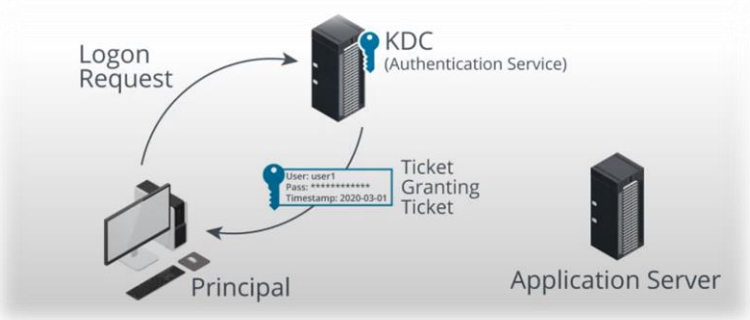
JSON Web Token(JWT)

الـJWT هو اختصار لـ " JSON Web Token" وهو عبارة عن بروتكول لتحقق من صحة المعلومات المدخلة للموقع او التطبيق تدخل معلومات ويتحقق من معلومات انها صحيحة ينشا لك قيم مشفرة تحتوي على بيانات المستخدم التي قام بإدخالها مثل (الاسم والايميل) ويرسلها لك كرد على Requestاللي ارسلته تبغا تسجل دخول وإذا تبغا تطلب أي صفحة او أي شيء داخل الموقع يضيع الـ Token معه بحيث يعلمها ان اللي طلبها هو صاحب هذا الحساب لكن بطريقة مشفرة

طبعاً الـ JWT يتكون من ثلاث أجزاء :

- Signature
- Payload
- Header

تم إنشاء الـToken عن طريق تشفير Header والـ Payload باستخدام خوارزمية التشفير التي قام بتوليدها، وبعدين يتم إضافة الـ Signature للتحقق من صحة لـToken إذا راح للسيرفر



بعض واهم الخصائص:

- Expiration : يتحكم بإعطاء صلاحيات مؤقتة للمستخدم بتحديد مدة صالحية الـtoken
- Refresh : تدعم التحديث من خلال عملية الـrefresh token، يمكن JWT من إدارة الصلاحيات المؤقتة بسهولة.
- Payload : يسمح لك بنقل بيانات مهمة بدون ما تحتاج تتصل بقاعدة البيانات مرة ثانية.
- Stateless : معناه إن JWT هو نظام للمصادقة stateless يعتمد على العميل بحفظ الحالة بدلاً من الـserver.

" باختصاره يمكن استخدام JWT لتمرير المعلومات بين السيرفرات والتطبيقات المختلفة بشكل آمن على سبيل المثال فكرة موقع النفاذ الوطني يحتوي على الـ SSO =>(Single Sign-On) يعني مجرد ما تدخل مره وحدة ويتحقق ان بياناتك صحيحة ينشا لك Tokenوتقدر تدخل على أي موقع تبغاه من خلال هذا الـ token يعني لو عندك موقع كبير تقدر تدخل أي URL تبغاه بدون ما يطلب منك كل شوي التحقق من بياناتك ومن صلاحياتك دون الحاجة إلى إعادة تسجيل الدخول.
لـ (Header) يحتوي على نوع الـ token والخوارزمية المستخدمة لتشفيره. الـ (Payload) يحتوي على البيانات المشفرة، كاسم المستخدم والصلاحيات وأي معلومات ثانية نحتاج نضيفها في الـ token. يتم عمل signatureلـ header and payload باستخدام مفتاح سري مشترك بين الموقع والسيرفر، ويتم إرسال الـ token إلى المستخدم ليتم استخدامه في الطلبات اللي سوف يتم ارسالها.

By Faisal Abdullah