Logroño

Dirección General de Tecnología e Innovación
Avenida de la Paz, 11
26071 – Logroño (La Rioja)

Guía generación y comprobación de huellas digitales.

Introducción

La huella digital de un archivo es un conjunto de datos asociados al archivo que permiten asegurar que el archivo no ha sido modificado.

La huella digital o resumen de un archivo se obtiene aplicando una función, denominada hash, a ese archivo. Esto da como resultado un conjunto de datos de longitud fija.

Una función hash tiene entre otras las siguientes propiedades:

- Dos archivos iguales producen huellas digitales iguales.
- Dos archivos parecidos producen huellas digitales diferentes.
- Dos huellas digitales idénticas pueden ser el resultado de dos archivos iguales o de dos archivos completamente diferentes. Existen múltiples funciones de hash cuyo comportamiento hacen que esta propiedad sea más o menos probable que ocurra, por lo que no todas las funciones de hash son aceptadas por el Esquema Nacional de Seguridad (ENS).
- Una función hash es irreversible, no se puede deshacer, por tanto, su comprobación se realizará aplicando de nuevo la misma función hash al archivo.

Teniendo en cuenta las propiedades anteriores se tiene la seguridad de que si se dispone de una huella digital de un archivo y posteriormente se genera una segunda huella digital a partir del archivo, si las huellas digitales son distintas, se puede afirmar que el archivo ha sufrido algún cambio entre el momento de la generación de ambas huellas.

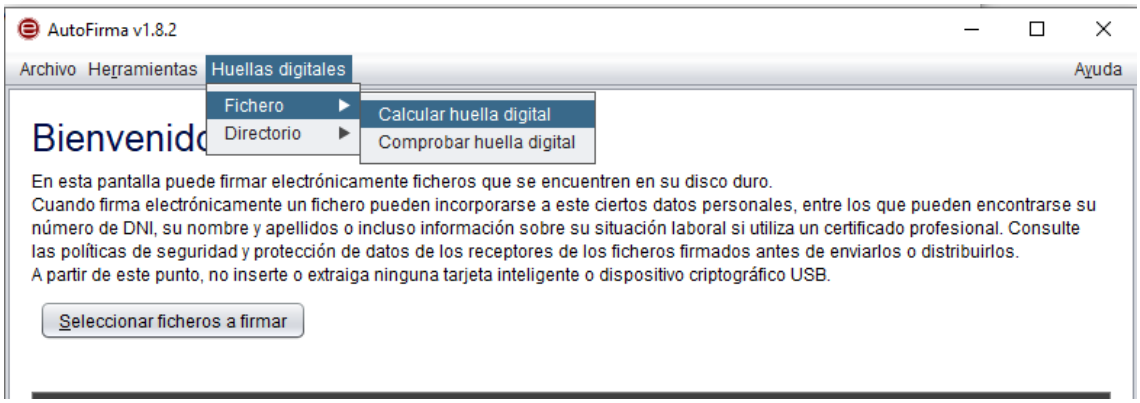
La aplicación Autofirma proporcionada por la Administración General del Estado permite la generación y comprobación de huellas digitales de archivos o directorios completos.

En la versión v 1.7.2 y anteriores de Autofirma, las opciones para generar y comprobar huellas digitales aparecían automáticamente con la instalación de la aplicación. A partir de la versión 1.8, es necesario descargar un plugin desde la url https://firmaelectronica.gob.es/Home/Descargas.html y agregarlo al producto a través de la opción de menú *Herramientas / Gestionar plugins* de Autofirma.

A continuación, se describen las operaciones a realizar para la generación y comprobación de huellas digitales utilizando Autofirma.

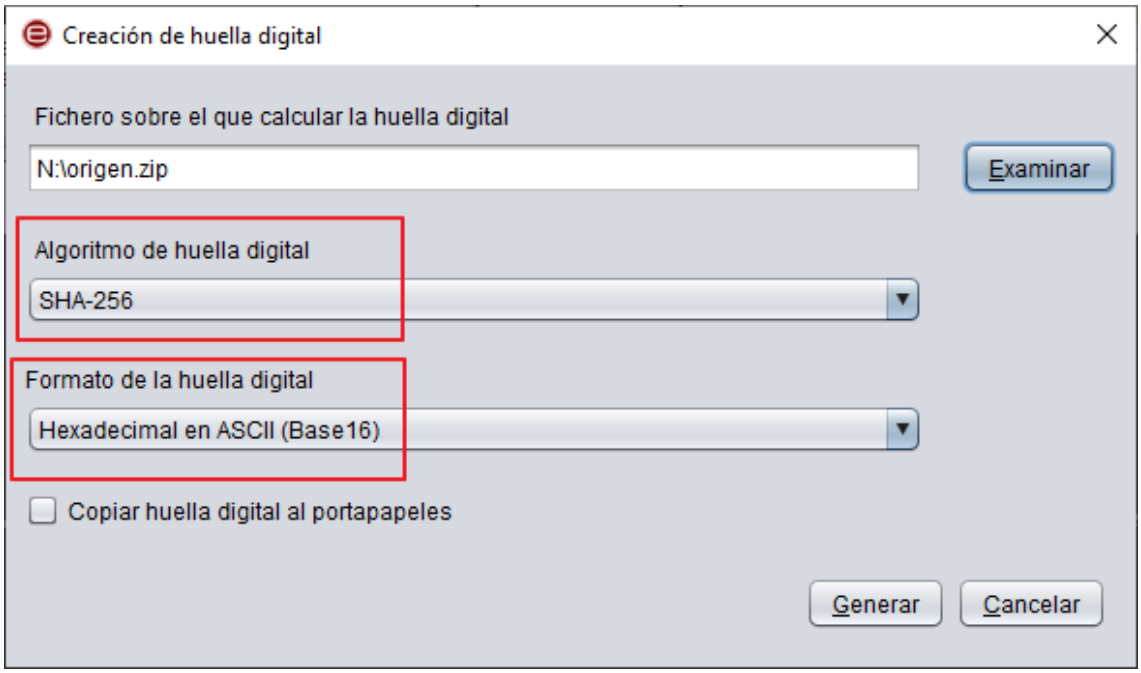
Generación huella digital con Autofirma

Para obtener la huella digital de un archivo utilizando Autofirma, se accederá al punto de menú *Huellas digitales / Fichero / Calcular huella digital*



Esta opción abre un formulario en el que se selecciona el fichero sobre el que se quiere generar la huella digital.

Además, se debe elegir el algoritmo a utilizar y el formato. Para la remisión de archivos al Ayuntamiento de Logroño se seleccionarán los valores indicados en la siguiente imagen. Cualquier variación en estos campos hará que la huella digital no se pueda comprobar posteriormente.



Una vez completados los datos del formulario anterior, se pulsará el botón Generar. Como resultado se generará un archivo cuyo nombre por defecto será el nombre

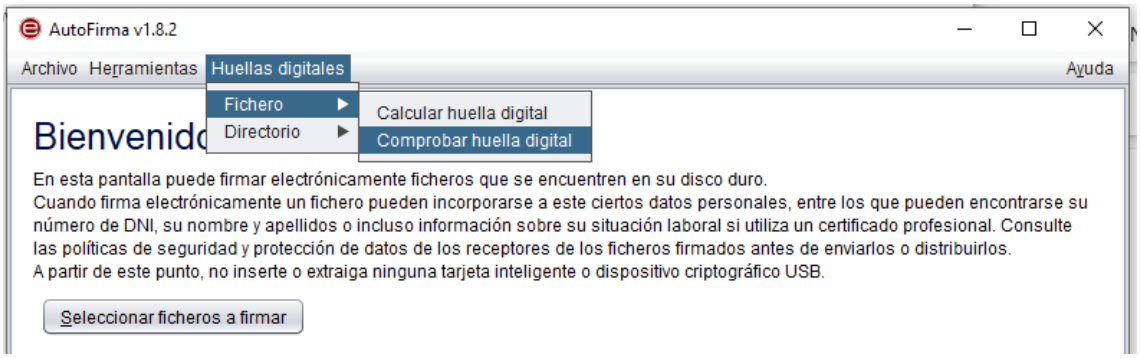
del archivo original y extensión hexhash. Este es el archivo que contine la huella digital y que deberá entregarse como prueba.

En el caso de las transmisiones de archivos de gran tamaño, si se requiere transmitir más de un archivo, se recomienda agrupar todos los archivos en un archivo comprimido de tipo zip. Así únicamente será necesario calcular y posteriormente validar una huella digital.

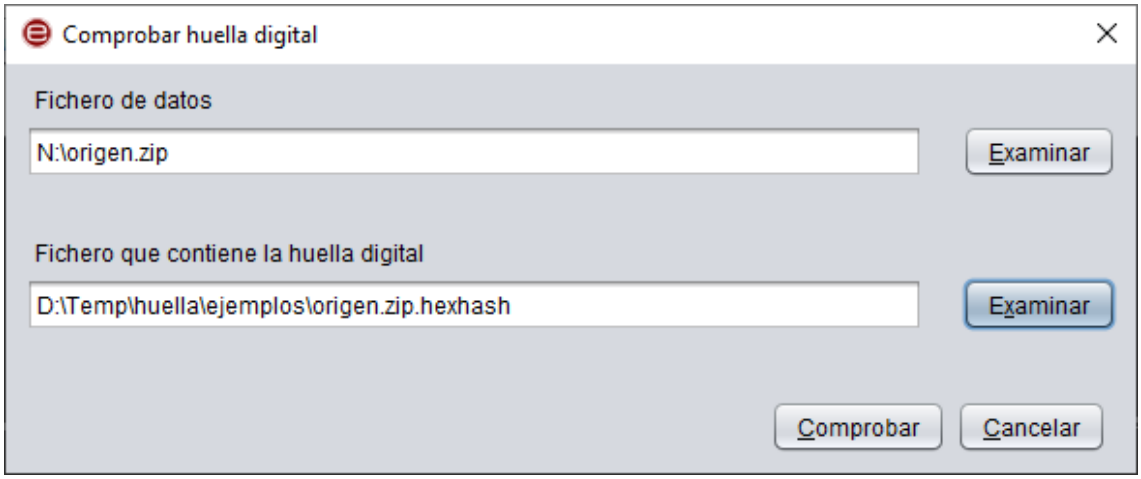
En los ficheros de tipo zip, cuando se sustituye uno de los archivos que contiene el zip, la huella digital será distinta si el contenido del archivo sustituido tiene el más mínimo cambio respecto al original.

Comprobación huella digital con Autofirma.

Para obtener la huella digital de un archivo utilizando Autofirma, se accederá al punto de menú *Huellas digitales / Fichero / Comprobar huella digital*



Esta opción abre un formulario en el que se selecciona el fichero sobre el que se quiere generar la huella digital y el fichero que contiene la huella.



Al pulsar el botón Comprobar, se realizará la verificación y se mostrará un mensaje indicando que las huellas digitales son coincidentes o no.