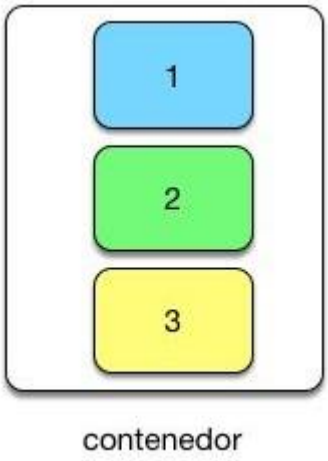
Definir la tecnología criptográfica para el token

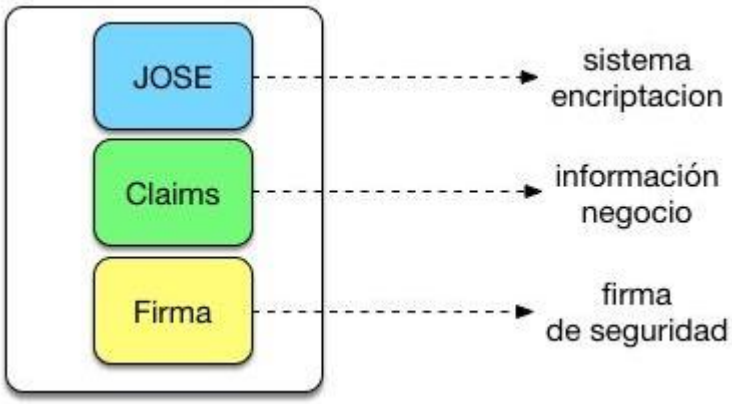
JSON TOKEN SEGURIDAD

El concepto de JSON Token es cada día más común en el desarrollo de aplicacione. Un JSON Token es un contenedor de información referente a la autenticación de un usuario.

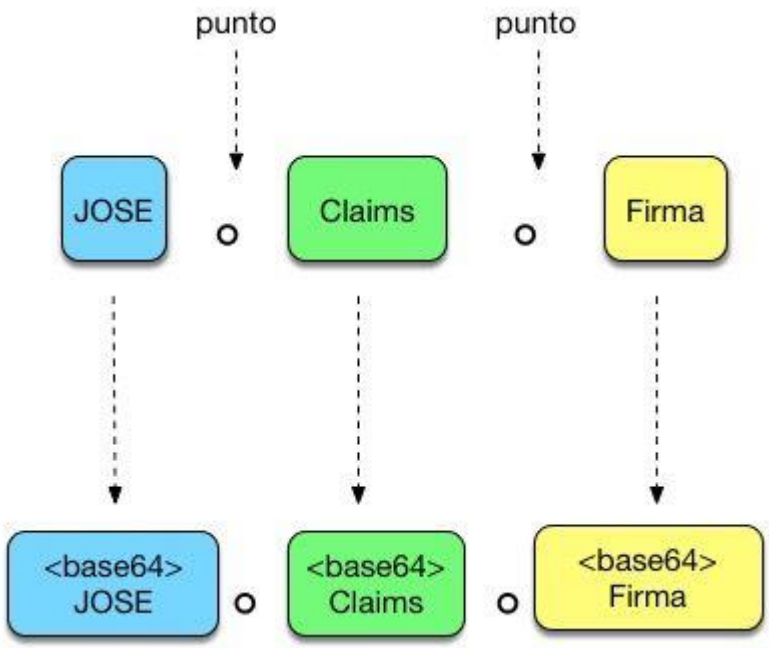


Un JSON Token está dividido en tres partes.

1. La primera es la que se denomina JOSE o JavaScript Object Signing and Encryption y define cual es la tecnología criptográfica que se va a aplicar al token para securizar la información.
2. La segunda parte es lo que se denomina JWT PayLoad o JWT Claims y almacena la información de negocio que necesitamos en el token. Esta parte se puede estructurar de muchas formas.
3. La tercera parte es la firma JWT que se encarga de dar validez al token.



Cada una de las partes esta codificada en Base64 y separadas por un punto.

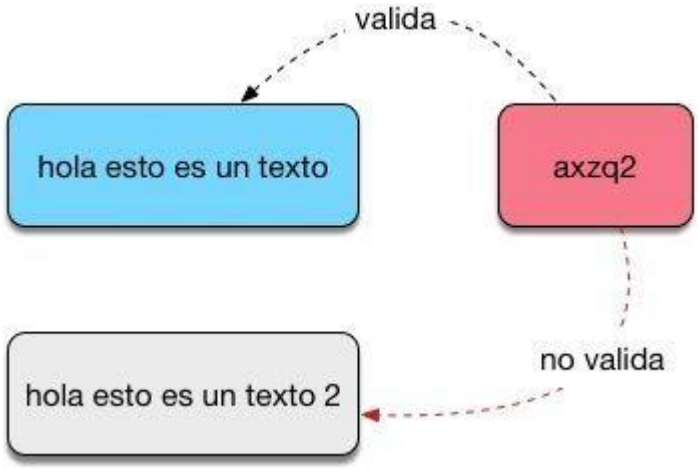


Esto está muy bien pero es difícil de entender cómo funciona.

Criptografia y JSON Token

Para entender JWT necesitamos repasar algunos de conceptos criptográficos. Lo primero que tenemos que entender es el concepto de algoritmo de HASH. Un algoritmo de HASH se encarga de generar un HASH (bloque de caracteres de longitud fila) a partir de una cadena arbitraria de texto.

Los algoritmos de hash sirven para comprobar que en ningún momento se ha modificado el texto original ya que se aseguran de que ante dos textos distintos siempre se genera un hash diferente. Por lo tanto si alguien nos cambia el texto original y lo intenta dar por valido podemos regenerar el hash y comprobar si cumple.


valida
hola esto es un texto
axzq2
no valida
hola esto es un texto 2