Este documento pretende permitir a cualquier usuario comprender el detalle del funcionamiento del servicio.

Procedimiento de Certificación de Mensajes para un usuario:

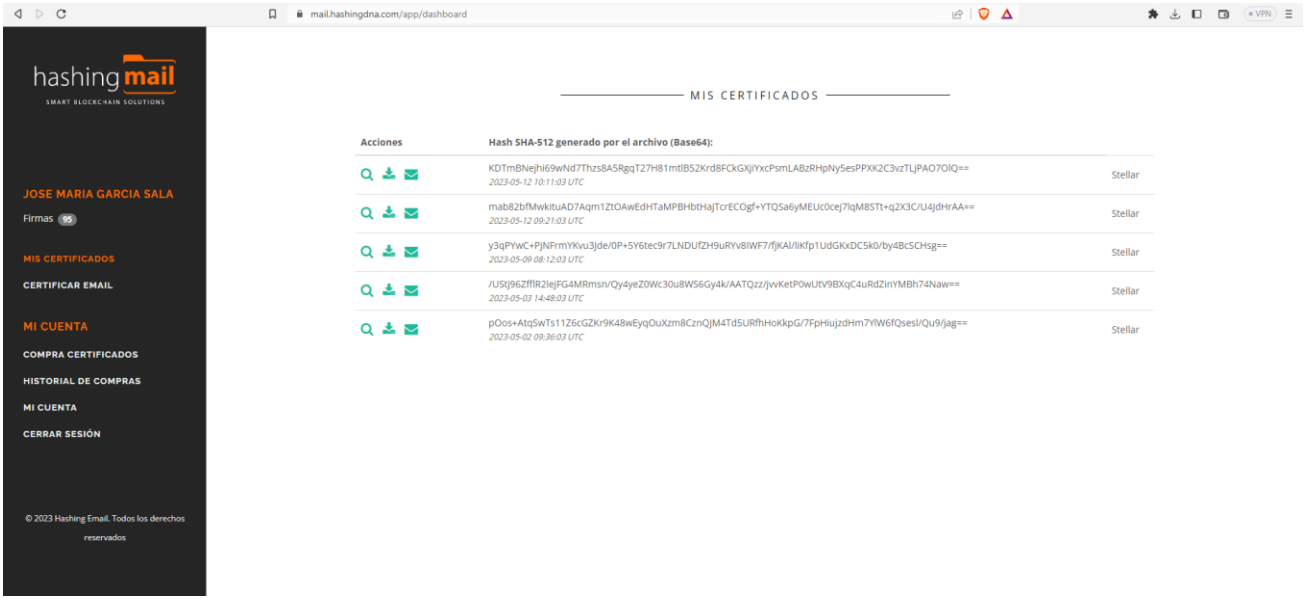
1) Enviar un mensaje de correo desde el cliente de correo del usuario.
2) Recepción del mensaje de certificación.
3) Comprobación de contenidos.
4) Comprobación de hashes
5) Comprobación de la operación en blockchain

Para activar el servicio es necesario darse de alta en la página: http://mail.hashingdna.com/

Y realizar un "Sign-Up" para registrarse en el sistema.

Finalizado el Sign-Up, pueden comprarse las firmas correspondientes y empezar a utilizar el servicio.

A partir de este momento se puede proceder a realizar el Login para acceder de forma habitual a la plataforma con el mismo dominio: http://mail.hashingdna.com/.



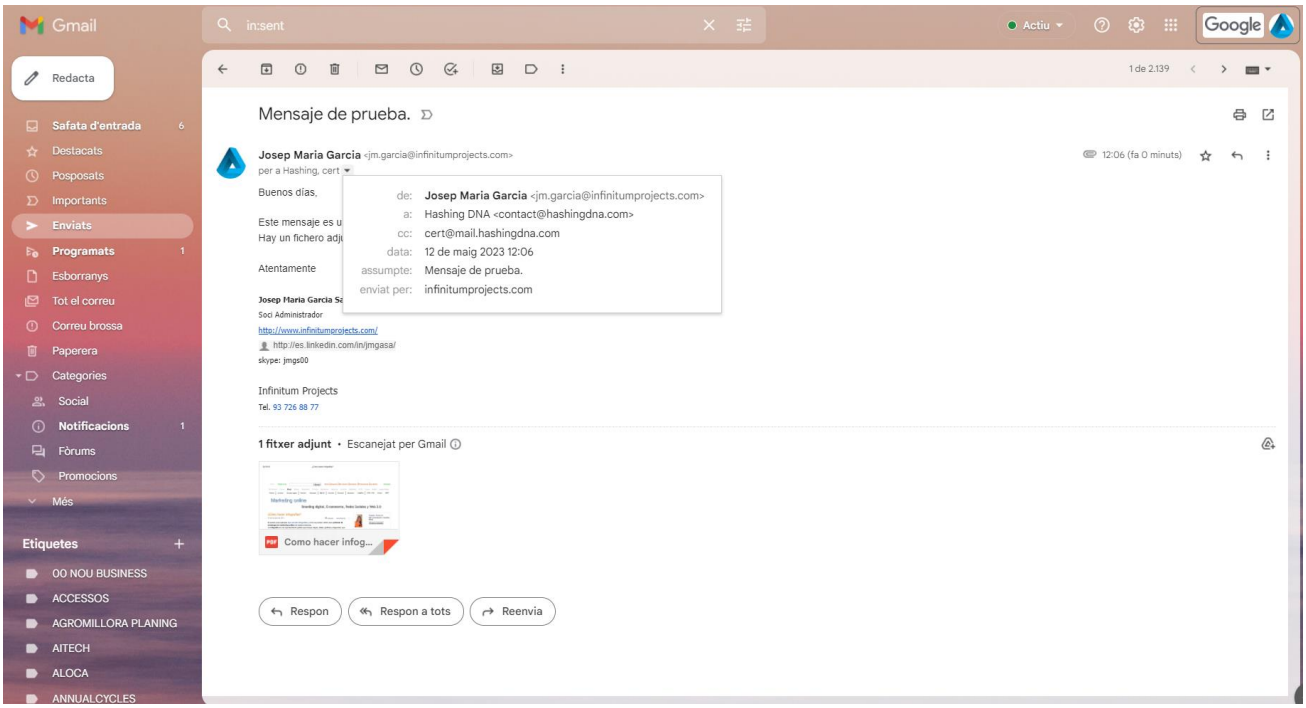
En la plataforma se pueden buscar los certificados y comprar más firmas, además de poder identificar las firmas que tengo disponibles.

También permite realizar algunos ajustes de la cuenta como el nombre y los datos de registro de la empresa (opcionales) en el selector “Mi cuenta”.

Enviar un mensaje de correo desde el cliente de correo del usuario.

Desde el cliente de correo habitual de cualquier usuario, podemos enviar un mensaje electrónico de forma corriente añadiendo el correo cert@mail.hashingdna.com en cualquiera de las casillas del destinatario, el destinatario en copia, o en copia oculta.

Eso implica que el correo llegará a los destinatarios previstos, pero también al sistema de certificación.

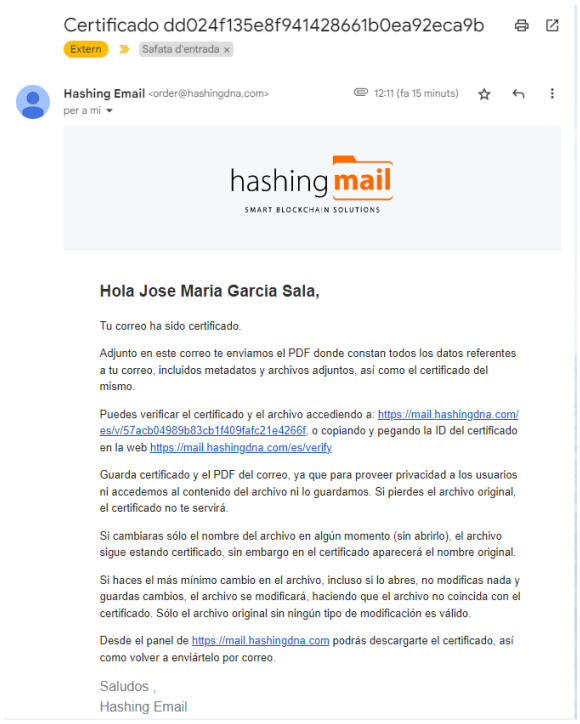


Recepción del mensaje de certificación.

Unos minutos después del envío del mensaje electrónico original, se recibe una respuesta con la certificación realizada en el mismo cliente del usuario.

Es importante recordar que la respuesta a la petición de certificación no es inmediata ya que la blockchain necesita de unos minutos, hasta 15, para cerrar el bloque de datos.

En este ejemplo, hemos recibido el siguiente correo.


Certificado dd024f135e8f941428661b0ea92eca9b

Extern · Safata d'entrada ×

Hashing Email <order@hashingdna.com> 12:11 (fa 15 minuts)
per a mi

hashing mail
SMART BLOCKCHAIN SOLUTIONS

Hola Jose Maria Garcia Sala,

Tu correo ha sido certificado.

Adjunto en este correo te enviamos el PDF donde constan todos los datos referentes a tu correo, incluidos metadatos y archivos adjuntos, así como el certificado del mismo.

Puedes verificar el certificado y el archivo accediendo a: https://mail.hashingdna.com/es/v/57acb04989b83cb1f409fafc21e4266f, o copiando y pegando la ID del certificado en la web https://mail.hashingdna.com/es/verify

Guarda certificado y el PDF del correo, ya que para proveer privacidad a los usuarios ni accedemos al contenido del archivo ni lo guardamos. Si pierdes el archivo original, el certificado no te servirá.

Si cambiaras sólo el nombre del archivo en algún momento (sin abrirlo), el archivo sigue estando certificado, sin embargo en el certificado aparecerá el nombre original.

Si haces el más mínimo cambio en el archivo, incluso si lo abres, no modificas nada y guardas cambios, el archivo se modificará, haciendo que el archivo no coincida con el certificado. Sólo el archivo original sin ningún tipo de modificación es válido.

Desde el panel de https://mail.hashingdna.com podrás descargarte el certificado, así como volver a enviártelo por correo.

Saludos ,
Hashing Email

Las instrucciones más relevantes son:

El enlace de verificación:

La necesidad de guardar el correo recibido de certificación y los archivos adjuntos.

También avisa de que las modificaciones realizadas en cualquier archivo o la pérdida de los mismos, invalida la certificación.

Este mensaje también adjunta 2 archivos:

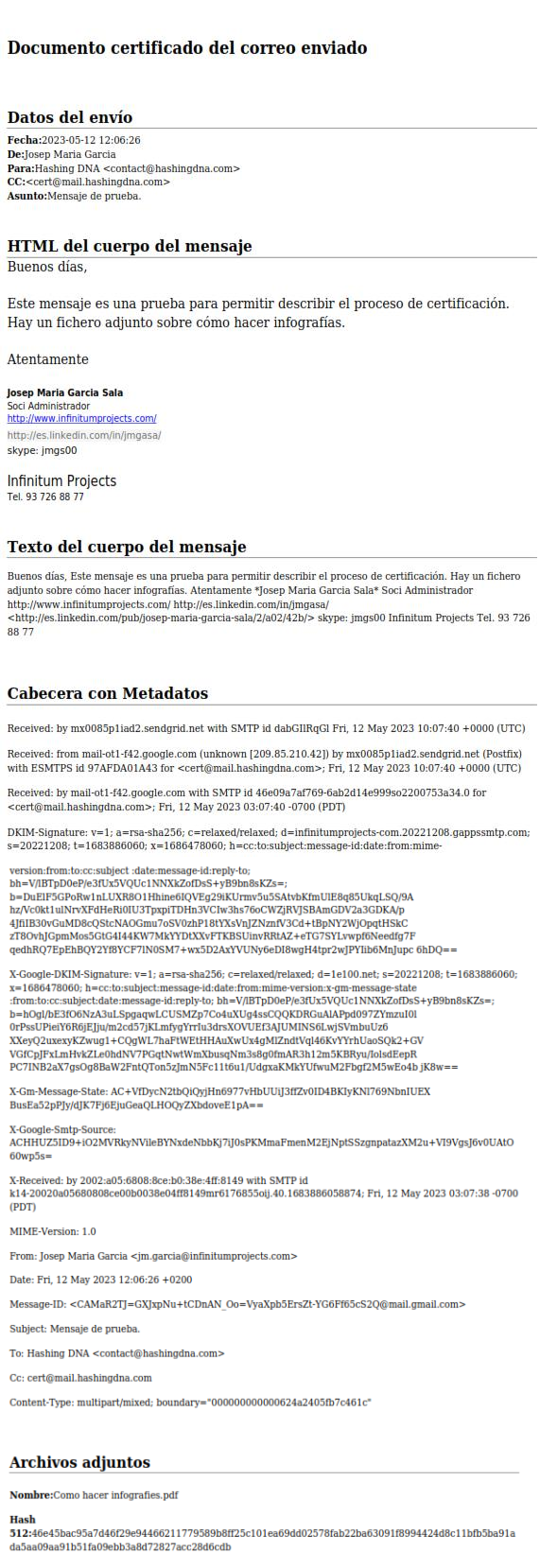
- El archivo certificado con los contenidos del mensaje, en formato pdf.
- El archivo de certificación con los datos de la misma.

Por esta razón se recomienda guardar en el cliente de correo el mensaje original y el de certificación.

Vamos a revisar el contenido de ambos archivos.

Comprobación de contenidos. Fichero de ejemplo

En el mensaje electrónico de respuesta, uno de los pdf incluye toda la información del mail original.



Documento certificado del correo enviado

Datos del envío

Fecha:2023-05-12 12:06:26
De: Josep Maria Garcia
Para: Hashing DNA <contact@hashingdna.com>
CC:<cert@mail.hashingdna.com>
Asunto: Mensaje de prueba.

HTML del cuerpo del mensaje

Buenos días,

Este mensaje es una prueba para permitir describir el proceso de certificación.
Hay un fichero adjunto sobre cómo hacer infografías.

Atentamente

Josep Maria Garcia Sala
Soci Administrador
http://www.infinitumprojects.com/
http://es.linkedin.com/in/jmgasa/
skype: jmgs00

Infinitum Projects
Tel. 93 726 88 77

Texto del cuerpo del mensaje

Buenos días, Este mensaje es una prueba para permitir describir el proceso de certificación. Hay un fichero adjunto sobre cómo hacer infografías. Atentamente *Josep Maria Garcia Sala* Soci Administrador http://www.infinitumprojects.com/ http://es.linkedin.com/in/jmgasa/ <http://es.linkedin.com/pub/josep-maria-garcia-sala/2/a02/42b/> skype: jmgs00 Infinitum Projects Tel. 93 726 88 77

Cabecera con Metadatos

Received: by mx0085p1iad2.sendgrid.net with SMTP id dabGIlRqGl Fri, 12 May 2023 10:07:40 +0000 (UTC)

Received: from mail-ot1-f42.google.com (unknown [209.85.210.42]) by mx0085p1iad2.sendgrid.net (Postfix) with ESMTPS id 97AFDA01A43 for <cert@mail.hashingdna.com>; Fri, 12 May 2023 10:07:40 +0000 (UTC)

Received: by mail-ot1-f42.google.com with SMTP id 46e09a7af769-6ab2d14e999so2200753a34.0 for <cert@mail.hashingdna.com>; Fri, 12 May 2023 03:07:40 -0700 (PDT)

DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=infinitumprojects-com.20221208.gappssmtp.com; s=20221208; t=1683886060; x=1686478060; h=cc:to:subject:message-id:date:from:mime-

version:from:to:cc:subject :date:message-id:reply-to;
bh=V/lBTpD0eP/e3fUx5VQUc1NNXkZofDsS+yB9bn8sKZs=;
b=DuElF5GPoRw1nLUXR8O1Hhine6lQVEg29iKUrmv5u5SAtvbKfmUlE8q85UkqLSQ/9A
hz/Vc0kt1uNrvXFdHeRi0IU3TpxpiTDHn3VClw3hs76oCWZjRVJSBAmGDV2a3GDKA/p
4JfIlB30vGuMD8cQStcNAOGmu7oSV0zhP18tYXsVnJZNznfV3Cd+tBpNY2WjOpqtHSkC
zT8OvhJGpmMos5GtG4I44KW7MkYYDtXXvFTKBSUinvRRtAZ+eTG7SYLvwpf6Needfg7F
qedhRQ7EpEhBQY2Yf8YCF7lN0SM7+wx5D2AxYVUNy6eDI8wgH4tpr2wJPYlb6MnJupc 6hDQ==

X-Google-DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=1e100.net; s=20221208; t=1683886060; x=1686478060; h=cc:to:subject:message-id:date:from:mime-version:x-gm-message-state
:from:to:cc:subject:date:message-id:reply-to; bh=V/lBTpD0eP/e3fUx5VQUc1NNXkZofDsS+yB9bn8sKZs=;
b=hOgl/bE3fO6NzA3uLSpgaqwLCUSMZp7Co4uXUg4ssCQQKDRGuAlAPpd097ZYmzuI0l
0rPssUPieiY6R6jEJju/m2cd57jKLmfygYrr1u3drsXOVUEf3AJUMINS6LwjSVmbuUz6
XXeyQ2uxexyKZwuq1+CQgWL7haFtWEtHHAuXwUx4gMlZndtVql46KvYYrhUaoSQk2+GV
VGfCpJFxLmHvkZLe0hdNV7PGqtNwtWmXbusqNm3s8g0fmAR3h12m5KBRyu/lolsdEepR
PC7lNB2aX7gsOg8BaW2FntQTon5zJmN5Fc11t6u1/UdgxaKMkYUfwuM2FbgfZM5wEo4b jK8w==

X-Gm-Message-State: AC+VfDycN2tbQiQyjHn6977vHbUUiJ3ffZv0ID4BKlyKNl769NbnIUEX
BusEa52pPJy/dJK7Fj6EjuGeaQLHOQyZXbdoveE1pA==

X-Google-Smtp-Source:
ACHHUZ5ID9+iO2MVRkyNVileBYNxdeNbbKj7iJ0sPKMmaFmenM2EjNptSSzgnpatazXM2u+Vl9VgsJ6v0UAtO
60wp5s=

X-Received: by 2002:a05:6808:8ce:b0:38e:4ff:8149 with SMTP id
k14-20020a05680808ce00b0038e04ff8149mr6176855oij.40.1683886058874; Fri, 12 May 2023 03:07:38 -0700 (PDT)

MIME-Version: 1.0

From: Josep Maria Garcia <jm.garcia@infinitumprojects.com>

Date: Fri, 12 May 2023 12:06:26 +0200

Message-ID: <CAMaR2TJ=GXJxpNu+tCDnAN_Oo=VyaXpb5ErsZt-YG6Ff65cS2Q@mail.gmail.com>

Subject: Mensaje de prueba.

To: Hashing DNA <contact@hashingdna.com>

Cc: cert@mail.hashingdna.com

Content-Type: multipart/mixed; boundary="000000000000624a2405fb7c461c"

Archivos adjuntos

Nombre: Como hacer infografies.pdf

Hash
512:46e45bac95a7d46f29e944662117795 89b8ff25c101ea69dd02578fab22ba63091f8994424d8c11bfb5ba91a da5aa09aa91b51fa09ebb3a8d72827acc28d6cdb

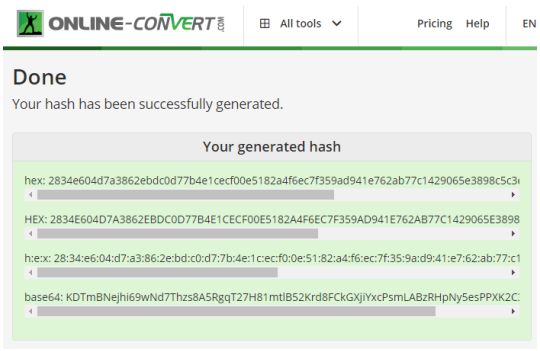
En los datos de envío podemos encontrar la cabecera del mensaje electrónico.

Posteriormente podemos leer el contenido del mail en html y texto.

En html que es el formato en que se presenta la información en el cliente de correo, pero también en texto para leer la totalidad del mensaje e identificar las instrucciones html del mismo.

Los metadatos del mensaje electrónico donde se encuentra toda la información que describe los servidores por los cuales se ha realizado el envío

Finalmente, si hay archivos adjuntos, podemos leer sus hashes. En este caso solo encontramos un archivo adjunto llamado “Como hacer infografías.pdf”



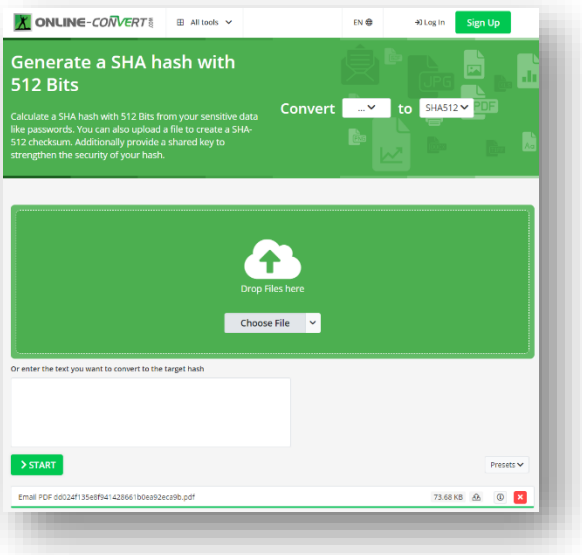
Comprobación de hashes

Para poder determinar que el mensaje es el original y no ha sido modificado, debemos comparar el hash del certificado (en el recuadro azul) con el obtenido a través de un lector de hashes después de hacerle leer el archivo "Email pdf XXXXXX" .

Se puede utilizar cualquier lector de hashes de archivos a disposición de los usuarios en internet. A modo de ejemplo proponemos el uso de la web "Online Convert"

Esta página web no tiene ningún coste y permite realizar tantas pruebas como queramos.

https://hash.online-convert.com/sha512-generator



Cargamos el fichero de contenidos, lo cargará y pulsamos "start". Después de unos segundos, nos entrega el hash de resultado:

base64:KDTmBNejhi69wNd7Thzs8A5RgqT27H81mtlB52Krd8FCkGXjiYxcPsmLABzRHpNy5esPPXK2C3vzTLjPAO7OlQ==

hex:2834e604d7a3862ebdc0d77b4e1cecf00e5182a4f6ec7f359ad941e762ab77c1429065e3898c5c3ec98b001cd11e9372e5eb0f3d72b60b7bf34cb8cf00eece95

Ambos hashes se corresponden al certificado, por lo que podemos concluir que el pdf de conenido es el original fechado y certificado en el timestamp que este indica. No se ha modificado ningún dato del mensaje original.

Archivos adjuntos

Nombre: Como hacer infografies.pdf

Hash
512:46e45bac95a7d46f29e94466211779589b8ff25c101ea69dd02578fab22ba63091f8994424d8c11bfb5ba91ada5aa09aa91b51fa09ebb3a8d72827acc28d6cdb

Si existen archivos adjuntos, como es este caso, el hash está en el pdf de contenidos.

Tendremos que realizar la misma operación con https://hash.online-convert.com/sha512-generator

Cargamos el fichero de contenidos, lo cargará y pulsamos “start”. Después de unos segundos, nos entrega el hash de resultado:

base64: base64:
RuRbrJWn1G8p6URmIRd5WJuP8lwQHqad0CV4+rIrpjCR+JlEJNjBG/tbqRraWqCaqRtR+gnrs6jXKCeswo1s2w==

hex: Your generated hash
hex:
46e45bac95a7d46f29e94466211779589b8ff25c101ea69dd02578fab22ba63091f8994424d8c11bfb5ba91ada5aa09aa91b51fa09ebb3a8d72827acc28d6cdb

Ambos hashes se corresponden al certificado, por lo que podemos concluir que el pdf de conenido es el original fechado y certificado en el timestamp que este indica. No se ha modificado ningún dato del mensaje original.

Comprobación de la operación en blockchain

hashing mail
SMART BLOCKCHAIN SOLUTIONS

ID DEL CERTIFICADO: dd024f135e8f941428661b0ea92eca9b

Puedes verificar este certificado en
https://mail.hashingdna.com/es/v/dd024f135e8f941428661b0ea92eca9b

CERTIFICADO DE EXISTENCIA

Hashing Mail certifica que el PDF contiene fielmente los datos extraídos del correo y se certificó el 2023-05-12 10:07:48 UTC (Tiempo Universal Coordinado).

DATOS CRIPTOGRÁFICOS

Hash SHA-512 generado por el archivo (Base64):

KDTmBNejhi69wNd7Thzs8A5RgqT27H81mtlB52Krd8FCkGXjiYxcPsmLABzRHpNy5esPPXK2C3vzTLjPAO7OlQ==

Hash SHA-512 generado por el archivo (hexadecimal):

2834e604d7a3862ebdc0d77b4e1cecf00e5182a4f6ec7f359ad941e762ab77c1429065e3898c5c3ec98b001cd11e9372e5eb0f3d72b60b7bf34cb8cf00eece95

Transacción de Stellar donde se ha incluido el Hash:

Ver transacción b36566d20671b74d7ea28f0647038d1e07135cf450cb0f76e6df91c6d76adfb7 en un explorador externo

Hora de creación del bloque en la blockchain de Stellar:

2023-05-12 10:08:55 UTC

En el certificado encontramos un enlace que permite verificar que Hahsing DNA ha realizado la certificación, en este caso podemos pulsarlo y recibiremos como respuesta en el navegador:

Verificar certificado

El certificado dd024f135e8f941428661b0ea92eca9b existe

Hashing Mail certifica que el PDF contiene fielmente los datos extraídos del correo y se certificó el 2023-05-12 10:07:48 UTC (Tiempo Universal Coordinado).

DATOS CRIPTOGRÁFICOS

Hash SHA-512 generado por el archivo (hexadecimal):

2834e604d7a3862ebdc0d77b4e1cecf00e5182a4f6ec7f359ad941e762ab77c1429065e3898c5c3ec98b001cd11e9372e5eb0f3d72b60b7bf34cb8cf00eece95

Transacción de Stellar donde se ha incluido el Hash:

Ver transacción b36566d20671b74d7ea28f0647038d1e07135cf450cb0f76e6df91c6d76adfb7 en un explorador externo

Hora de creación del bloque en la blockchain de Stellar:

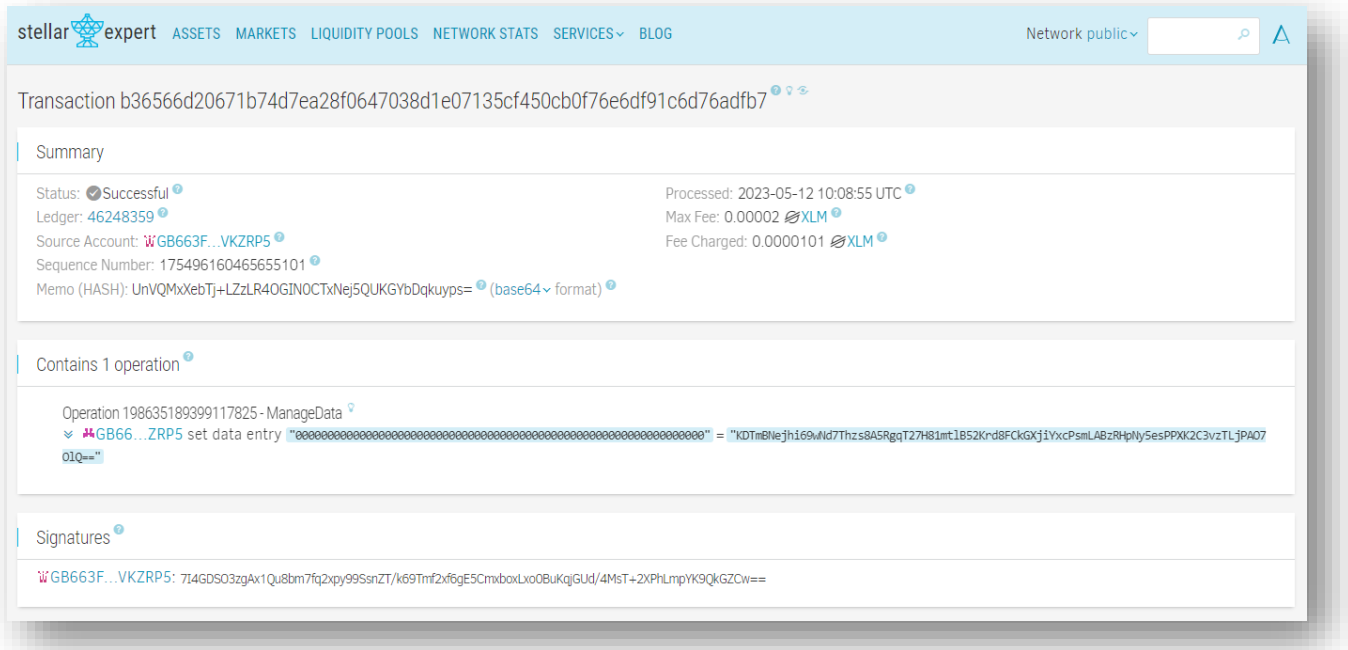
2023-05-12 10:08:55 UTC

Hash SHA-512 generado por el archivo (Base64):

KDTmBNejhi69wNd7Thzs8A5RgqT27H81mtlB52Krd8FCkGXjiYxcPsmLABzRHpNy5esPPXK2C3vzTLjPAO7OlQ==

En ambos casos, los datos coinciden y aseguran al cliente que HashingDNA ha realizado la certificación.

Pero también puede verificar este punto pulsando sobre el enlace al buscador de la transacción de la blockchain. Este navegador está a disposición de los usuarios de la blockchain de Stellar y asegura que la transacción se ha registrado y se corresponde a los datos del certificado.



stellar expert ASSETS MARKETS LIQUIDITY POOLS NETWORK STATS SERVICES BLOG Network public

Transaction b36566d20671b74d7ea28f0647038d1e07135cf450cb0f76e6df91c6d76adfb7

Summary

Status: Successful
Ledger: 46248359
Source Account: GB663F...VKZRP5
Sequence Number: 175496160465655101
Memo (HASH): UnVQMxXebTj+LZzLR4OGINOCTxNej5QUKGYbDqkuyps= (base64 format)

Processed: 2023-05-12 10:08:55 UTC
Max Fee: 0.00002 XLM
Fee Charged: 0.0000101 XLM

Contains 1 operation

Operation 198635189399117825 - ManageData
GB66...ZRP5 set data entry "0000000000000000000000000000000000000000000000000000000000000000" = "KDTmBNejhi69wNd7Thzs8A5RgqT27H81mtlB52Krd8FCkGXjiYxcPsmLABzRHpNy5esPPXK2C3vzTLjPAO7OlQ=="

Signatures

GB663F...VKZRP5: 7I4GDSO3zgAx1Qu8bm7fq2xpy99SsnZT/k69Tmf2xf6gE5CmxboxLxo0BuKqjGUd/4MsT+2XPhLmpYK9QkGZCw==

Este navegador no tiene ninguna relación con HashingDNA, es público y cualquiera puede utilizarlo para asegurar que las transacciones se han realizado.