如何使用Ktor作为服务器和客户端网络请求框架并且使用JWT作为身份安全验证

李卓轩 | Ikutsu 2023/07/23

1. 什么是JWT

eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXV
CJ9.eyJpc3MiOiJodHRwczovL3d3dy5rb
3RsaW5sYW5nLm9yZyIsIm5hbWUiOiJLb3
RsaW4gSmV0YnJhaW5zIiwiYWRtaW4iOnR
ydWV9.o1v1Mg5QHbNumUI8c9JyMSUt4sf
BgKOClxMnc6jWTnQ

JWT（JSON Web Token）

1. 什么是JWT

Base64Url？为什么要用？

2. JWT的解构

- Header (头部)
- Paylod (载荷)
- Signature（签名）

HEADER: ALGORITHM & TOKEN TYPE

```
{
  "alg": "HS256",
  "typ": "JWT"
}
```

PAYLOAD: DATA

```
{
  "iss": "https://www.kotlinlang.org",
  "name": "Kotlin Jetbrains",
  "admin": true
}
```

VERIFY SIGNATURE

```
HMACSHA256(
  base64UrlEncode(header) + "." +
  base64UrlEncode(payload),
  KotlinIsTheBest
) ☐ secret base64 encoded
```

2.1 Header（头部）

- “alg” – Algorithm（算法）
  例如：HMAC，RSA和ECDSA
- “typ” – Type （类型）
  固定为JWT

```
{
  "alg": "HS256",
  "typ": "JWT"
}
```

2.2 Payload（载荷）

iss	Issuer
sub	Subject
aud	Audience
exp	Expiration Time
nbf	Not Before
iat	Issued At
jti	JWT ID

Registered cl

2.2 Payload（载荷）

```
{
  "iss": "https://www.kotlinlang.org",
  "name": "Kotlin Jetbrains"
  "admin": true
}
```

Public claim（公共声明）

https://www.iana.org/assignments/jwt/jwt.xhtml#claims

2.2 Payload（载荷）

```
{
  "iss": "https://www.kotlinlang.org",
  "name": "Kotlin Jetbrains",
  "admin": true
}
```

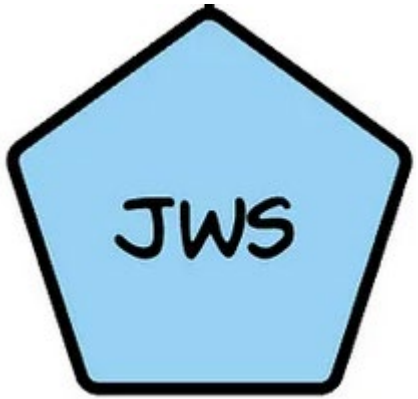
Private claim（私人声明）

2.3 Signature（签名）

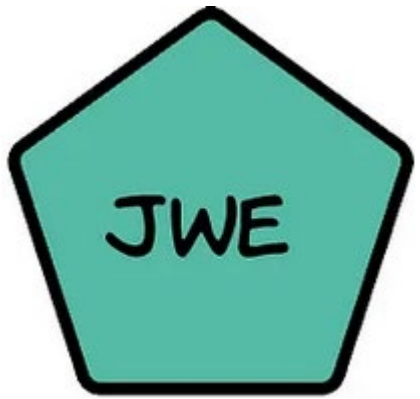
```
HMACSHA256(
  base64UrlEncode(header) + "." +
  base64UrlEncode(payload),
  KotlinIsTheBest
) ☐ secret base64 encoded
```

签名

3. JWT类型

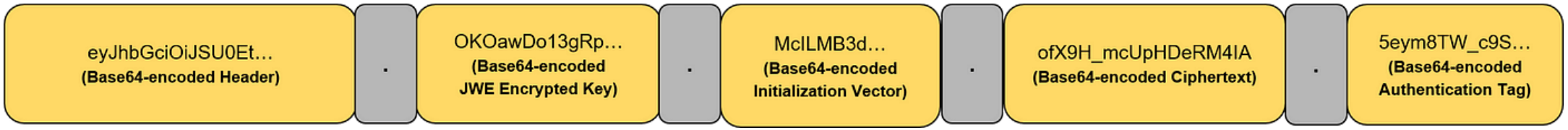


JWS（JSON Web Signature）



JWE（JSON Web Encryption）

3. JWT类型

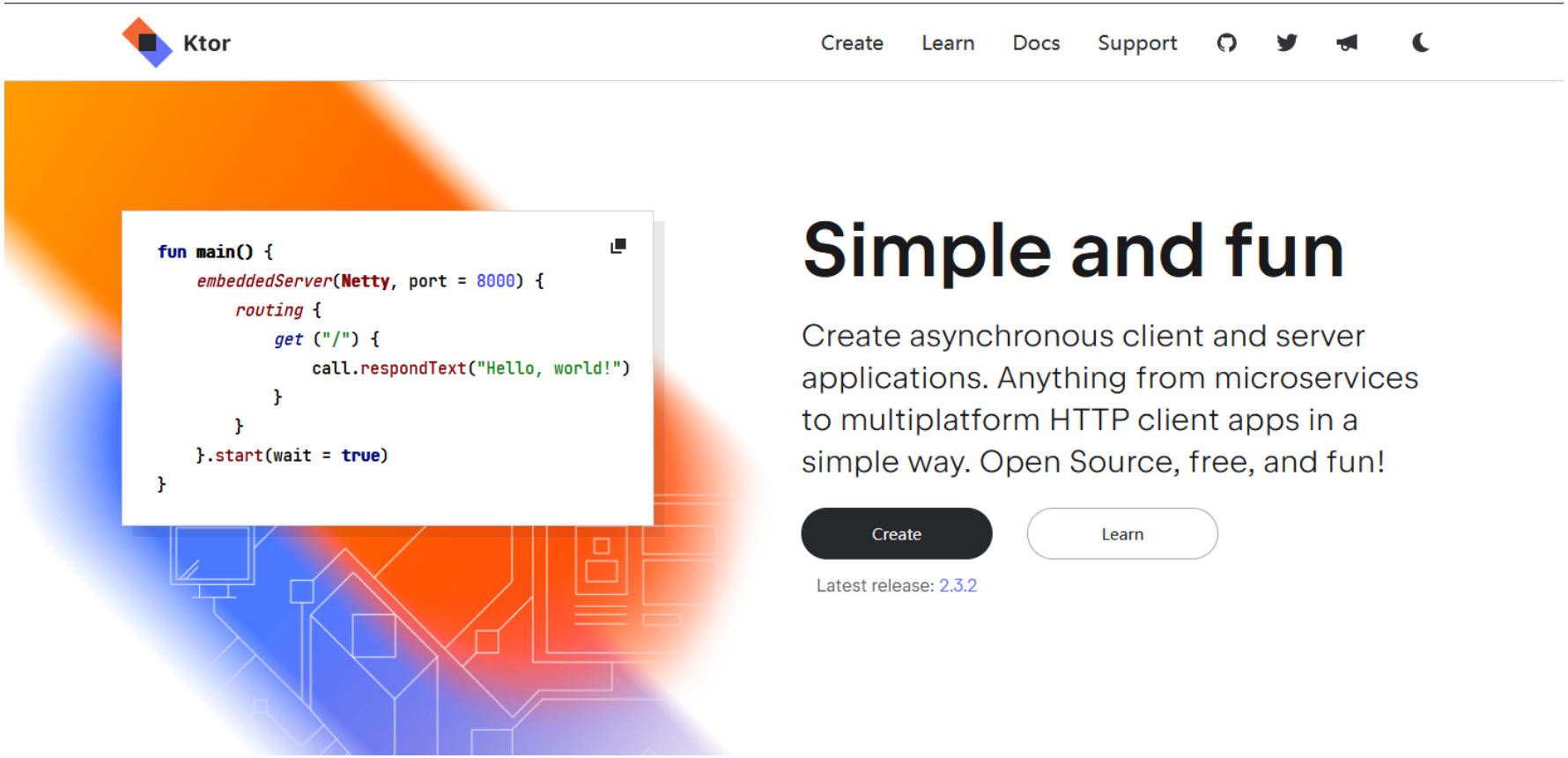


头部　　加密密钥　　初始化向量　　密文　　认证标签

4. JWT的优势

无状态 自包含 高通用性 安全

5. Ktor?



https://ktor.io/

6. Ktor的优势

异步 插件化

7. Ktor中的JWT

Security of JWTs JWT 的安全性

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.

JSON 对象中包含的信息是经过数字签名的，因此可以验证和信任。虽然 JWT 也可以加密，以便在各方之间保密，但 Auth0 签发的 JWT 是 JSON Web 签名（JWS），这意味着它们是经过签名而不是加密的。

As such, we will focus on signed tokens, which can verify the integrity of the claims contained within them, while encrypted tokens hide those claims from other parties.

因此，我们将把重点放在签名令牌上，因为签名令牌可以验证其中所含声明的完整性，而加密令牌则可以向其他方隐藏这些声明。

来源:https://auth0.com/docs/secure/tokens/json-web-tokens#security-of-jwts

8. 项目技术栈

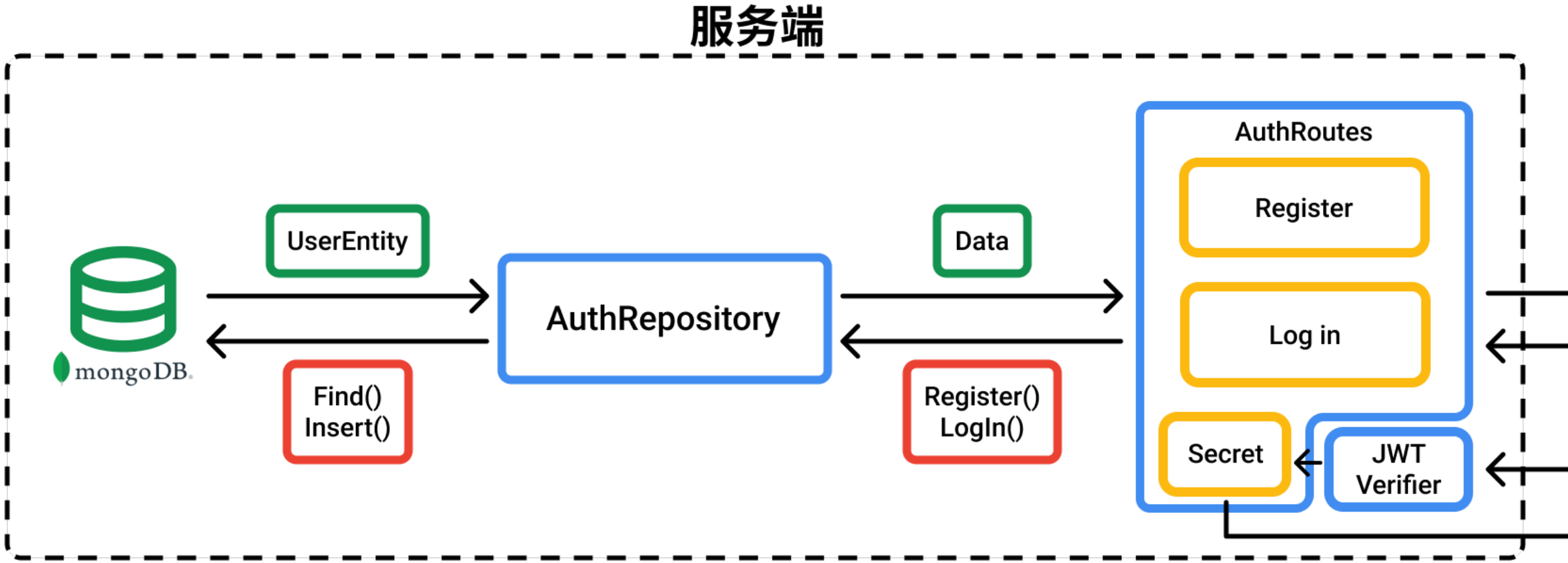
服务端

- IDE - Intellij IDEA 2023.1.3
- Kotlin - 1.9.0
- Ktor - 2.3.2
  - Engine - Netty
  - Serialize - Kotlinx-json
- KMongo - MongoDB SDK

客户端

- IDE - Android Studio Giraffe
- Kotlin - 1.8.10
- AGP - 8.1.0-rc01
- Compose - 2023.06.01
- Material 3
- Navigation
- Hilt
- Ktor - 2.3.2
  - Engine - CIO
  - Serialize - Kotlinx-json

9. 项目结构


服务端
mongoDB
UserEntity
Find()
Insert()
AuthRepository
Data
Register()
LogIn()
AuthRoutes
Register
Log in
Secret
JWT
Verifier

10. 参考文献

https://jwt.io/

https://auth0.com/docs/secure/tokens/json-web-tokens

https://www.cisco.com/c/zh_cn/support/docs/security/web-security-appliance/117925-technote-csc-00.html

https://datatracker.ietf.org/doc/html/rfc7519

https://www.loginradius.com/blog/engineering/guest-post/what-are-jwt-jws-jwe-jwk-jwa/

11. 延伸阅读

Ktor官方文档

https://ktor.io/docs/jwt.html

掘金文章

https://juejin.cn/post/7251104465730175031

Medium文章 *全英文

https://medium.com/swlh/all-you-need-to-know-about-json-web-token-jwt-8a5d6131157f

https://medium.com/@er.imran4u/kotlin-ktor-with-jwt-authentication-ed78251629c2