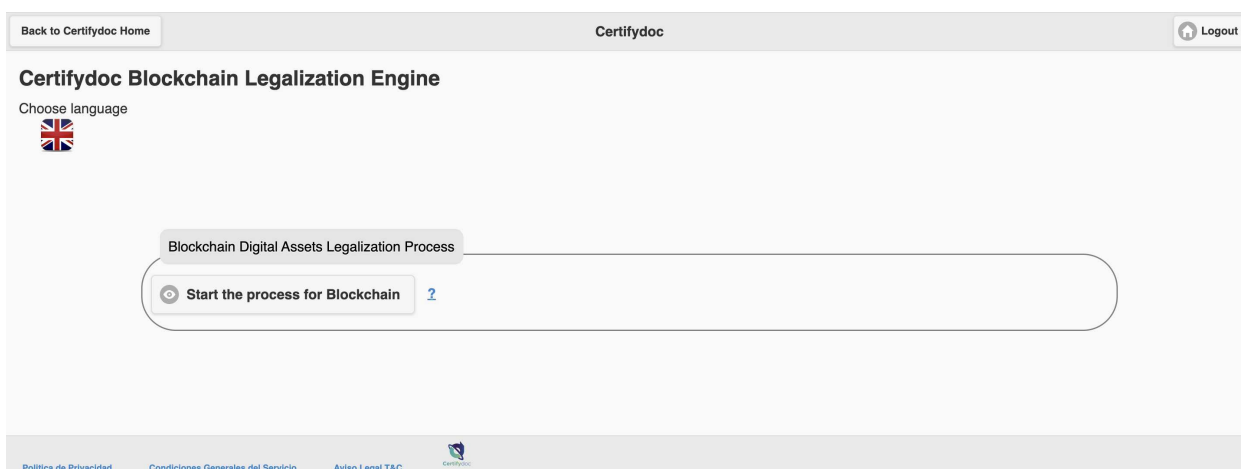
El marco proporcionado por eIDAS es indispensable para la operación y expansión de servicios como los ofrecidos por Certifydoc. Además, establece los cimientos legales y técnicos necesarios para una adopción más amplia de soluciones de certificación basadas en blockchain, asegurando que estas tecnologías se integren armoniosamente en el marco legal y de negocios de la Unión Europea.

5. Análisis Blockchain Legalization Engine

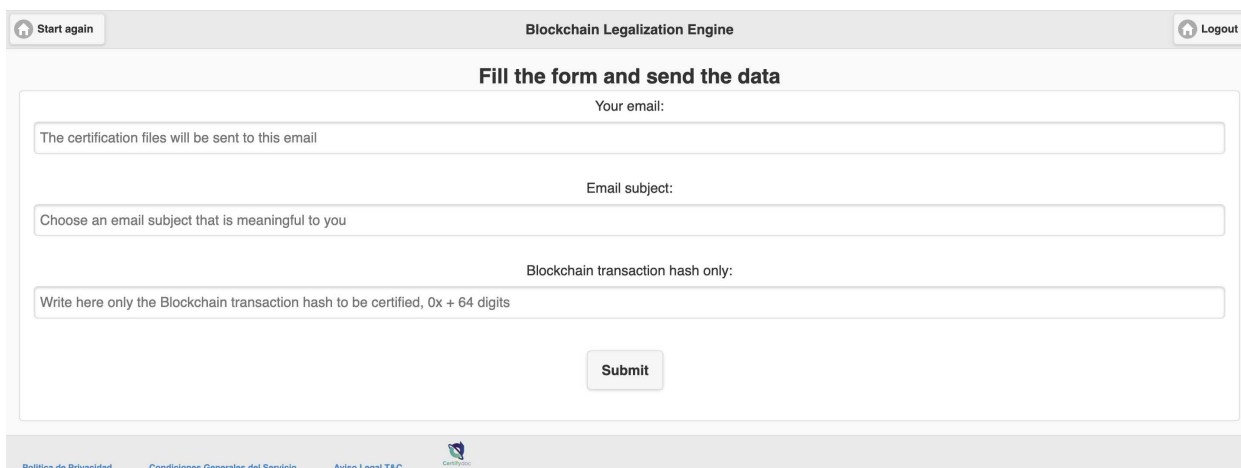
Este apartado detalla el funcionamiento del Blockchain Legalization Engine, describiendo los protocolos y procedimientos utilizados para la generación y certificación de timestamp, así como los métodos de interacción a través de la aplicación web y la API.

5.1. Certificación de transacciones Blockchain vía aplicación web

La Blockchain Certification Engine de Certifydoc dispone de una aplicación web (<https://www.certifydoc.eu/blockchain-legalization-engine/>) desde la que los clientes pueden generar certificados utilizando una interfaz gráfica.



Hay un único proceso para generar certificados de transacciones de la Blockchain:

The screenshot displays the "Blockchain Legalization Engine" form. The form is titled "Fill the form and send the data" and is enclosed in a light gray border. At the top of the form, there are two buttons: "Start again" on the left and "Logout" on the right. The form contains three input fields: 1. "Your email:" with a placeholder text "The certification files will be sent to this email". 2. "Email subject:" with a placeholder text "Choose an email subject that is meaningful to you". 3. "Blockchain transaction hash only:" with a placeholder text "Write here only the Blockchain transaction hash to be certified, 0x + 64 digits". Below the input fields is a "Submit" button. The footer of the form includes links for "Política de Privacidad", "Condiciones Generales del Servicio", "Aviso Legal T&C", and the Certifydoc logo.

En este menú el usuario debe completar la siguiente información:

1. **Email:** Correo al que llegara la certificación.
2. **Email subject:** Asunto del correo con la certificación.

3. Blockchain transaction hash: El hash en hexadecimal de la transacción de Blockchain a certificar.

Una vez se envía el formulario, el usuario consume una certificación.

Al usuario le llegará un correo electrónico con información y una serie de documentos relacionados con la certificación:

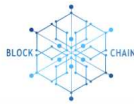
Legal certification for the Blockchain digital assets

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.

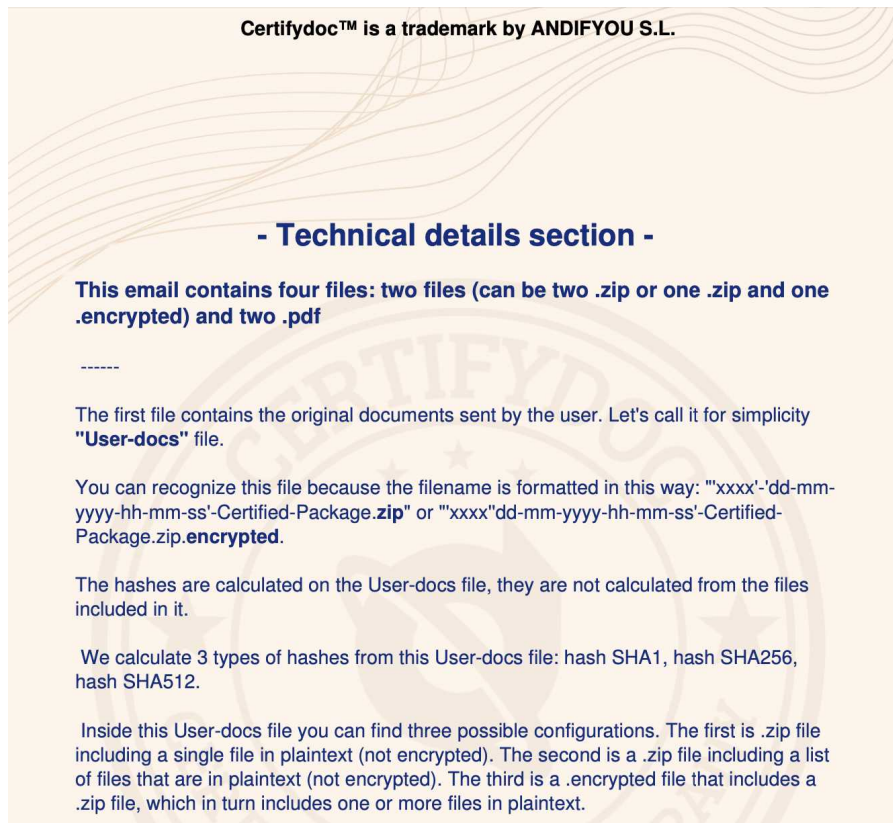
According to EU eIDAS regulation No 910/2014, **the verification of the certification is executed checking that the hashes (fingerprints) of the certified evidence match the correctly signed hashes by the certifying authority** at the time of certification. For this purpose Certifydoc attaches the file 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. Detalles técnicos: Archivo PDF que explica los detalles técnicos de los demás archivos del correo.



2. **Reporte de la certificación:** Archivo PDF es una explicación de la certificación. Es importante tener en cuenta que este archivo solo representa un informe explicativo de la certificación. En caso de pericial forense el valor legal certificado consiste en los ficheros respuesta .tsr y el certificado publico .pem de la autoridad certificadora.



3. **Datos de usuario:** Archivo ZIP que contiene un .txt con el hash de la transacción de Blockchain certificada.

```
→ 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. **Certificación:** Archivo ZIP que contiene la certificación y los archivos necesarios para verificarla.

```
1519807286XJTlEf-Namirial.tsr 2078436848b5f0wW-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. Certificación de transacciones Blockchain vía API

La Blockchain Certification Engine de Certifydoc dispone de una API que nos permite generar certificaciones de forma programática. La API dispone de 4 posibles procesos distintos:

1. **Email response:** La API nos enviará un correo con los archivos. Este proceso tiene el mismo resultado que hacer la certificación vía web.

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

?submitthereum=submitthereum

&hashethereum=0x9c820dc62b09fcb517ff22d4888d06c8cc858d59cbeff8830865814a852e1a3

&response_type=email_response

&emailsubjectthereum=Test API sandbox Blockchain to email En 230508

&emailethereum=email@dominio.es

&language=en

2. **API response complete:** Recibimos los mismos archivos que en el correo pero como respuesta de la API. Los archivos están codificados en base64.

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

?submitthereum=submitthereum

&hashethereum=0x9c820dc62b09fcb517ff22d4888d06c8cc858d59cbeff8830865814a852e1a3

&response_type=api_response

&api_response_options=complete

&language=en

3. **API response reduced:** Recibimos la respuesta por la API. Nos envía el Timestamp Response (.tsr), la CA certificate (.pem) y el reporte de la certificación (.pdf). Los archivos están codificados en base64.

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

?submitthereum=submitthereum

&hashethereum=0xa85c41d8ffd5212a7537b4556eb8c748b723fbb51a56f67b7961e830087adb6b

&response_type=api_response

&api_response_options=reduced

&language=en

4. **API response minimized:** Recibimos la respuesta por la API. Nos envía el Timestamp Response (.tsr) y la CA certificate (.pem). Los archivos están codificados en 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. Proceso de verificación

Podemos verificar la información que contienen los diferentes archivos:

1. El **Timestamp Query** (.tsq) contiene información útil como el hash que se va a certificar. Puedes verificar sus datos ejecutando el 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 información útil como el hash certificado y el sello de tiempo del certificado. Puedes verificar sus datos ejecutando el 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 información útil como el CN del certificador. Se pueden verificar sus datos ejecutando el 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 vez hemos verificado que los archivos tienen el contenido esperado, podemos verificar el certificado ejecutando el siguiente comando:

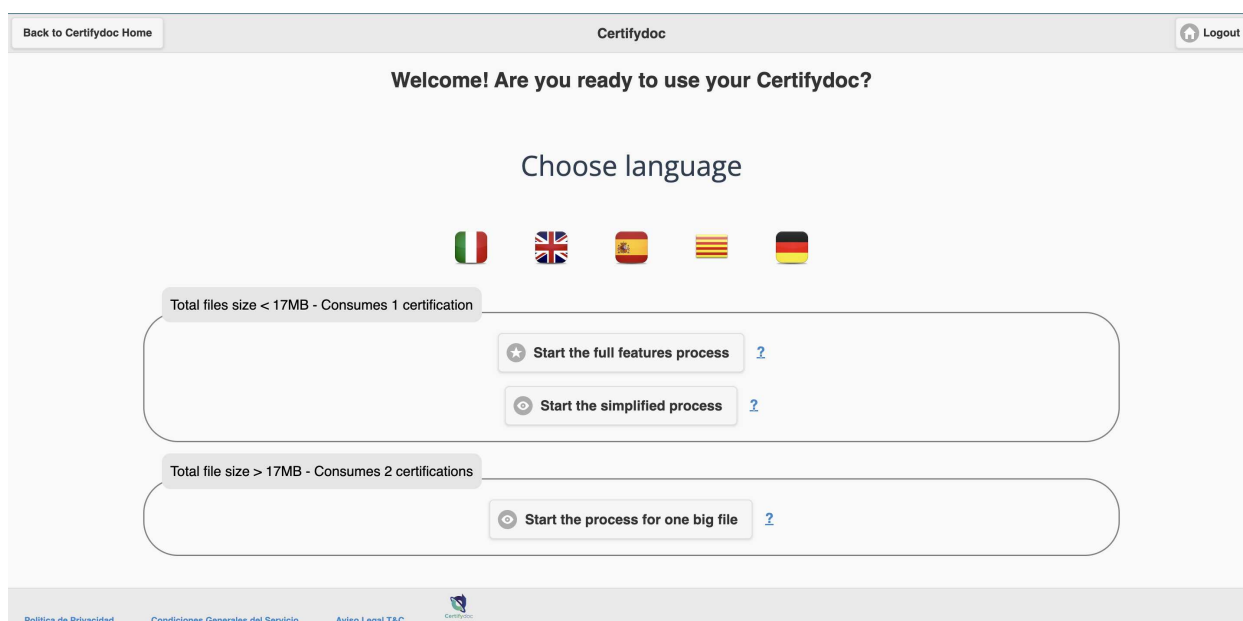
```
openssl ts -verify -in <tsr_filename>.tsr -CAfile <pem_filename>.pem -digest $(cat <transaction_to_verify>.txt)
```


6. Certificación de archivos

Este apartado detalla el funcionamiento para la certificación de archivos, describiendo los protocolos y procedimientos utilizados para la generación y certificación de timestamp, así como los métodos de interacción a través de la aplicación web y la API.

6.1. Certificación archivos vía aplicación web

La certificación de archivos de Certifydoc dispone de una aplicación web (<https://www.certifydoc.eu/certification/>) desde la que los clientes pueden generar certificados utilizando una interfaz gráfica.



La aplicación web tiene 3 procesos distintos:

- 1. Proceso completo:** Puedes subir múltiples archivos, que se guardaran dentro de un ZIP. También puedes cifrar el contenido. Tiene una limitación de 17MB.

Start again Certifydoc Logout

Please select one or more files to generate the Zip package

Note : your browser will process the zip file, don't choose a file larger than 17MB

Elegir archivos images.png

Please check the files list before generating the package

illustration-gallery-icon_53876-27002.jpg.avif
images.png

Reset

Save the Package File

Política de Privacidad Condiciones Generales del Servicio Aviso Legal T&C

Start again Certifydoc Logout

Please choose if your documents have to be treated as:

Normal Documents Confidential Documents

Política de Privacidad Condiciones Generales del Servicio Aviso Legal T&C

Start again Certifydoc Logout

Encrypt your package file

Please input a password to encrypt using AES 256

Password

Please select the zip package to get the AES 256 file encryption. **** Warning **** The resulting file size will be almost 80% bigger.

Seleccionar archivo Ninguno archivo selec.

Política de Privacidad Condiciones Generales del Servicio Aviso Legal T&C

Start again Certifydoc Logout

Please fill in the data and submit to the legal certifier Time Stamping Authority (TSA)

Your Name: Type your name without spaces

Your email: Your email..

Email subject: Choose an email subject to be sent to yourself

Package to select: (< 17MB) Seleccionar archivo illustration-gallery-icon_53876-27002.jpg.avif

Política de Privacidad Condiciones Generales del Servicio Aviso Legal T&C

2. Proceso simplificado: Solo puedes subir un único archivo. Tiene una limitación de 17MB.

Start again Certifydoc Logout

Please fill in the data and submit to the legal certifier Time Stamping Authority (TSA)

Your Name:

Your email:

Email subject:

Package to select: (< 17MB) Ninguno archivo selec.

[Política de Privacidad](#) [Condiciones Generales del Servicio](#) [Aviso Legal T&C](#)

- 3. Proceso para un solo archivo de gran tamaño:** Puede subir el hash sha256 de un único archivo o porción de file system sin limitación de tamaño. Este archivo puede ser un ZIP o un disco duro entero, así que a efectos prácticos puedes certificar múltiples archivos.

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 Logout

One big file Certifier

- + 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](#)

Start again Logout

One big file Certifier

- + Step 1. Folder creation
- + Step 2. Move the file into the folder
- + Step 3. Calculate the Hash SHA 256
- Step 4. Obtain the certification

Your email:

The certification files will be sent to this email

Email subject:

Choose an email subject that is meaningful to you

Hash SHA256 Hexadecimal only:

Write here only the HEX SHA256 Hash of the file to be certified, 64 digits

- + Step 5. Receive and archive the email

[Política de Privacidad](#) |
 [Condiciones Generales del Servicio](#) |
 [Aviso Legal T&C](#)

Start again Logout

One big file Certifier

- + Step 1. Folder creation
- + 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

Sub-steps

After few seconds you'll receive Certifydoc email

Save the whole email (file .eml) in the 2018-06-16-ConstructionFinalInspection-Certifydoc created folder

As an alternative, save the four attachments in the created folder

Done! The digital evidence has been archived and is ready to be retrieved and used according to the law

[Política de Privacidad](#) |
 [Condiciones Generales del Servicio](#) |
 [Aviso Legal T&C](#)

6.2. Certificación archivos vía API

También podemos certificar archivos utilizando la API. Existen 4 posibles procesos (son los mismos que en Blockchain Legalization Engine):

1. **Email response:** La API nos enviará un correo con los archivos. Este proceso tiene el mismo resultado que hacer la certificación vía web.
2. **API response complete:** Recibimos los mismos archivos que en el correo pero como respuesta de la API. Los archivos están codificados en base64.
3. **API response reduced:** Recibimos la respuesta por la API. Nos envía el Timestamp Response (.tsr), la CA certificate (.pem) y el reporte de la certificación (.pdf). Los archivos están codificados en base64.
4. **API response minimized:** Recibimos la respuesta por la API. Nos envía el Timestamp Response (.tsr) y la CA certificate (.pem). Los archivos están codificados en base64.

6.3. Verificar la certificación de archivos

A la hora de verificar el certificado de archivos, lo que estamos verificando es si la Timestamp Response (.tsr) contiene el hash SHA256 del archivo a verificar y si ha sido firmado por alguna autoridad certificadora. Tenemos dos posibilidades:

1. Si solo hemos certificado un archivo, el Timestamp Response contiene hash SHA256 del archivo.

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

2. Si hemos certificado varios archivos, el Timestamp Response contiene el hash SHA256 del ZIP de los archivos.

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

7. Conclusiones

Después de un exhaustivo análisis que implicó el uso repetido tanto de la Aplicación Web como de la API de Certifydoc Blockchain Certification Engine y certificación de archivos mediante un enfoque de prueba Black Box, se han obtenido resultados consistentes y satisfactorios en todas las certificaciones realizadas.

A través de múltiples interacciones con la plataforma, se han verificado todas las certificaciones emitidas sin encontrar ningún inconveniente significativo. Este proceso de verificación involucró la creación de timestamps con el hash de transacciones de Ethereum y de todas las transacciones de otras blockchain con el mismo formato hexadecimal, además de su posterior certificación utilizando la herramienta proporcionada por Certifydoc. Así como el proceso de certificación de archivos.

Se ha observado que tanto la Aplicación Web como la API de Certifydoc ofrecen una experiencia de usuario fluida y eficiente. La interfaz de usuario de la Aplicación Web es intuitiva y fácil de navegar, lo que facilita el proceso de certificación de transacciones. Asimismo, la API ha demostrado ser robusta y confiable, permitiendo la interacción programática con la plataforma de manera efectiva.

Durante el proceso de verificación de certificaciones utilizando OpenSSL, se ha confirmado la autenticidad y validez de todas las certificaciones emitidas por Certifydoc. La herramienta OpenSSL ha validado correctamente los timestamps generados, lo que respalda la integridad del proceso de certificación de tiempo implementado por la plataforma.

En resumen, los resultados obtenidos indican que la herramienta de Certifydoc Blockchain Certification Engine (BLM) así como el proceso de certificación de archivos funciona correctamente y cumple con su propósito de certificar transacciones de Blockchain y ficheros de manera confiable y precisa.

Estos hallazgos son alentadores y respaldan la eficacia de la plataforma como una solución viable para la certificación de tiempo e integridad en el contexto de transacciones de Ethereum y de transacciones de otras blockchain que presentan el mismo formato hexadecimal. Además se ha comprobado el correcto funcionamiento de la certificación de archivos.