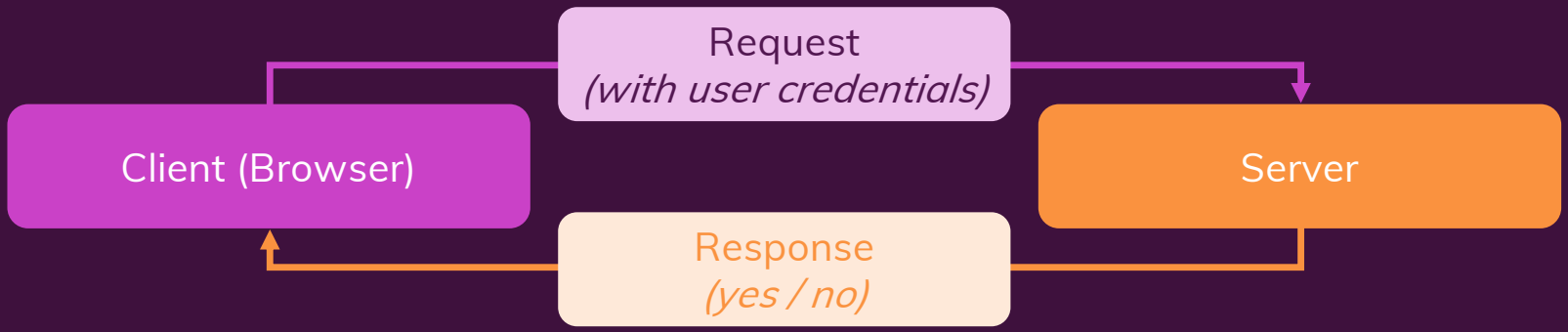
How Does Authentication Work?



Is that enough?

A “yes” alone is not enough to then access protected resources (API endpoints)

How Does Authentication Work?

We can't just save and use the "yes"

We could send a fake "yes" to the server to request protected data

Server-side Sessions

Store unique identifier on server, send same identifier to client

Client sends identifier along with requests to protected resources

Authentication Tokens

Create (but not store) "permission" token on server, send token to client

Client sends token along with requests to protected resources

SPAs Work With Tokens Instead Of Sessions

Pages are served directly and populated with logic without hitting the server

+

Backend APIs work in a “stateless” way (they don’t care about connected clients)

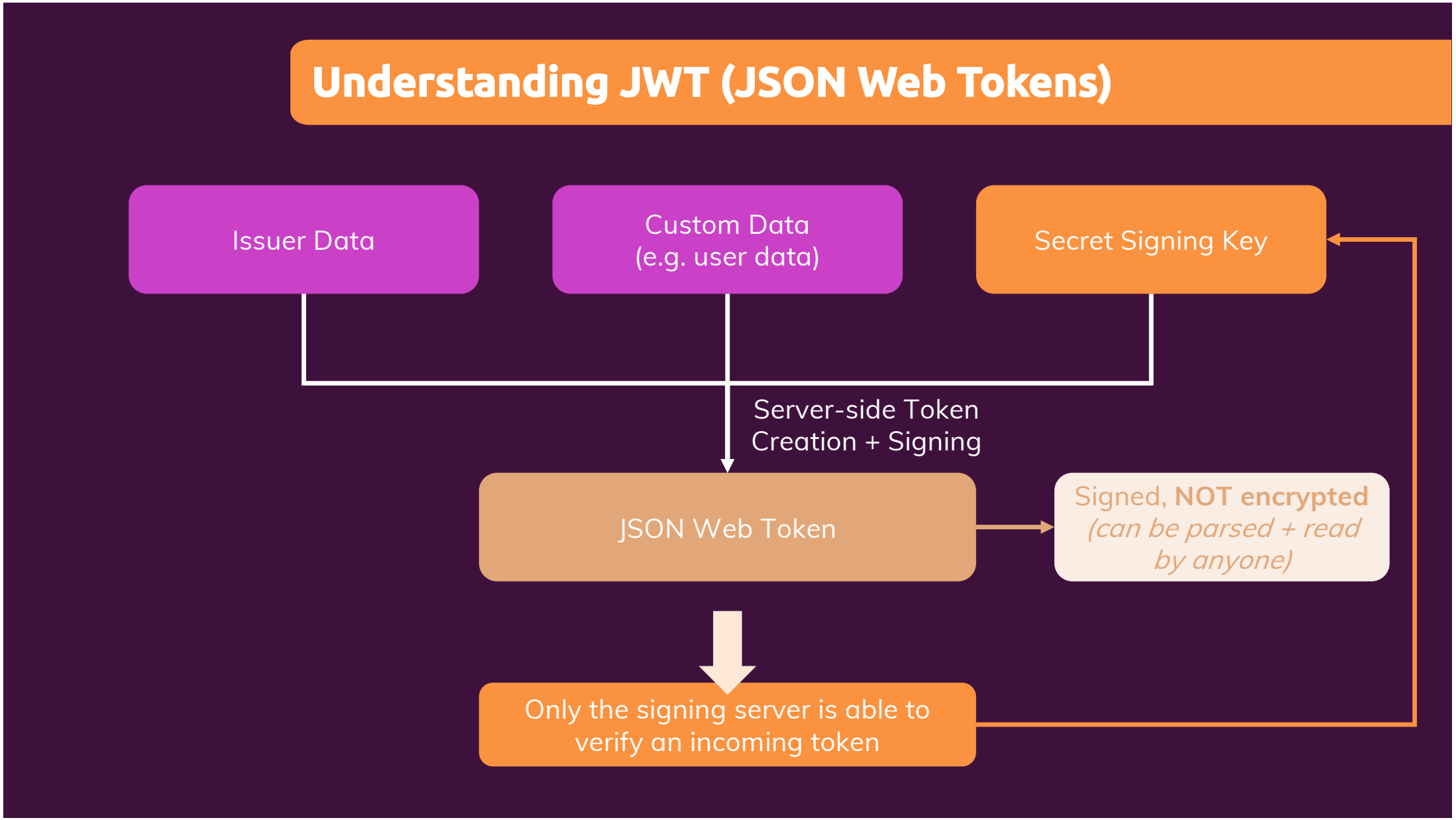
Detached

Frontend ⟷ Backend

Servers don’t save information about authenticated clients

Instead, clients should get information that allows them to prove their authentication

Tokens
(JWT: JSON Web Tokens)


Understanding JWT (JSON Web Tokens)
Issuer Data
Custom Data
(e.g. user data)
Secret Signing Key
Server-side Token
Creation + Signing
JSON Web Token
Signed, NOT encrypted
(can be parsed + read
by anyone)
Only the signing server is able to
verify an incoming token