องค์ประกอบของ JWT
header ส่วนนี้ประกอบด้วย ประเภทของโทเคน และ algorithm ที่ใช้เข้ารหัส
payload ส่วนนี้ประกอบด้วย ข้อมูลของuser ที่ต้องการส่งมาให้ใช้ และ วันที่สร้างวันที่หมด อายุของ token
signature เป็นตัวบ่งชี้ว่า token ที่ส่งมา นั้น เป็นของจริงหรือไม่

เมื่อ user login เข้าระบบ มา เซิฟเวอร์จะทำการสร้าง token ให้user ไปใช้ โดยtoken ที่ได้ จะยกตัวอย่างดังข้างล่าง
header = { alg: “hs256” type: “jwt”}
Payload = { id: 5 ,name: xxxx , age : 000, exp: “10/7/2563”}
Signature = asdf256
หาก user ต้องการจะเข้าไปในส่วนที่เป็นข้อมูลส่วนตัว หรือส่วนที่ต้องได้รับอนุญาติ เซิฟเวอร์จะทำการเช็ค token ของ user ว่าถูกต้องหรือไม่ โดย จะนำส่วน header กับ payload ของtoken user มา hash ด้วย รหัสลับ(secret หรือ key) แล้วนำมาเช็ค signature ของ token user อีกทีว่าตรงกันมั้ย
ถ้าไม่ตรงกัน แสดงว่ามีการปลอมแปลง หรือ แก้ไขtoken บางอย่าง

เพราะ ตัว signature จะเข้ามาทำหน้าที่ตรวจสอบความถูกต้อง
โดยวิธีการทำงานของมันคือ นำส่วน header กับ payload ที่ผ่านการ encryptions มาต่อกันแล้วทำการ hash (ใช้ รหัสลับที่ทางฝั่งเซิฟเวอร์เท่านั้นที่รู้ นำ2ส่วนมาเข้ารหัส) สิ่งที่ผ่านการ hash มาแล้ว เราจึงจะนำมาใช้เป็น signature
หมายความว่า ถ้าข้อมูลใน payload เปลี่ยนไป signature จะต้องเปลียนด้วย

Access Token จะใช้แทน Username และ Password (สามารถใช้อย่างอื่นเพื่อขอ Token ก็ได้) เพื่อนำไปใช้กับบริการอื่น ๆ ทำให้มีความปลอดภัยมากขึ้น รวมถึงบอกว่าทำมีสิทธิ์ทำอะไรได้บ้างกับบริการยกตัวอย่างการ authen ด้วย facebook จะบอกว่า เราจะสามารถเข้าถึงข้อมูลหรือบริการส่วนได้ได้บ้าง นอกจากนี้ จะยังสามารถเพิกถอนหรือ revok สิทการเค้าถึงได้อีกโว้ย ส่วน Refresh Tokens คือแนวคิดของการแก้ไขปัญหาหาก Access Token หมดอายุเร็วเรื่องจากข้อมูลใน Access Token จะได้รับการ Update อยู่เสมอ สามารถยกเลิกการเข้าใช้งานของ ผู้ใช้ โดยไม่จำเป็นต้องให้ผู้ใช้ทำการ Authen บ่อยๆ โดย ยกตัวอย่างคร่าวๆ หากเราตั้งเวลาให้ access token หมดอายุหลังจาก 1 นาที เวลาที่สามารถ refresh token ได้เป็น 2 นาที เรา login และได้ access token ตัวแรกที่นาทีที่ 0 เมื่อเราใช้งานไปสักพักถึงนาทีที่ 1.1 token หมดอายุ ระบบทำการ refresh token ได้ตามปกติ แล้วเราก็ใช้งาน token ตัวใหม่ต่อไปจนถึงนาทีที่ 2.1 token หมดอายุ ระบบทำการ refresh token จะได้ error กลับมาว่า token นั้นหมดอายุแล้ว เนื่องจากเลยกำหนดเวลาที่สามารถ refresh token ได้