



Embarcadero Conference



JSON Web Tokens De onde vêm? Como se reproduzem?

[Wagner R. Landgraf - TMS Software]

[Palestrante]

Wagner Landgraf

- Formação em Engenharia Elétrica com Ênfase em Eletrônica e Telecomunicações – UTFPR – Universidade Tecnológica Federal do Paraná
- Mestrado em Informática Industrial - UTFPR
- Experiência com Delphi desde a primeira versão – 1995.
- Arquiteto de frameworks Delphi: TMS Aurelius, XData, Scripter, etc.

[TMS Software]

<http://www.tmssoftware.com>

- Fundada em 1995
- Matriz: Bélgica. Presença física no Brasil, Uruguai, França e Rússia.
- Missão: Produtos e soluções para desenvolvimento de software
- Atende o mercado Delphi desde a sua primeira versão em 1995

[JSON Web Token]

- Padrão (RFC-7519) para representação de “claims” de forma segura
- “Fulano, tenho essa informação!”
- “E ela é verdadeira porque foi VOCÊ que assinou, veja a sua assinatura!”

[JSON Web Token]

aaaaaaaaaaaaaaaaa.bbbbbbbbbbbbbbbbbb.cccccccccccccccc

Uma string com três seções separadas por pontos

Duas primeiras seções: JSON codificado com BASE64

Exemplo real:

eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6IkpvaG4gRG9lIiwiaWF0IjE0NjQ5OTI0Mj0.dWV9.TJVA95OrM7E2cBab30RMHrHDcEfxjoYZgeFONFh7HgQ

[JSON Web Token]

Payload

aaaaaaaaaaaaaaaaa.bbbbbbbbbbbbbbbbbb.cccccccccccccccc

[JSON Web Token]

Header

Payload

aaaaaaaaaaaaaaaaa.bbbbbbbbbbbbbbbbbb.cccccccccccccccc

[JSON Web Token]

Header

Payload

Signature

aaaaaaaaaaaaaaaaa.bbbbbbbbbbbbbbbbbb.cccccccccccccccc

[JSON Web Token]

Header

Payload

Signature

aaaaaaaaaaaaaaaaa.**bbbbbbbbbbbbbb**.ccccccccccccccc

```
{  
  "name": "wagner",  
  "admin": true  
}
```

[JSON Web Token]

Header

Payload

Signature

aaaaaaaaaaaaaaaaa.bbbbbbbbbbbbbbb.ccccccccccccccc

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


[JSON Web Token]

Header

Payload

Signature

aaaaaaaaaaaaaaaa.bbbbbbbbbbbbbb.**ccccccccccccccc**

HMACSHA256(

base64UrlEncode(header) + "." +

base64UrlEncode(payload),

secret

)

[JSON Web Token]

Demonstração JWT Debugger

<http://jwt.io>

[JSON Web Token]

- Autocontido: todas as informações necessárias estão nele
- Pode ser usado com JavaScript, .NET, Node.js, Java, PHP, Ruby, Python e... Delphi!
- Pode ser usado na própria URL (query string), em Cookies, header HTTP, etc.

[JSON Web Token]

Framework Delphi para JWT:
Delphi JOSE and JWT Library

<https://github.com/paolo-rossi/delphi-jose-jwt>

[Autenticação com JWT]

Vantagens (JWT vs Cookies/Outros)

- Stateless, escalável
- Desacoplado: Rest API, multiservidor, SPA
- Cross Domain + CORS
- Performance: autocontido
- Mobile + IoT

[Autenticação com JWT]

Pontos de atenção

- Tamanho do token
- Expiração
- Dados não-criptografados
- Armazenamento

[Autenticação Tradicional Usando Cookies]



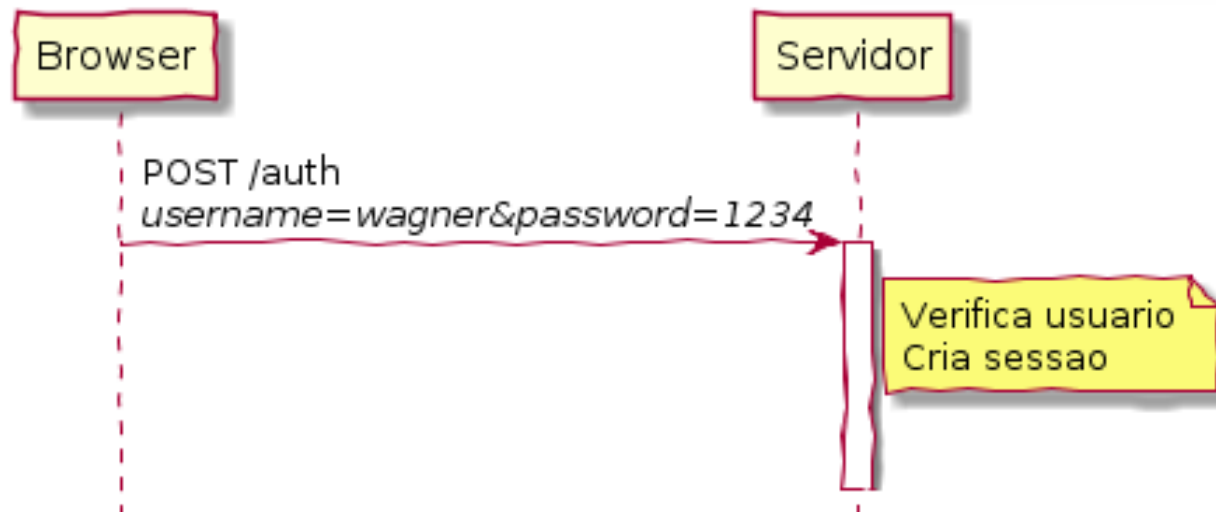
Browser

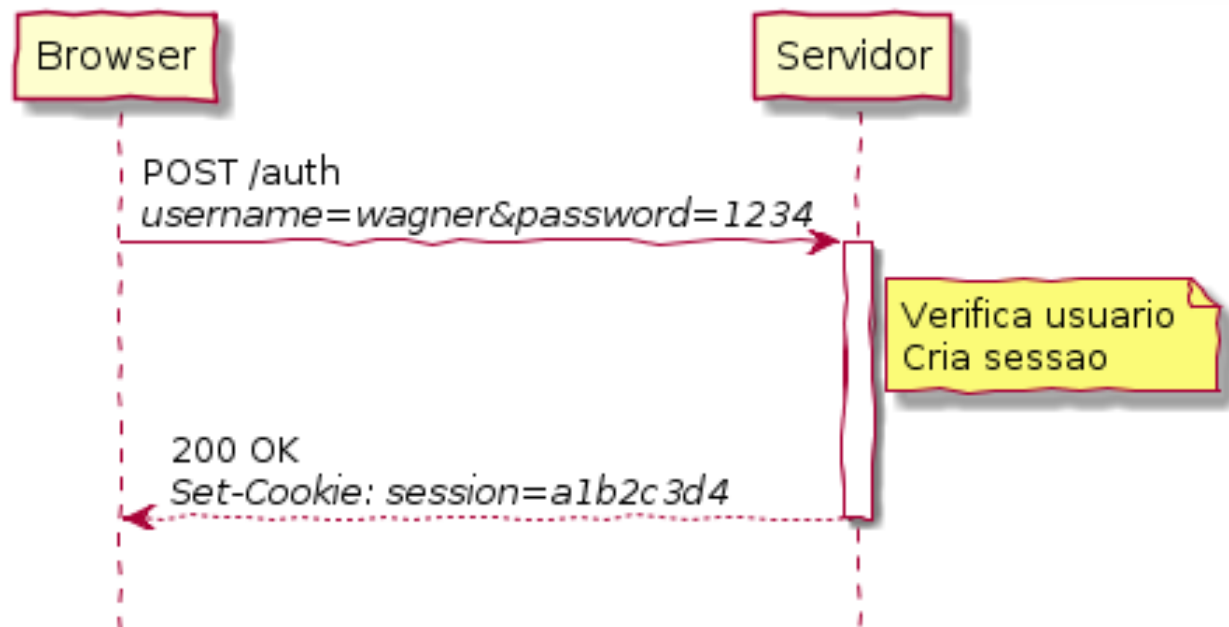
Servidor

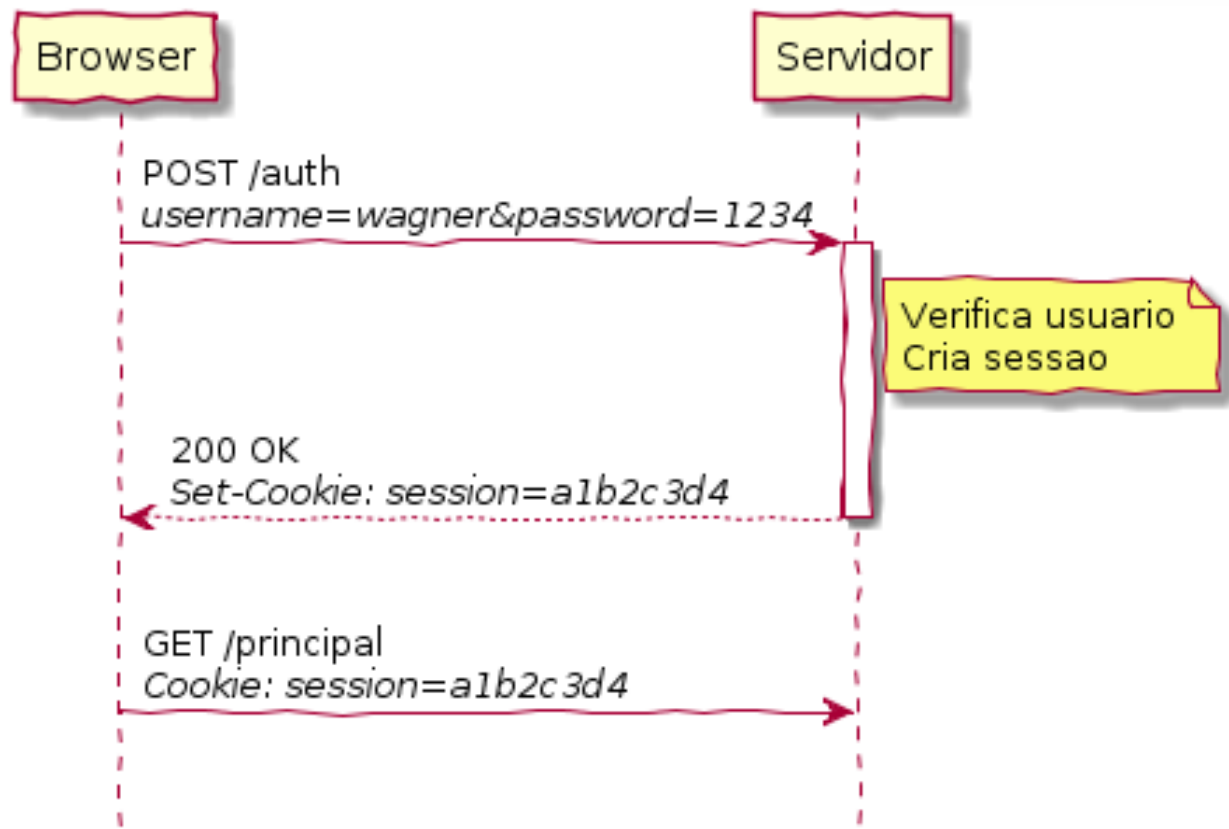
POST /auth
username=wagner&password=1234

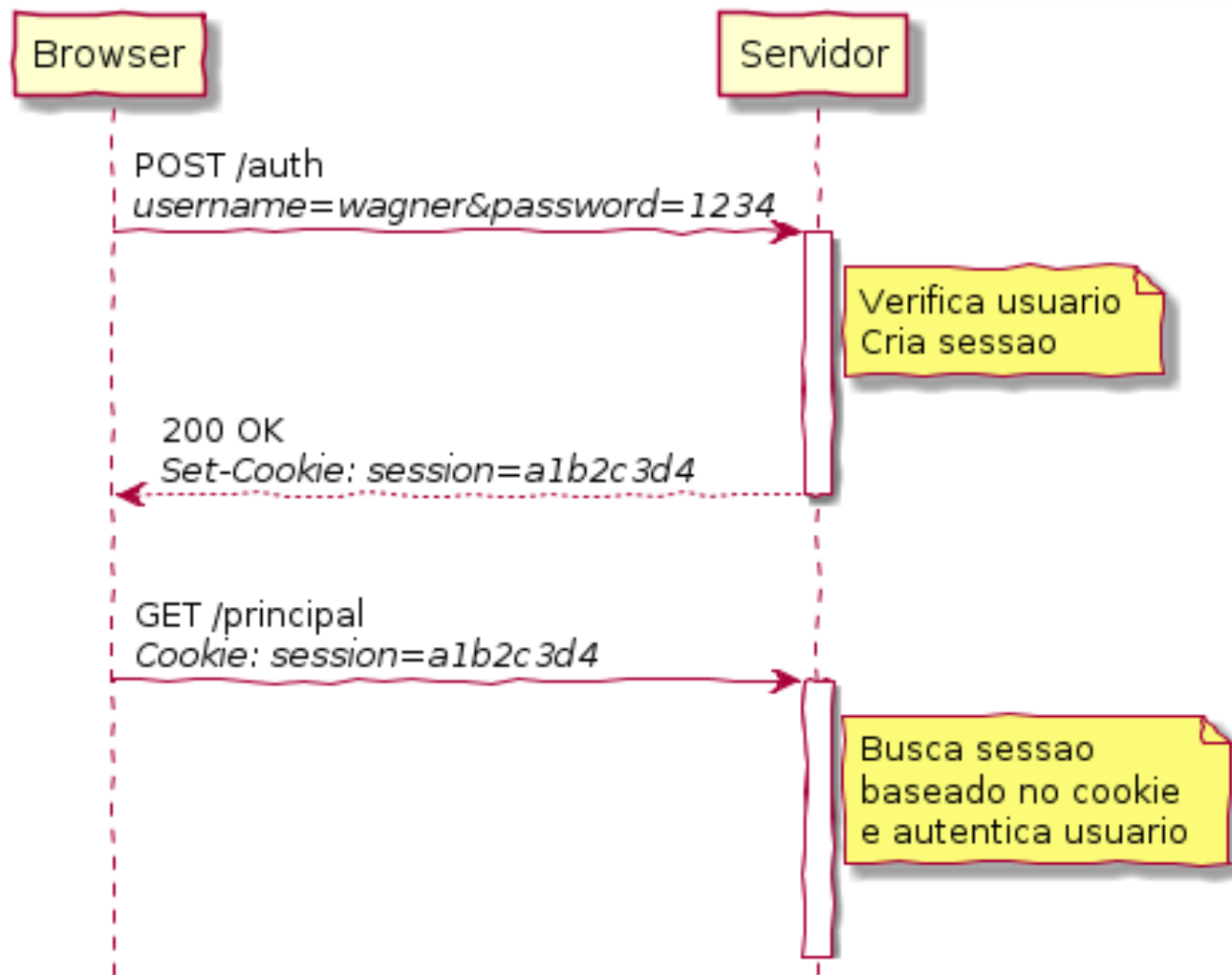


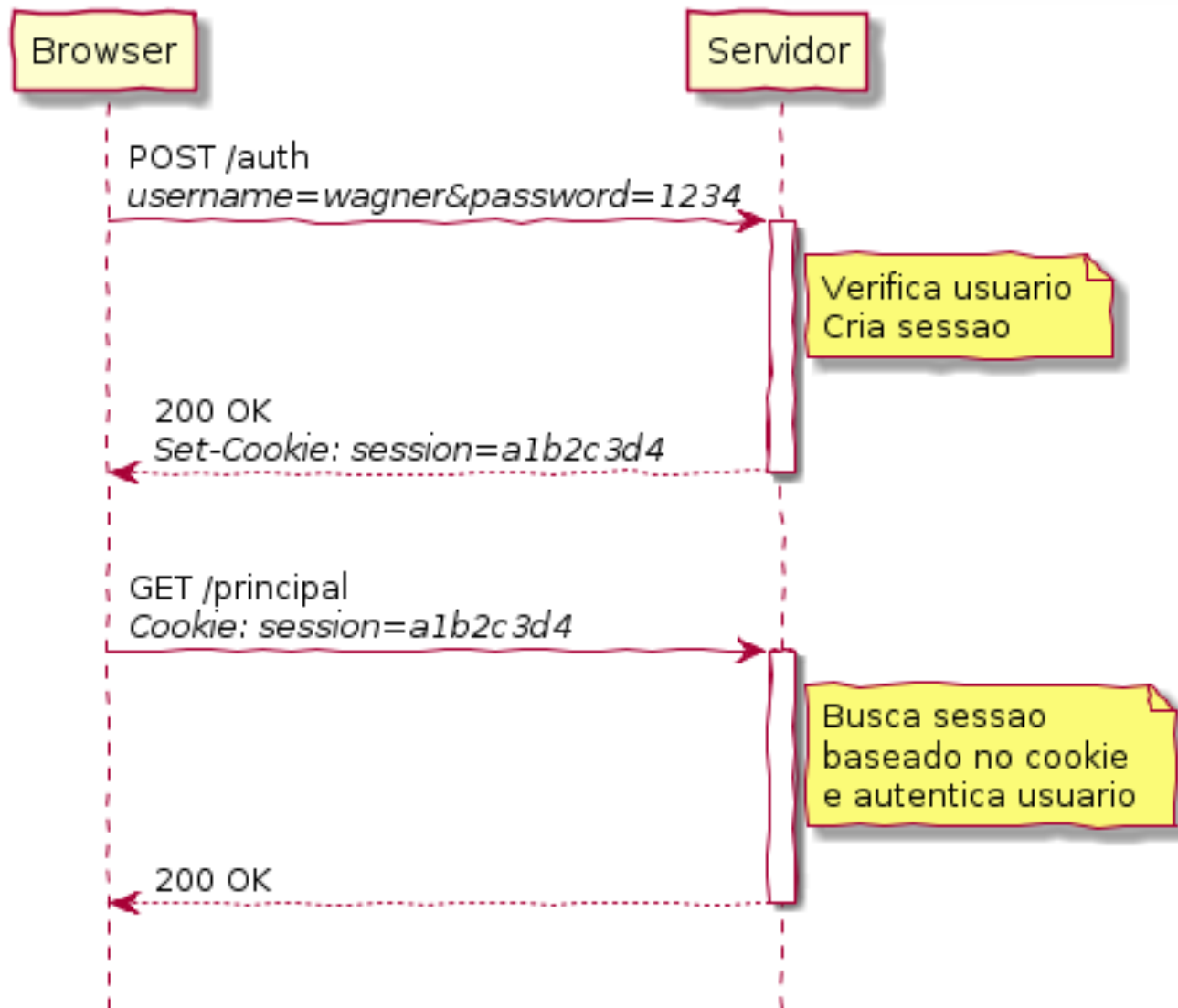
```
sequenceDiagram
    participant Browser
    participant Servidor
    Browser->>Servidor: POST /auth  
username=wagner&password=1234
```











[Autenticação Usando JSON Web Tokens]

Browser

Servidor

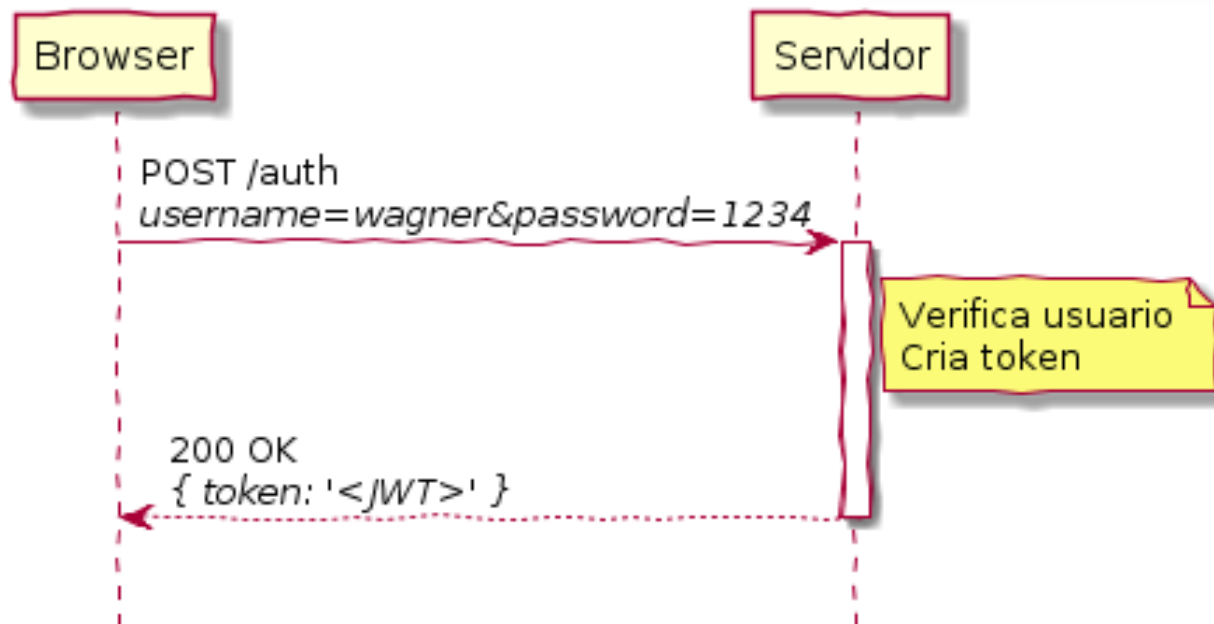
POST /auth
username=wagner&password=1234

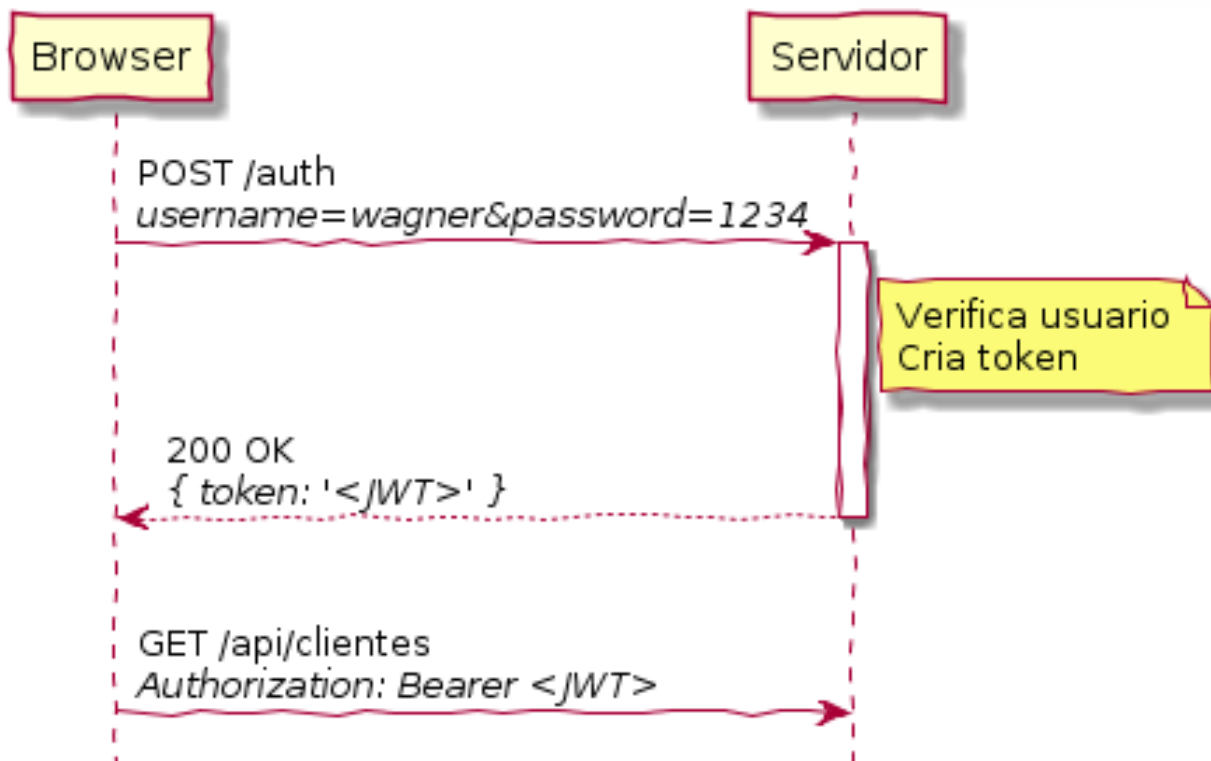
Browser

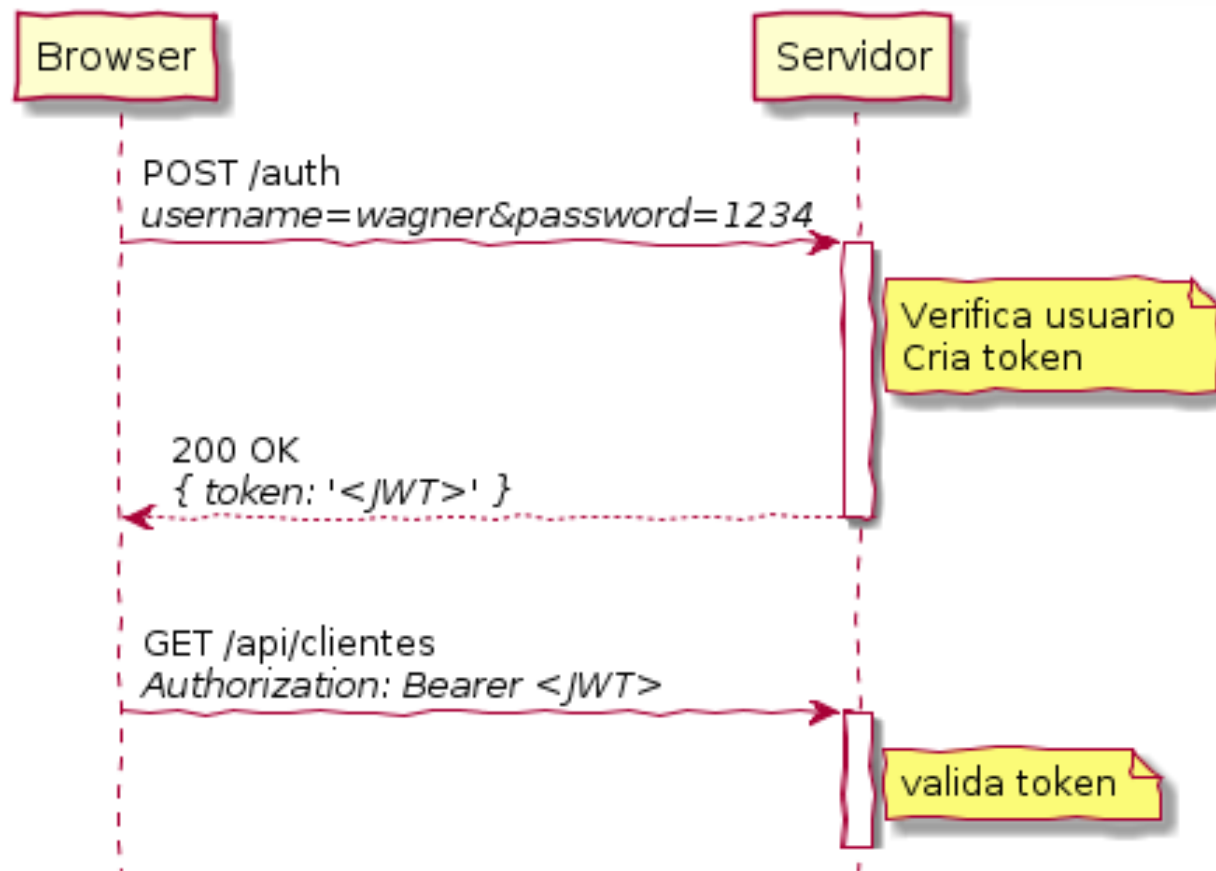
Servidor

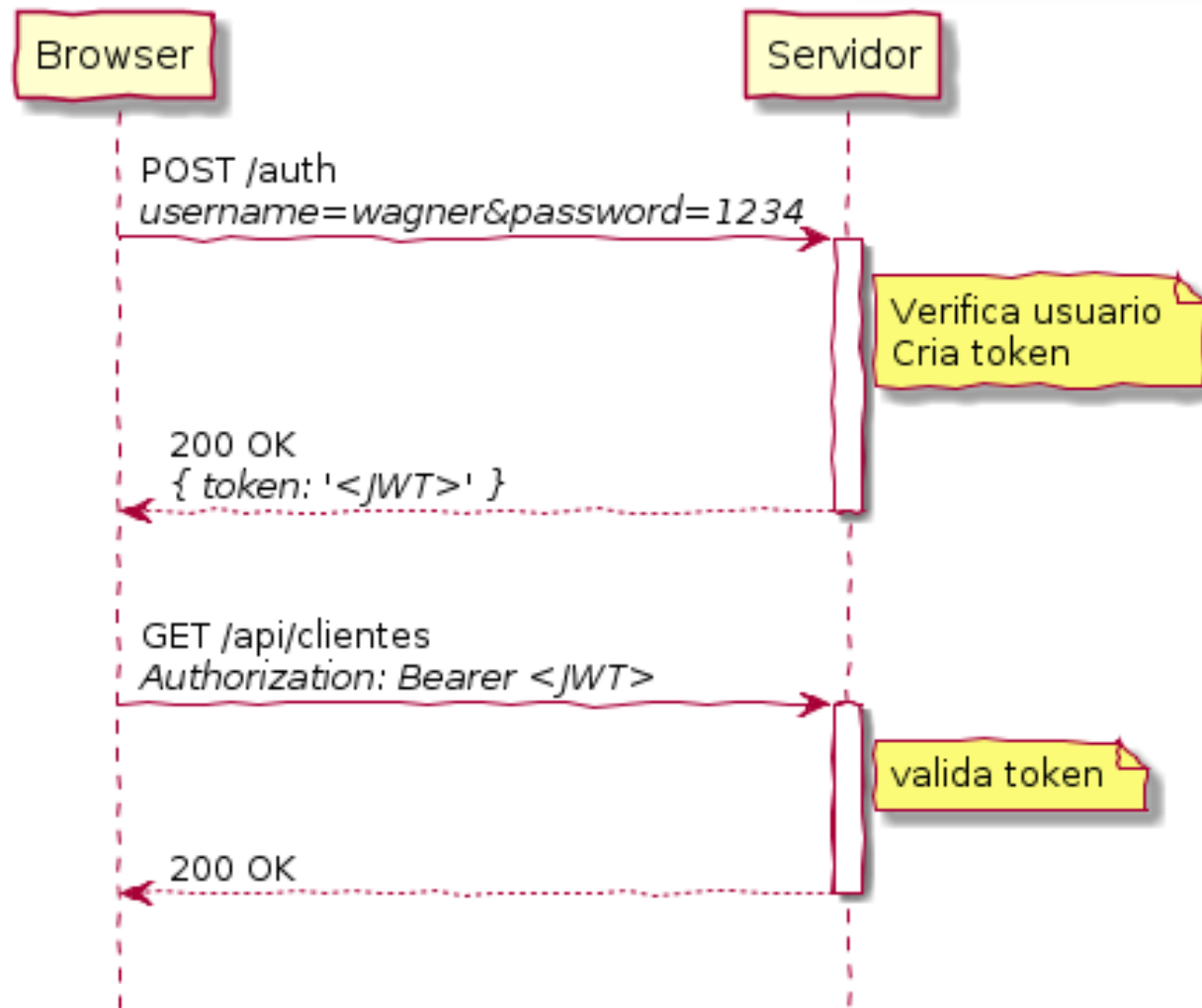
POST /auth
username=wagner&password=1234

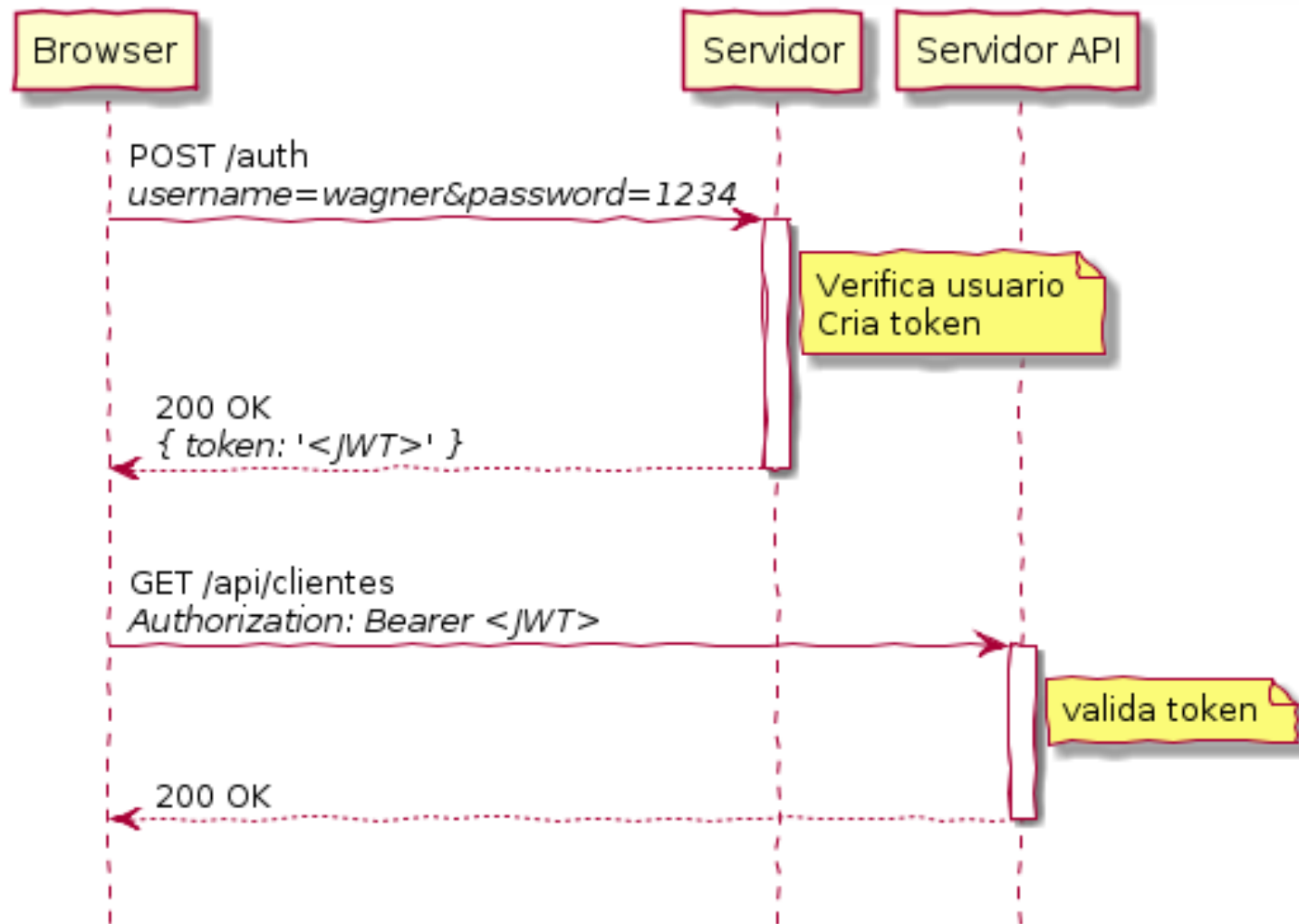
Verifica usuario
Cria token

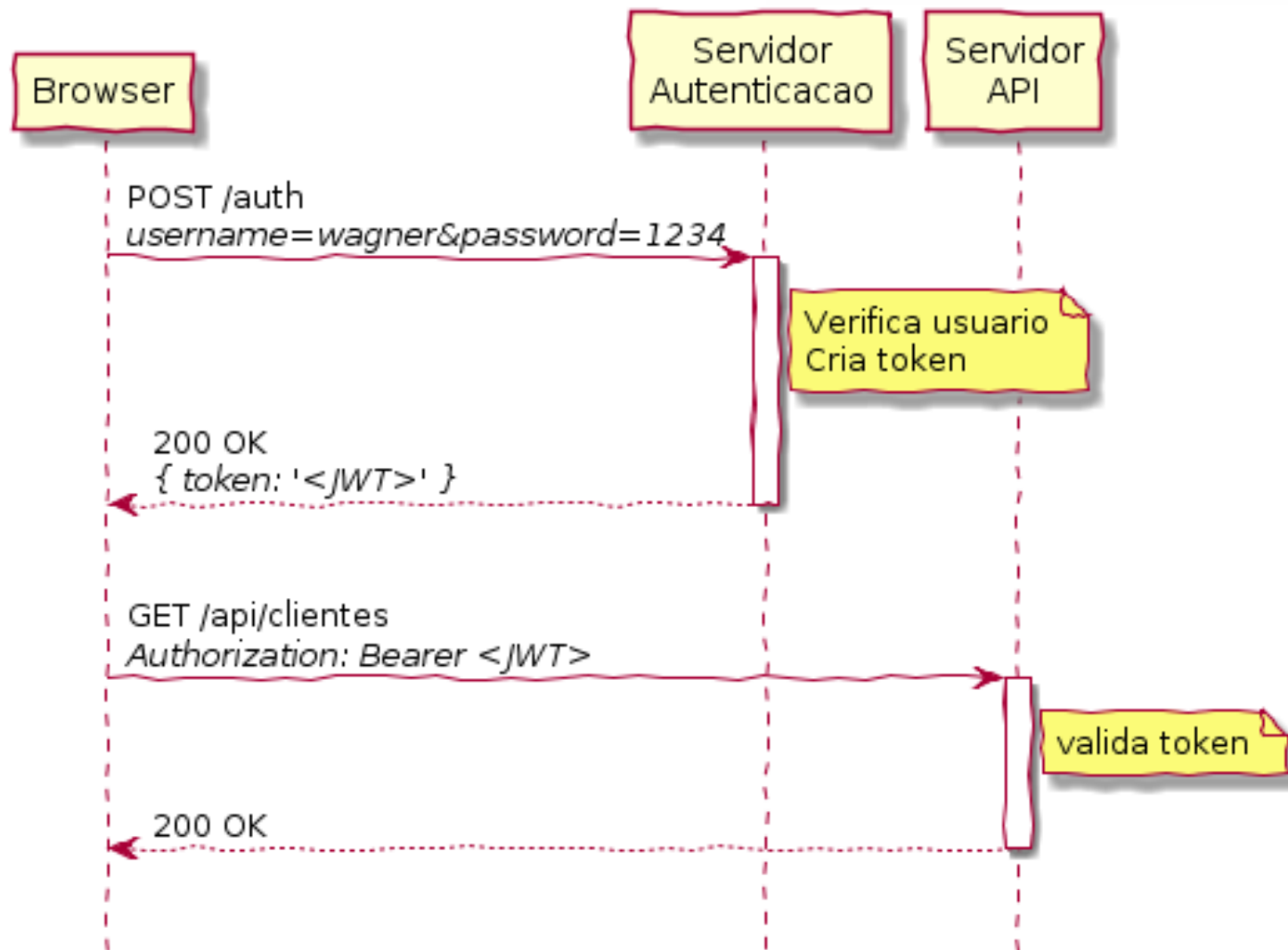


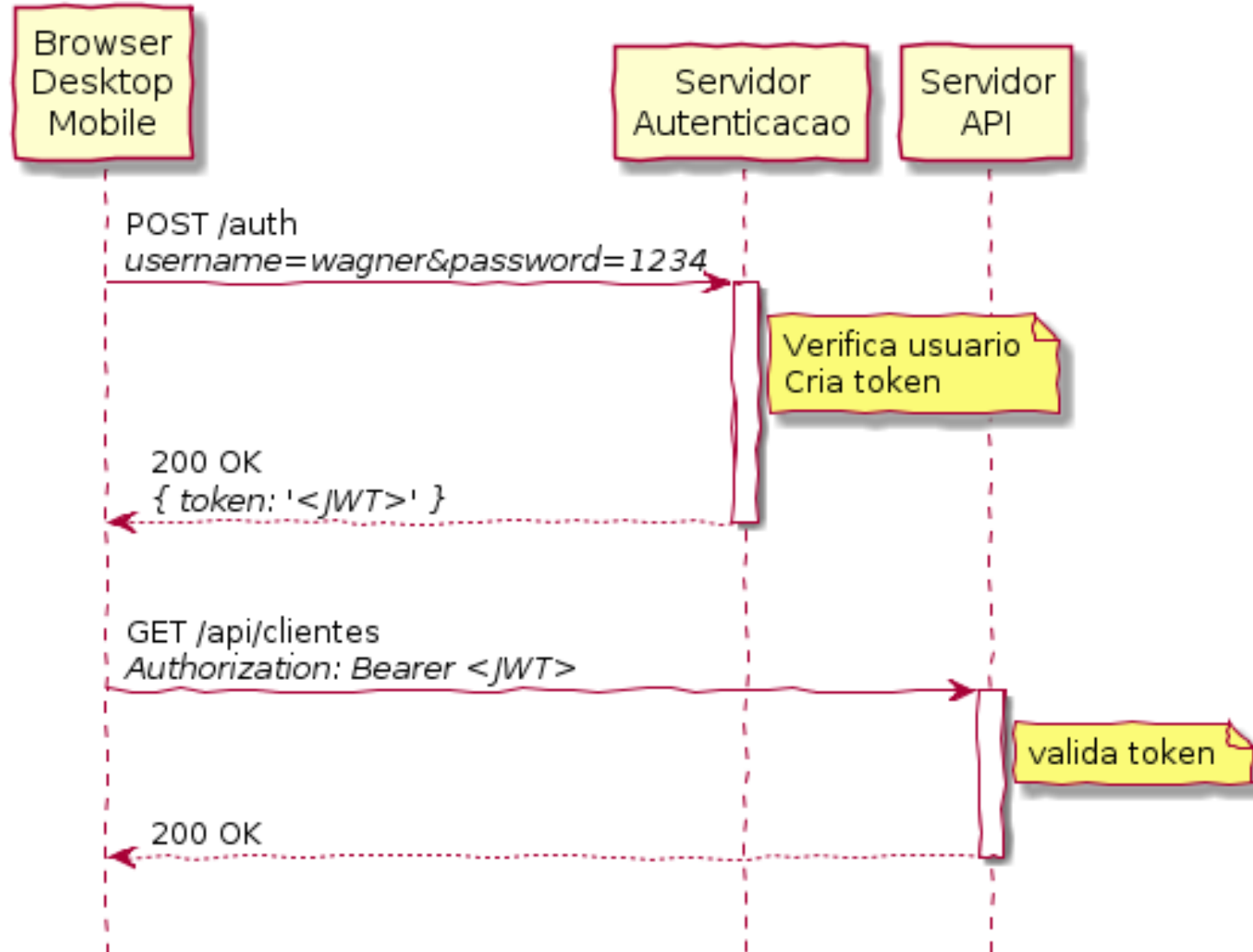












[Demonstração]

- Servidor autenticação – Delphi
- Servidor API – Delphi
- Cliente Delphi
- Cliente Web
- Utiliza TMS Business
<http://www.tmssoftware.com/site/bipack.asp>
(conceito pode ser utilizado com qualquer framework)

@ info@tmssoftware.com

TMSSoftwareNews

f TMSSoftware

[OBRIGADO]

Embarcadero  conference



Embarcadero Conference

embarcadero®