JWT

Dominika Bobik

South Tyrol Free Software Conference 2024

Web

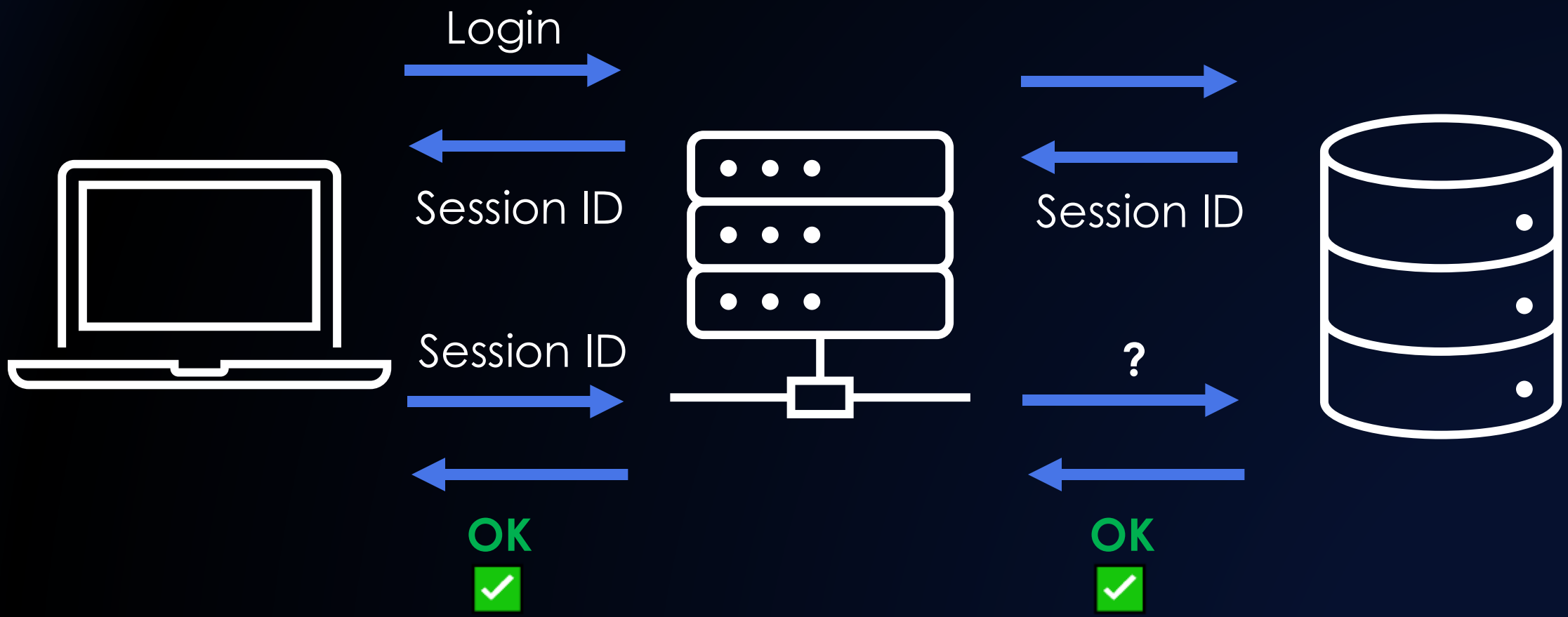
JWT

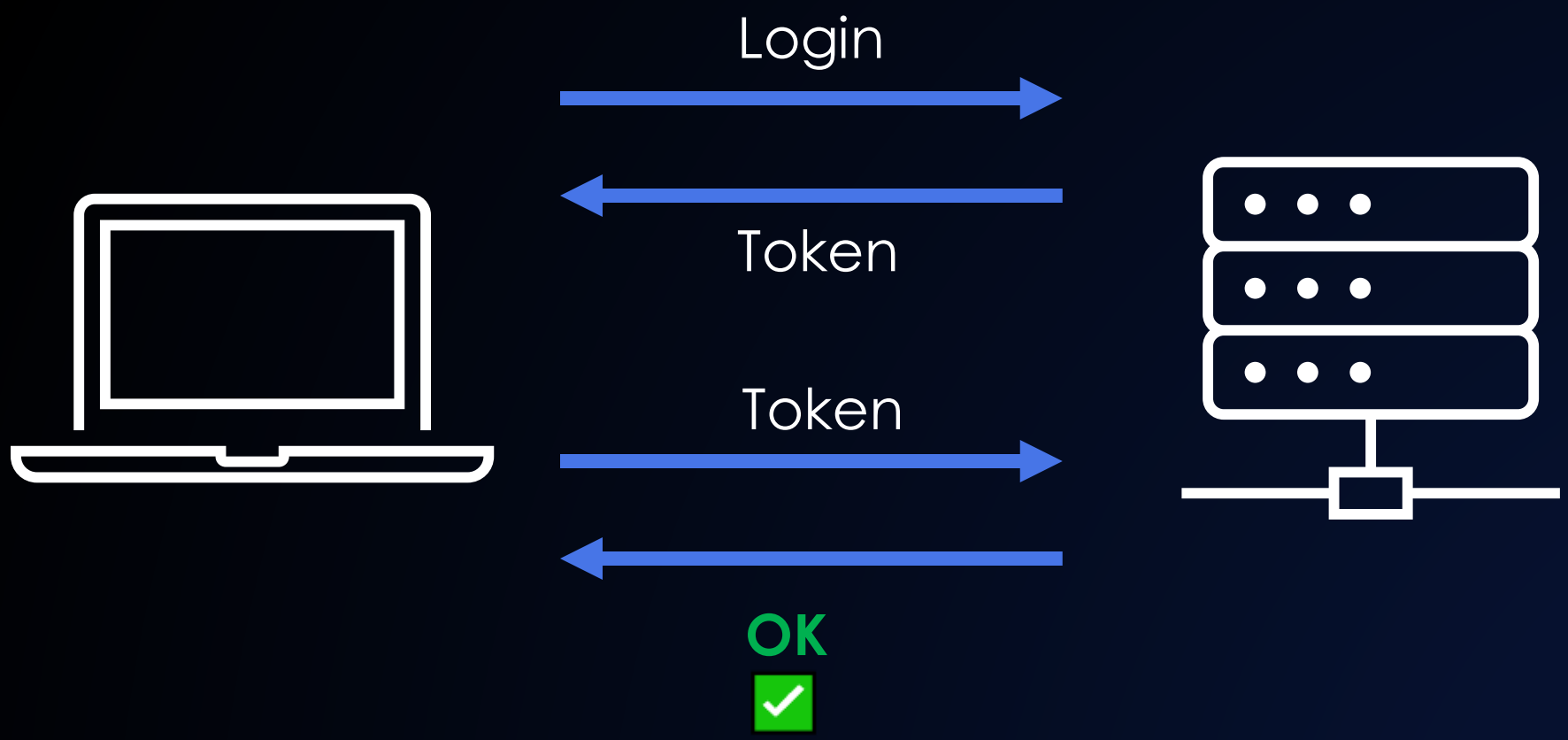
JSON

Token

JSON Web Token

eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJpc3MiOiJkb21pbmlrYWJv
YmlrLmNvbSIsImlhdCI6MTczMDAwMzA2MCwiZXhwIjoxNzYxNTM5MDU5LCJhd
WQiOiJTRlNDT04iLCJzdWIiOiJkYm9iaWtAZXhhbXBsZS5jb20iLCJuYmYiOi
IxNzYxNTM5MDU5IiwianRpIjoidW5pcXVlSUQiLCJuYW1lIjoiRG9taW5pa2E
gQm9iaWsiLCJteXNwZWNpYWxjbGFpbSI6InNwZWNpYWx2YWx1ZSJ9.JGxvQgp
b0BEUzkSuD9oySwU68WqLQjslOPLVE9cA_T8


Login
Session ID
Session ID
Session ID
?
OK
OK


Login
Token
Token
OK

1. Token as a query parameter in a URL
2. Token as a value of Sec-WebSocket-Protocol header
3. Custom payload protocol which includes the token
4. Token as a first message

eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJpc3MiOiJkb21pbmlrYWJv
YmlrLmNvbSIsImlhdCI6MTczMDAwMzA2MCwiZXhwIjoxNzYxNTM5MDU5LCJhd
WQiOiJTRlNDT04iLCJzdWIiOiJkYm9iaWtAZXhhbXBsZS5jb20iLCJuYmYiOi
IxNzYxNTM5MDU5IiwianRpIjoidW5pcXVlSUQiLCJuYW1lIjoiRG9taW5pa2E
gQm9iaWsiLCJteXNwZWNpYWxjbGFpbSI6InNwZWNpYWx2YWx1ZSJ9.JGxvQgp
b0BEUzkSuD9oySwU68WqLQjslOPLVE9cA_T8

Header

```
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9
.
eyJpc3MiOiJkb21pbmlrYWJvYmlrLmNvbSIsImlhdCI
6MTczMDAwMzA2MCwiZXhwIjoxNzYxNTM5MDU5LCJhdW
QiOiJTRlNDT04iLCJzdWIiOiJkYm9iaWtAZXhhbXBsZ
S5jb20iLCJuYmYiOiIxNzYxNTM5MDU5IiwianRpIjoi
dW5pcXVlSUQiLCJuYW1lIjoiRG9taW5pa2EgQm9iaWs
iLCJteXNwZWNpYWxjbGFpbSI6InNwZWNpYWx2YWx1ZS
J9
.
JGxvQgpb0BEUzkSuD9oySwU68WqLQjslOPLVE9cA_T8
```

```
Base64Encode(
    {
        "alg": "RS256",
        "typ": "JWT",
        "kid": "NjVBRjY5MDlCMUIwNzU4RTA2QzZFMDQ4",
        "jku": "https://known.endpoint.com",
        "jwk": {"keys”: [{}]}
    }
)
```

Payload

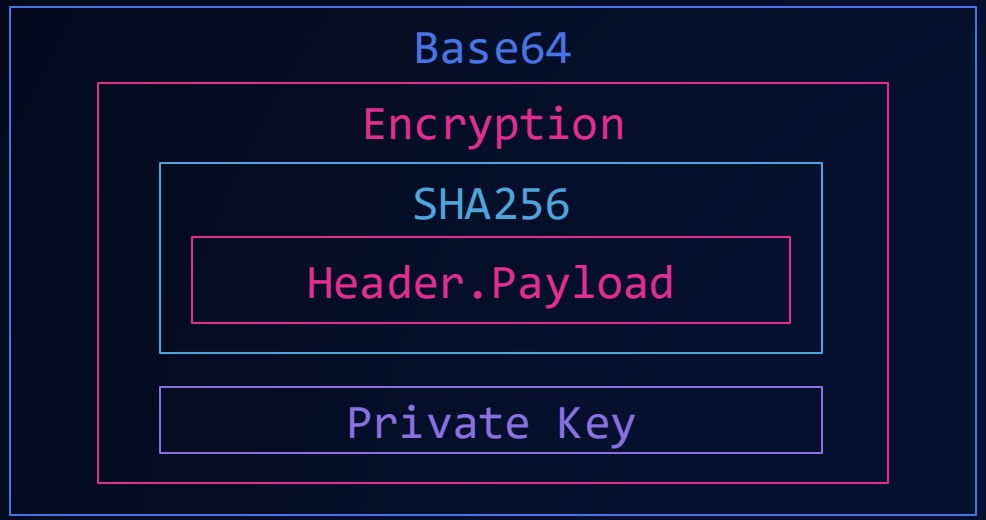
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9
.
eyJpc3MiOiJkb21pbmlrYWJvYmlrLmNvbSIsImlhdCI6MTczMDAwMzA2MCwiZXhwIjoxNzYxNTM5MDU5LCJhdWQiOiJTRlNDT04iLCJzdWIiOiJkYm9iaWtAZXhhbXBsZS5jb20iLCJuYmYiOiIxNzYxNTM5MDU5IiwianRpIjoidW5pcXVlSUQiLCJuYW1lIjoiRG9taW5pa2EgQm9iaWsiLCJteXNwZWNpYWxjbGFpbSI6InNwZWNpYWx2YWx1ZSJ9
.
JGxvQgpb0BEUzkSuD9oySwU68WqLQjslOPLVE9cA_T8

```
Base64Encode(
    {
        "iss": "dominikabobik.com",
        "iat": 1730003060,
        "exp": 1761539059,
        "aud": "SFSCON",
        "name": "Dominika Bobik",
        "myspecialclaim": "specialvalue"
    }
)
```

Signature

```
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9
.
eyJpc3MiOiJkb21pbmlrYWJvYmlrLmNvbSIsImlhdCI
6MTczMDAwMzA2MCwiZXhwIjoxNzYxNTM5MDU5LCJhdW
QiOiJTRlNDT04iLCJzdWIiOiJkYm9iaWtAZXhhbXBsZ
S5jb20iLCJuYmYiOiIxNzYxNTM5MDU5IiwianRpIjoi
dW5pcXVlSUQiLCJuYW1lIjoiRG9taW5pa2EgQm9iaWs
iLCJteXNwZWNpYWxjbGFpbSI6InNwZWNpYWx2YWx1ZS
J9
.
JGxvQgpb0BEUzkSuD9oySwU68WqLQjslOPLVE9cA_T8
```

```
Base64Encode(
    Encrypt(
        SHA256(
            base64UrlEncode(header)
            + "." +
            base64UrlEncode(payload)
        ) , key
    )
)
```

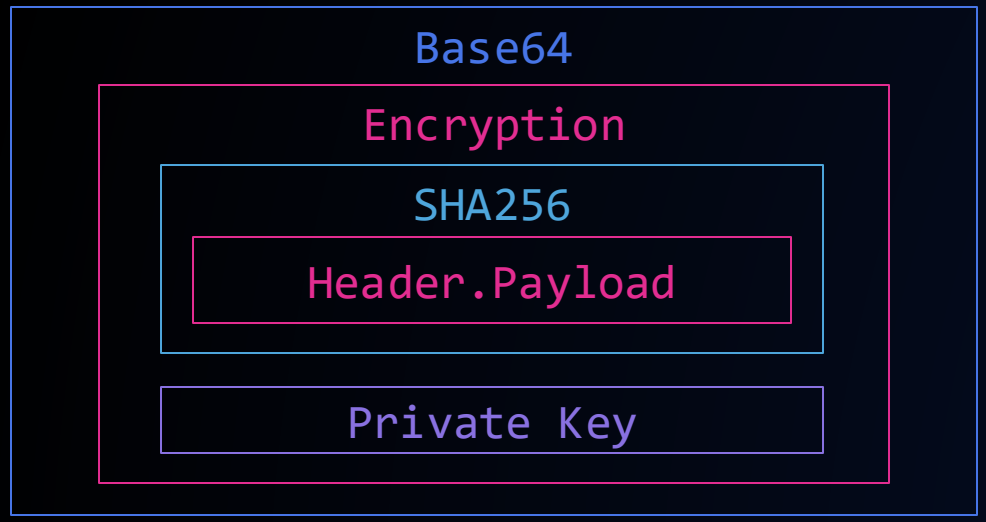


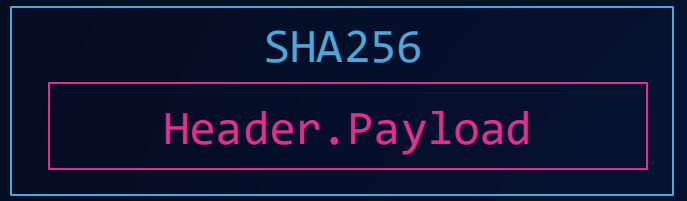
```
token =
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJpc3MiOiJkb21pbmlrYWJvYmlrLmNvbSIsImlhdCI6MTczMDAwMzA2MCwiZXhwIjo
xNzYxNTM5MDU5LCJhdWQiOiJTRlNDT04iLCJzdWIiOiJkYm9iaWtAZXhhbXBsZS5jb20iLCJuYmYiOiIxNzYxNTM5MDU5IiwianRpIjo
idW5pcXVlSUQiLCJuYW1lIjoiRG9taW5pa2EgQm9iaWsiLCJteXNwZWNpYWxjbGFpbSI6InNwZWNpYWx2YWx1ZSJ9.JGxvQgpb0BEUzk
SuD9oySwU68WqLQjslOPLVE9cA_T8

(header, payload, signature) = token.split(“.”)
decoded_header = decode64(header)
decoded_payload = decode64(payload)
decoded_signature= decode64(signature)

algorithm = decoded_header.alg
if (algorithm != expected_algorithm) exit(“Token is invalid”)
```

```
// 1 - Verify the signature
publicKey = getPublicKey()
decrypted_signature = decrypt(decoded_signature, public_key)
computed_signature = algorithm_function(header + “.” + payload)
if (decrypted_signature != computed_signature) exit(“Token is invalid”)
```





```
// 2 – Verify claims
if(decoded_payload.iss != trustedIssuer) exit(“Token is invalid”)
if(decoded_payload.sub != subject) exit(“Token is invalid”)
if(decoded_payload.aud != “SFSCON”) exit(“Token is invalid”)
if(decoded_payload.exp < Date.now()) exit(“Token is invalid”)
if(decoded_payload.name != “Dominika Bobik”) exit(“Token is invalid”)
if(decoded_payload.myspecialclaim != specialValue) exit(“Token is invalid”)
else exit(“Token is valid!”)
```

Thank you!

 linkedin.com/in/dominika-bobik

 github.com/dominikabobik

 dominikabobik.com