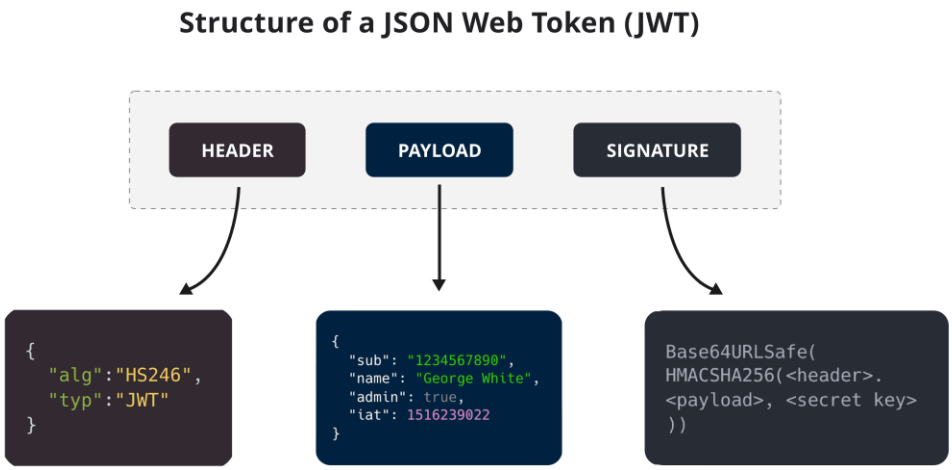
JSON Web Token

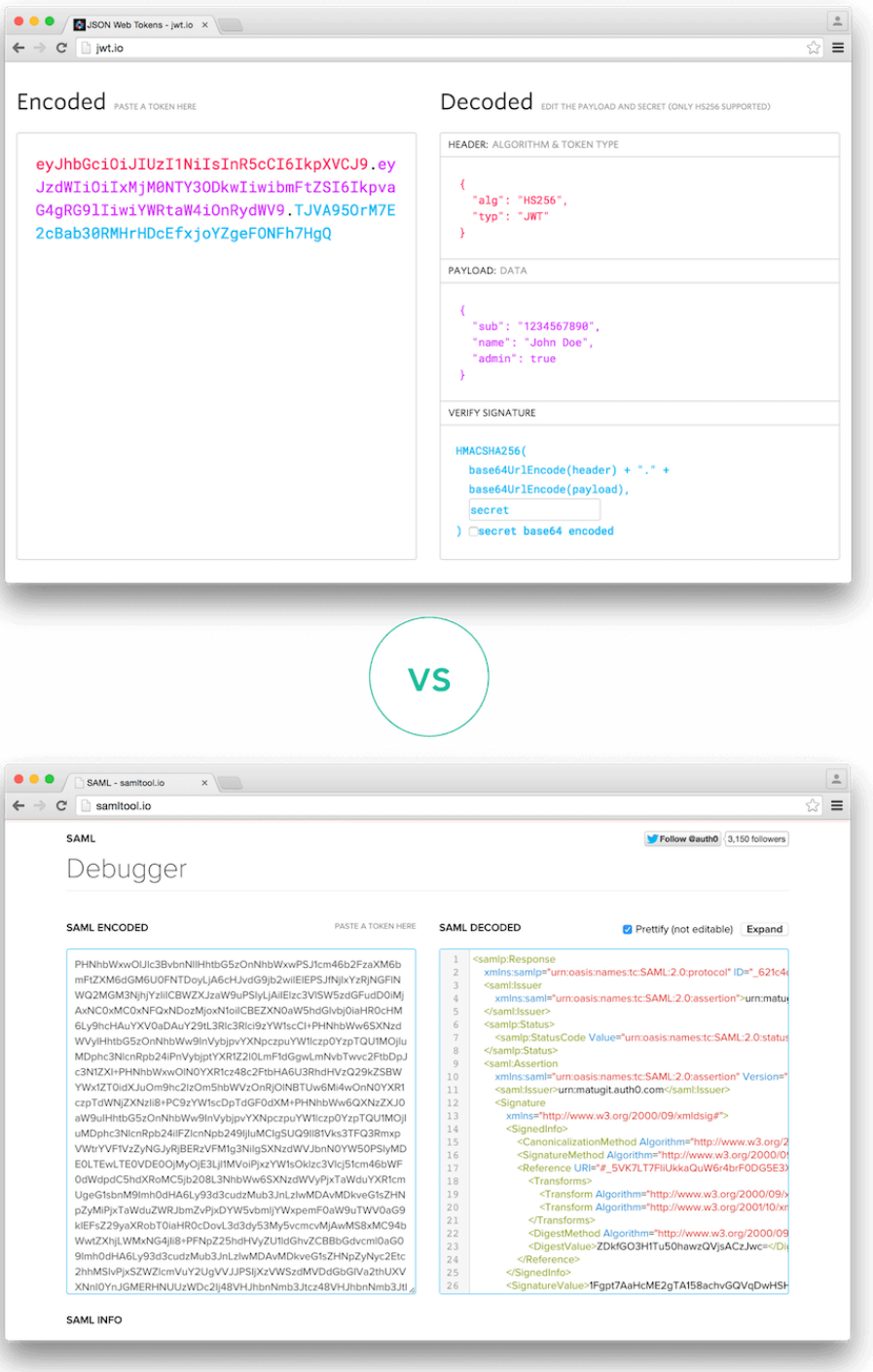
JSON Web Token is a proposed Internet standard for creating data with optional signature and/or optional encryption whose payload holds JSON that asserts some number of claims.



Benefits

There are benefits to using JWTs when compared to simple web tokens (SWTs) and Security Assertion Mark-up Language (SAML) tokens.

1. **More compact**: JSON is less verbose than XML, so when it is encoded, a JWT is smaller than a SAML token. This makes JWT a good choice to be passed in HTML and HTTP environments. **More secure, More common, Easier to process.**



2. Use

JWTs can be used in various ways:

- **Authentication**: When a user successfully logs in using their credentials, an ID token is returned, an ID token is always a JWT.

- **Authorization**: Once a user is successfully logged in, an application may request to access routes, services, or resources (e.g., APIs) on behalf of that user. To do so, in every request, it must pass an Access Token, which may be in the form of a JWT. Single Sign-on (SSO) widely uses JWT because of the small overhead of the format, and its ability to easily be used across different domains.
- **Information Exchange**: JWTs are a good way of securely transmitting information between parties because they can be signed, which means you can be sure that the senders are who they say they are. Additionally, the structure of a JWT allows you to verify that the content hasn't been tampered with.

3. Security

The information contained within the JSON object can be verified and trusted because it is digitally signed. Although JWTs can also be encrypted to provide secrecy between parties, Auth0-issued JWTs are JSON Web Signatures (JWS), meaning they are signed rather than encrypted.