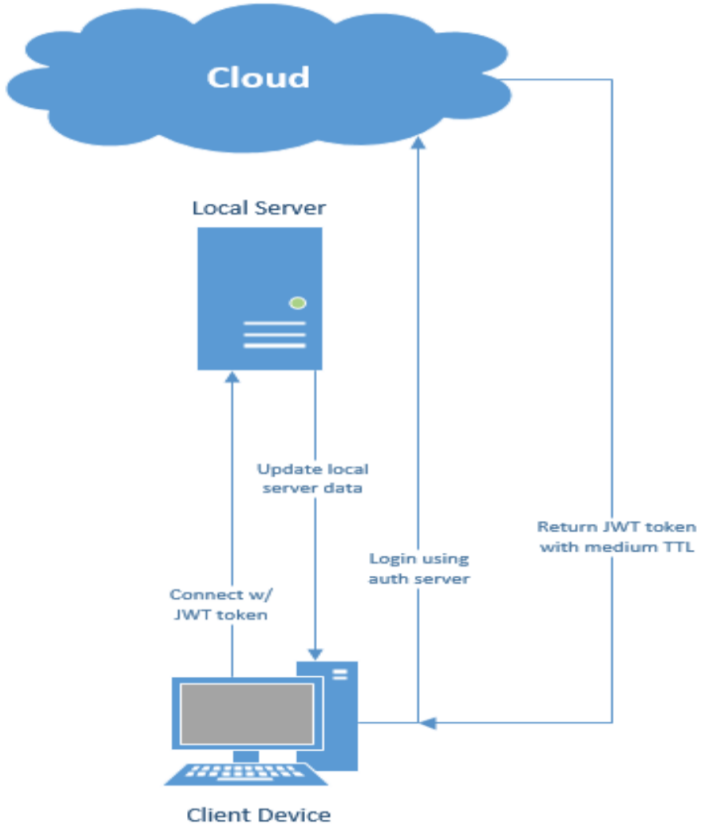
JWT Introduction
by
Michael Claudius

JWT Authentication



JWT Structure

Header	<pre>{
	"alg" : "HS256",
	"typ" : "JWT"
	}</pre>
		Identifies which algorithm is used to generate the signature
		`HS256` indicates that this token is signed using HMAC-SHA256.
		Typical cryptographic algorithms used are HMAC with SHA-256 (HS256) and RSA signature with SHA-256 (RS256). JWA (JSON Web Algorithms) RFC 7518 introduces many more for both authentication and encryption.[9]

Payload	<pre>{
	"loggedInAs" : "admin",
	"iat" : 1422779638
	}</pre>
		Contains a set of claims. The JWT specification defines seven Registered Claim Names which are the standard fields commonly included in tokens[1]. Custom claims are usually also included, depending on the purpose of the token.
		This example has the standard Issued At Claim (`iat`) and a custom claim (`loggedInAs`).

Signature	<pre>HMAC-SHA256(
	base64urlEncoding(header) + '.' +
	base64urlEncoding(payload),
	secret
	)</pre>
		Securely validates the token. The signature is calculated by encoding the header and payload using Base64url Encoding and concatenating the two together with a period separator. That string is then run through the cryptographic algorithm specified in the header, in this case HMAC-SHA256. The *Base64url Encoding* is similar to base64, but uses different non-alphanumeric characters and omits padding.