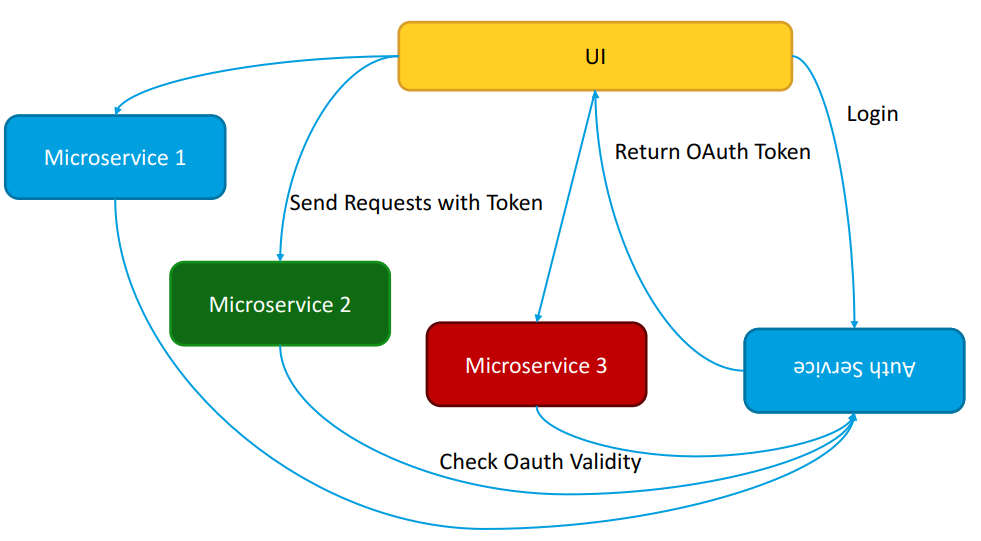
Overview

* Introduction
* What’s the problem anyway?
* And how exactly do JSON Web Tokens help here?
* What are JSON Web Tokens?
* Some examples
* Mind the gap
* JWS vs. JWE

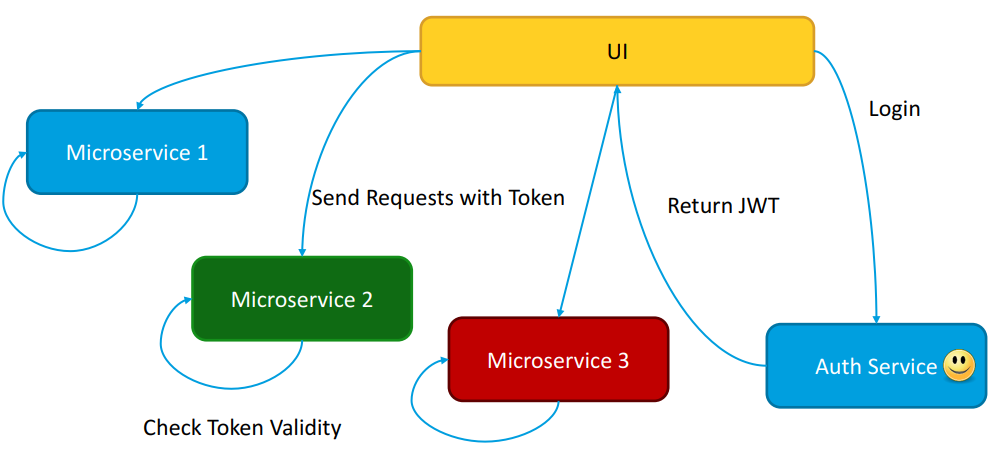
Introduction

And how do JWT exactly help here?

Typical Auth Flow



And now with JWT



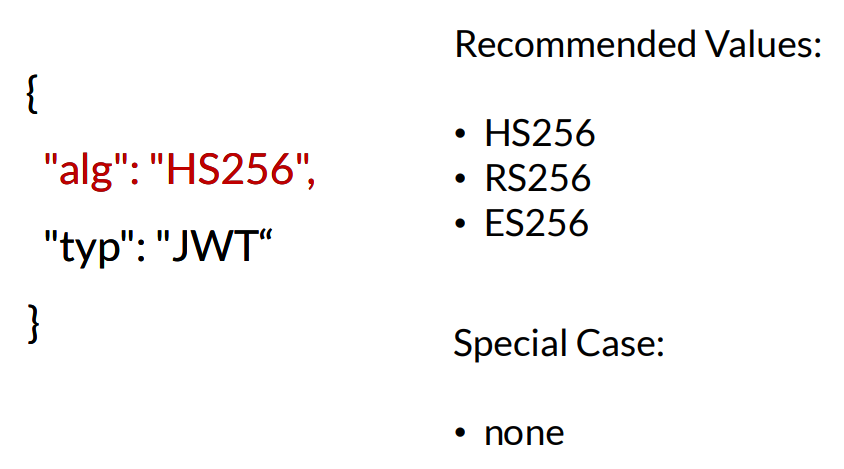
What are JSON Web Tokens?

RFC 7519: “JSON Web Token (JWT) is a compact, URL-safe means of representing claims to be transferred between two parties.”

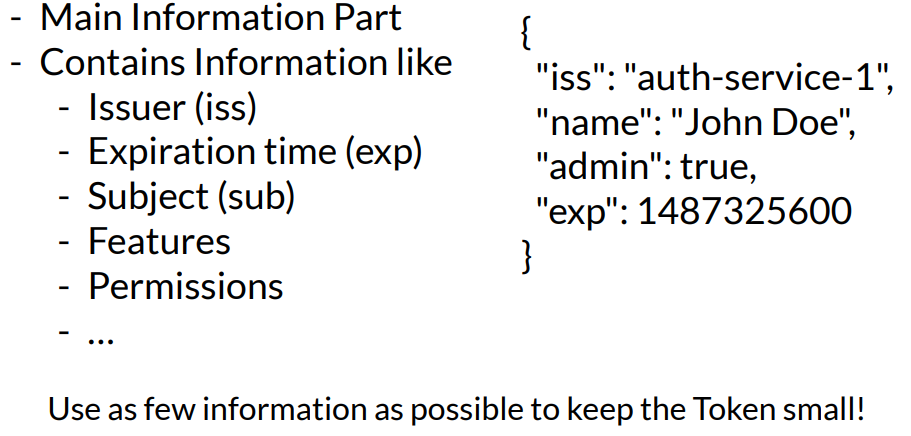
Two Types:-

* JSON Web Signature
* JSON Web Encryption
* JSON Web Signature (RFC 7515)  
  Header  
  Payload (Claims)  
  Signature

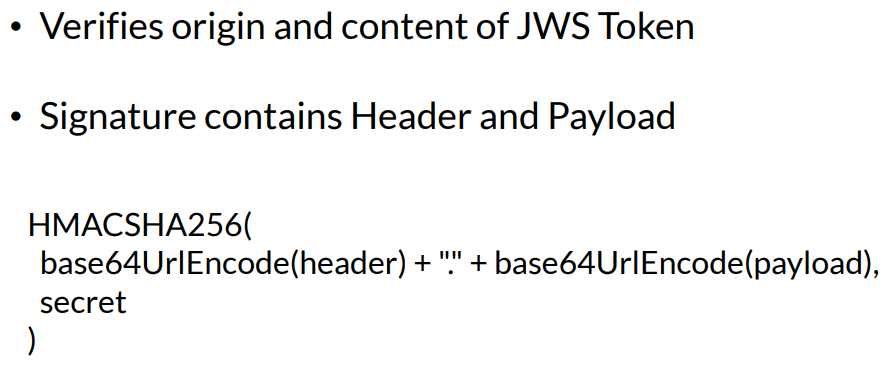
JWS - Header



JWS – Payload



JWS – Signature

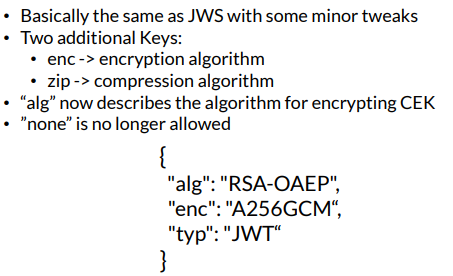
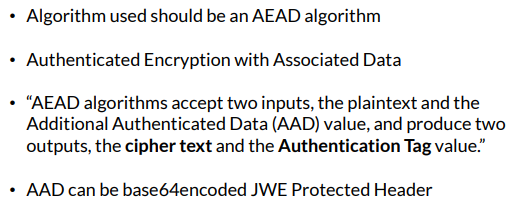
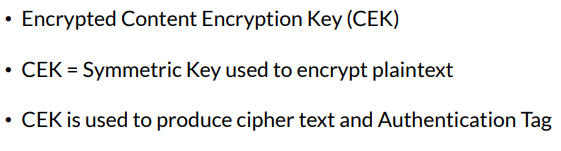
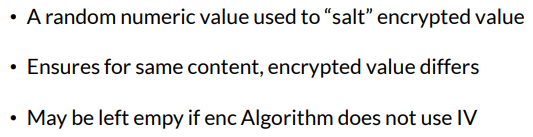
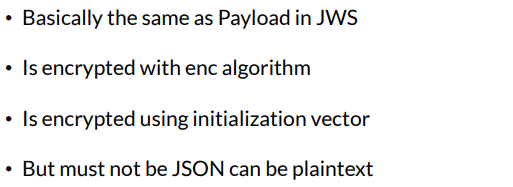
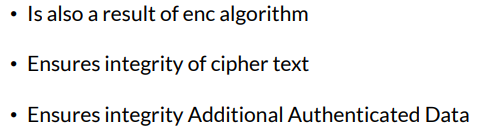
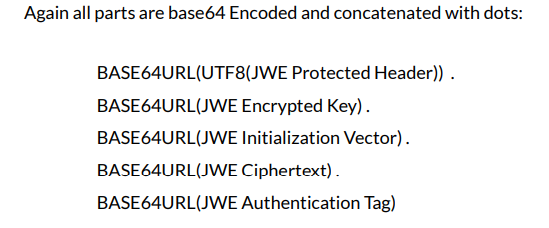


JWS Example

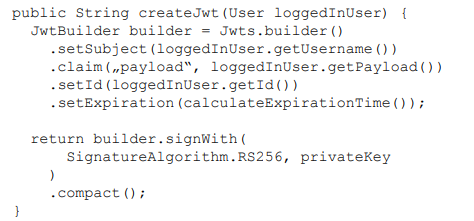


JSON Web Encryption (RFC 7516)

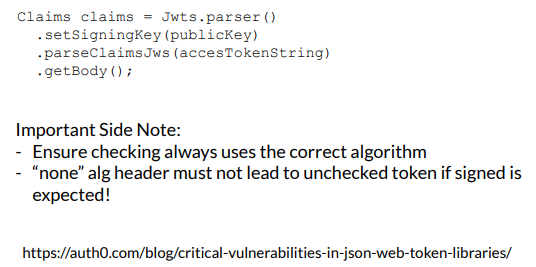
Five Parts (JWE)

1. Protected Header
2. Encrypted Key
3. Initialization Vector
4. Cipher text
5. Authentication Tag
6. JWE Protected Header  
   
7. JWE Protected Header  
   
8. JWE Encrypted Key  
   
9. JWE Initialization Vector  
   
10. JWE Ciphertext  
    
11. JWE Authentication Tag  
    
12. JWE  
    

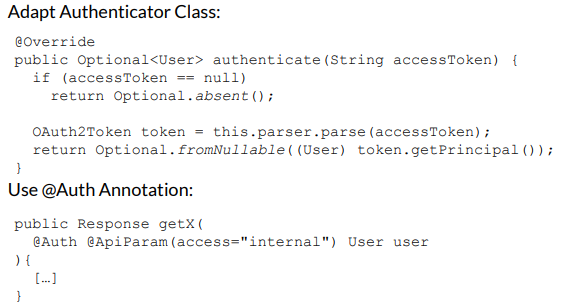
JWS creation in Java



JWS checking in Java

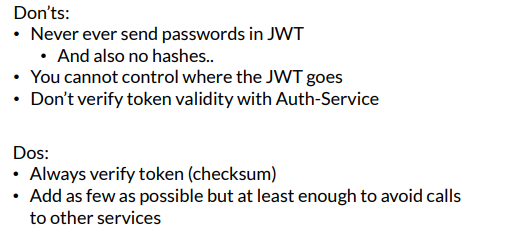


JWS Usage in Java with Dropwizard



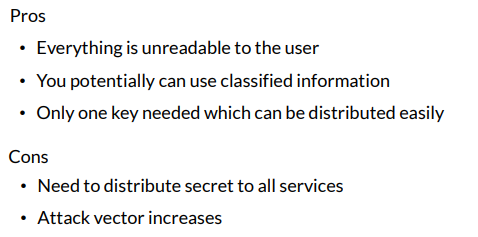
Mind the gap

Mind the gap

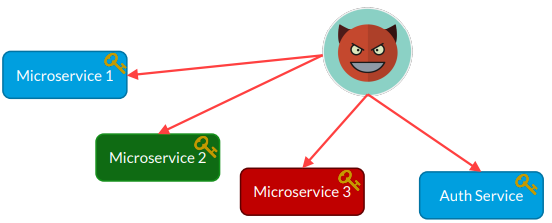


Back to JWS vs JWE

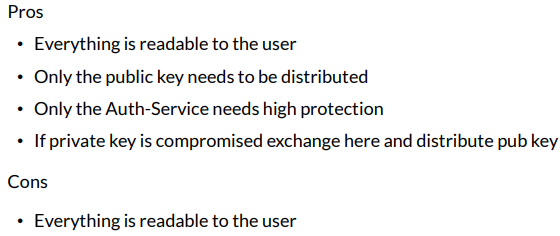
JSON Web Encryption (JWE)



JSON Web Encryption (JWE)



JSON Web Signature (JWS)



JSON Web Signature (JWS)

