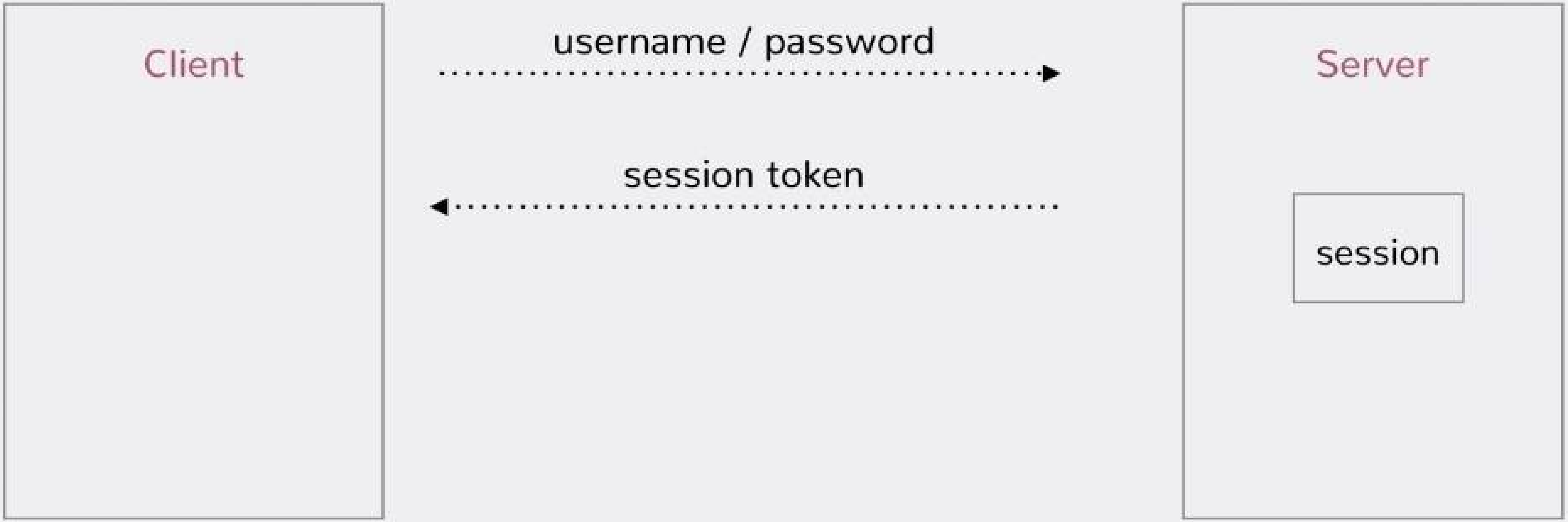
Classic session-based authentication



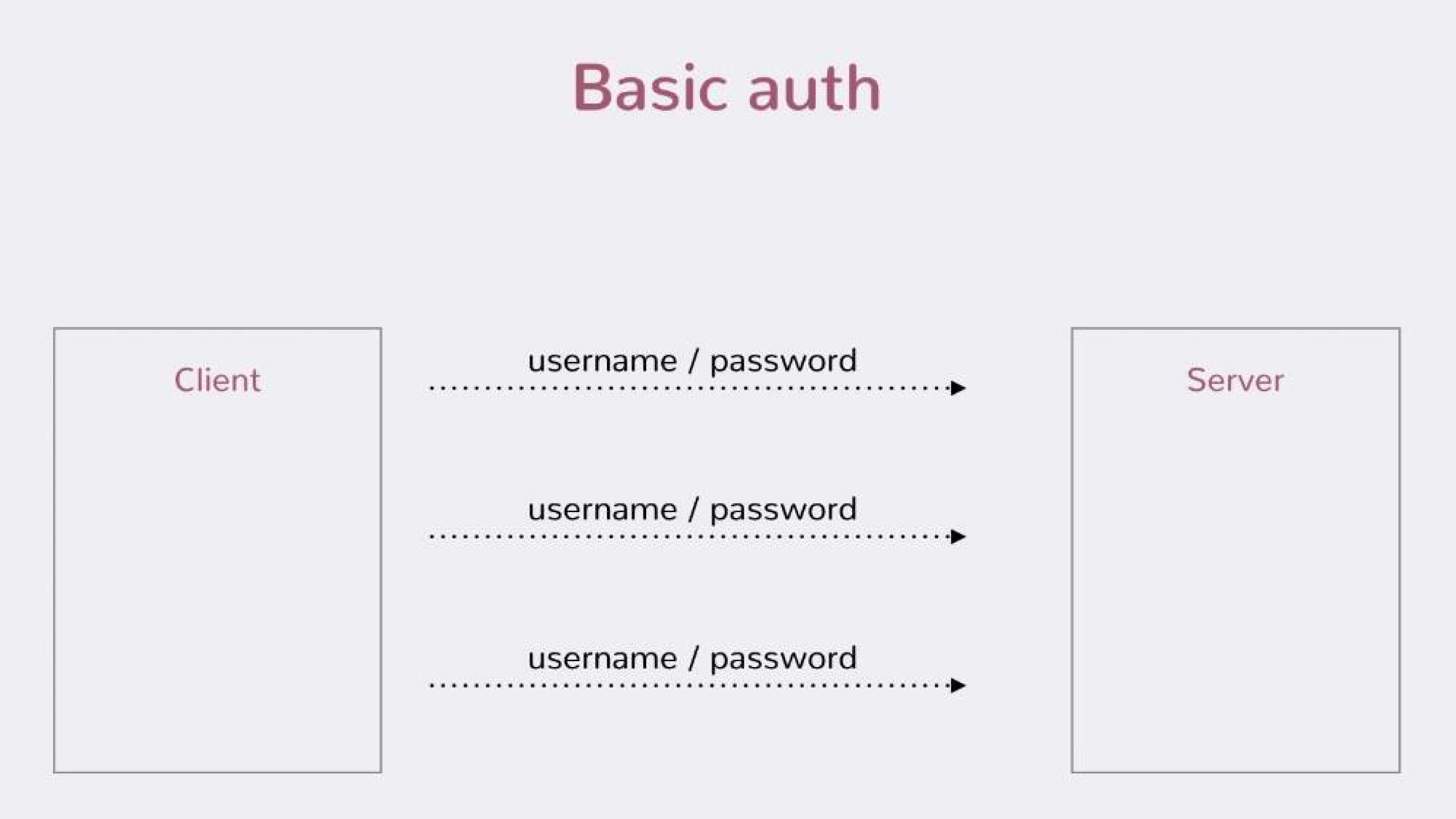
Client

username / password

session token

Server

session



Basic auth

Client

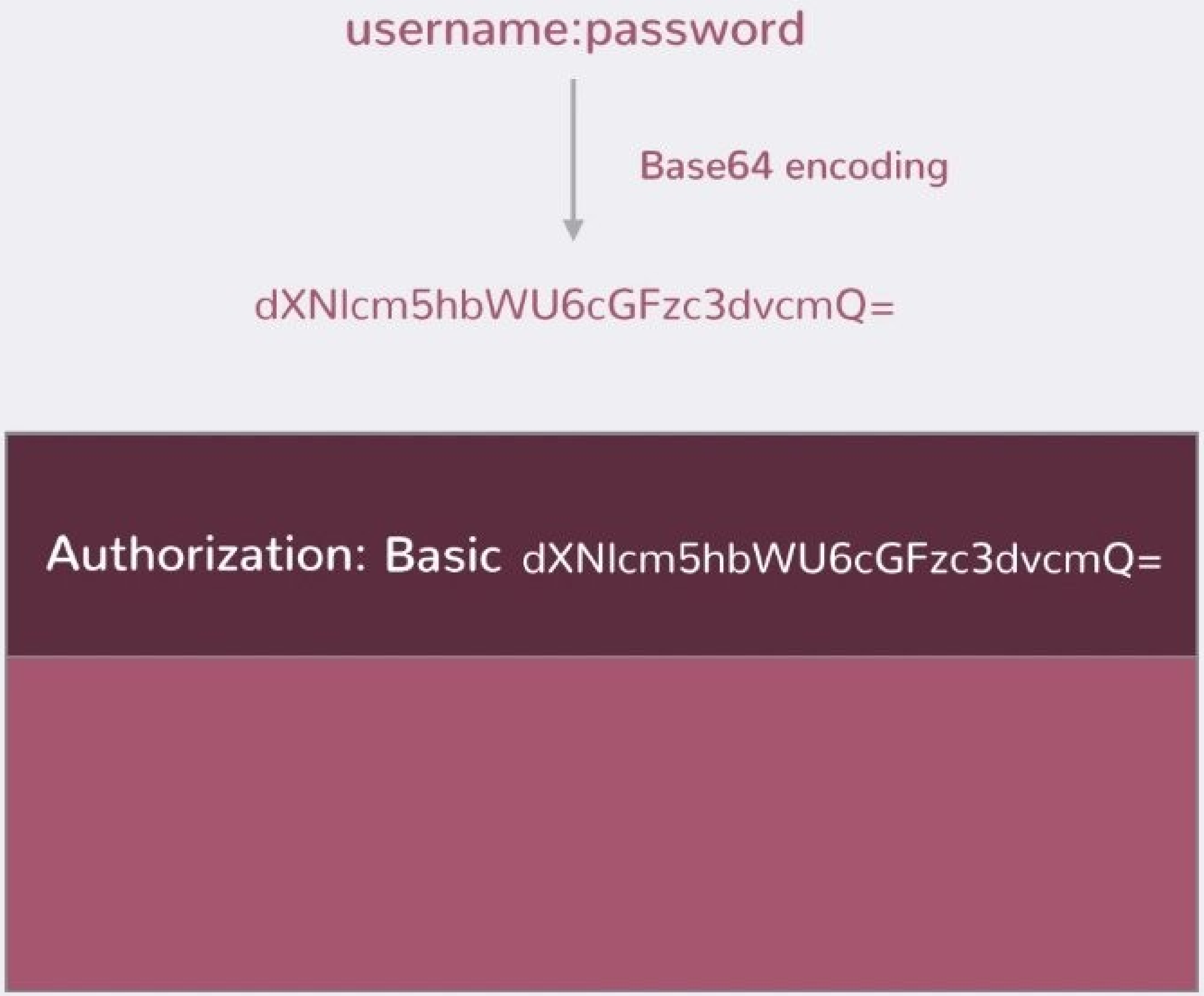
username / password

username / password

username / password

Server

Basic auth - client side



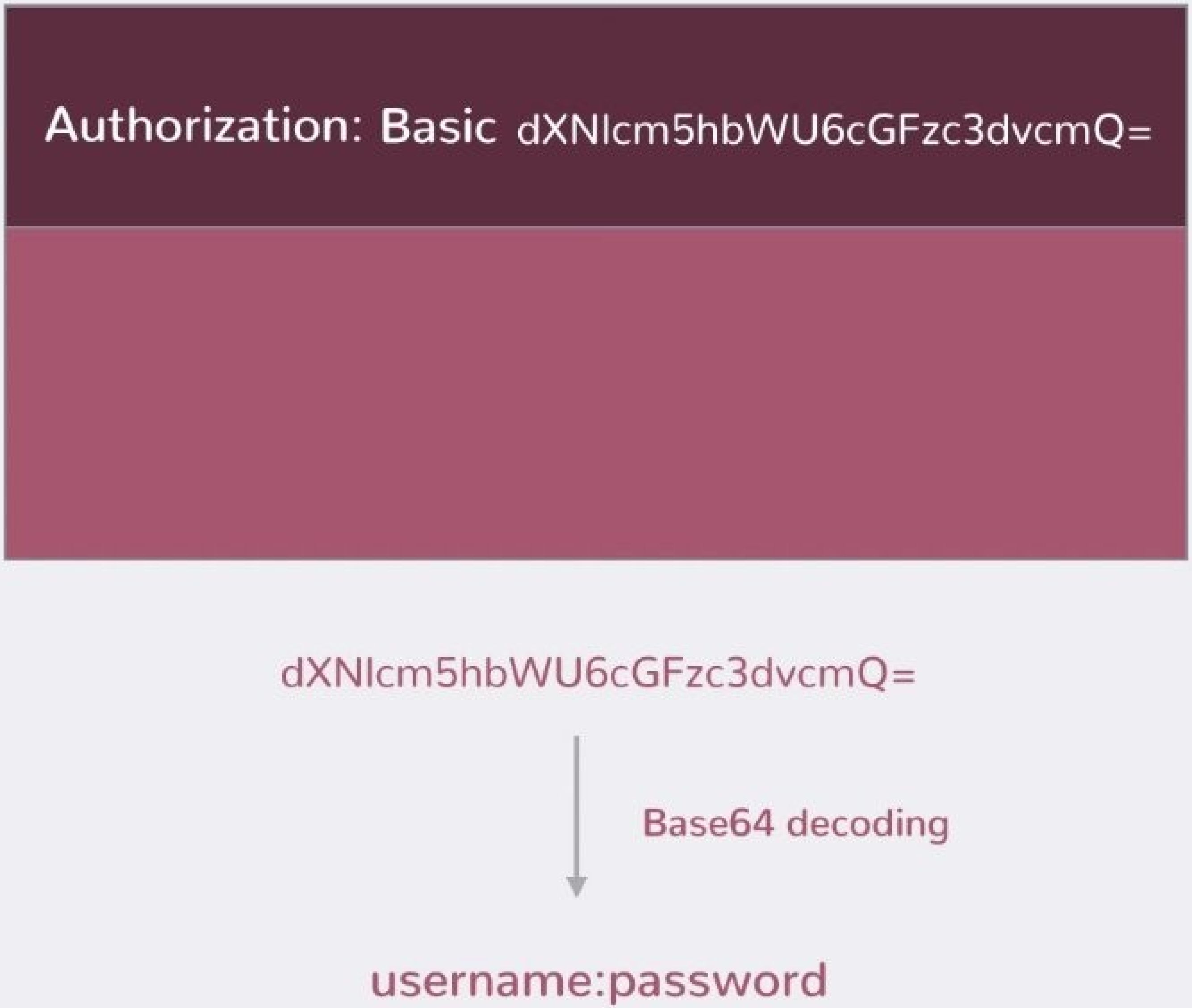
username:password

Base64 encoding

dXNlcm5hbWU6cGFzc3dvcmQ=

Authorization: Basic dXNlcm5hbWU6cGFzc3dvcmQ=

Basic auth - server side



Authorization: Basic dXNlcm5hbWU6cGFzc3dvcmQ=

dXNlcm5hbWU6cGFzc3dvcmQ=

Base64 decoding

username:password

Base64 Encoding

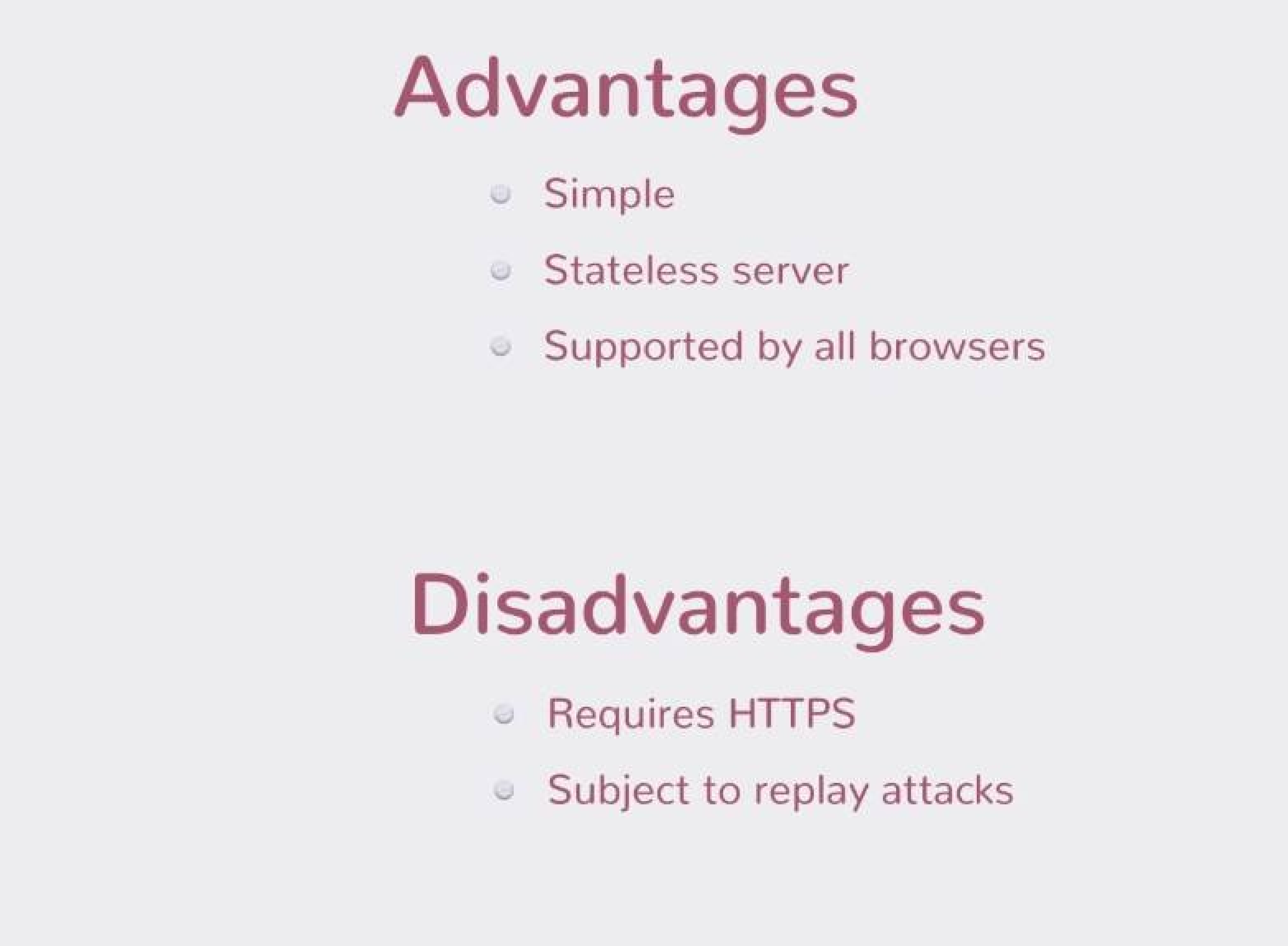
dXNlcm5hbWU6cGFzc3dvcmQ=

This is **not** secure!

Always over HTTPS

Security is not the intent of the encoding step. Rather, the intent of the encoding is **to encode non-HTTP-compatible characters** that may be in the user name or password into those that are HTTP-compatible.

https://en.wikipedia.org/w/index.php?title=Basic_access_authentication&oldid=339510542



Advantages

- Simple
- Stateless server
- Supported by all browsers

Disadvantages

- Requires HTTPS
- Subject to replay attacks

Better Solutions

- Digest access authentication

(https://en.wikipedia.org/wiki/Digest_access_authentication)

- Asymmetric cryptography

(https://en.wikipedia.org/wiki/Public-key_cryptography)

- OAuth

(https://en.wikipedia.org/wiki/OAuth)

- JSON Web Tokens