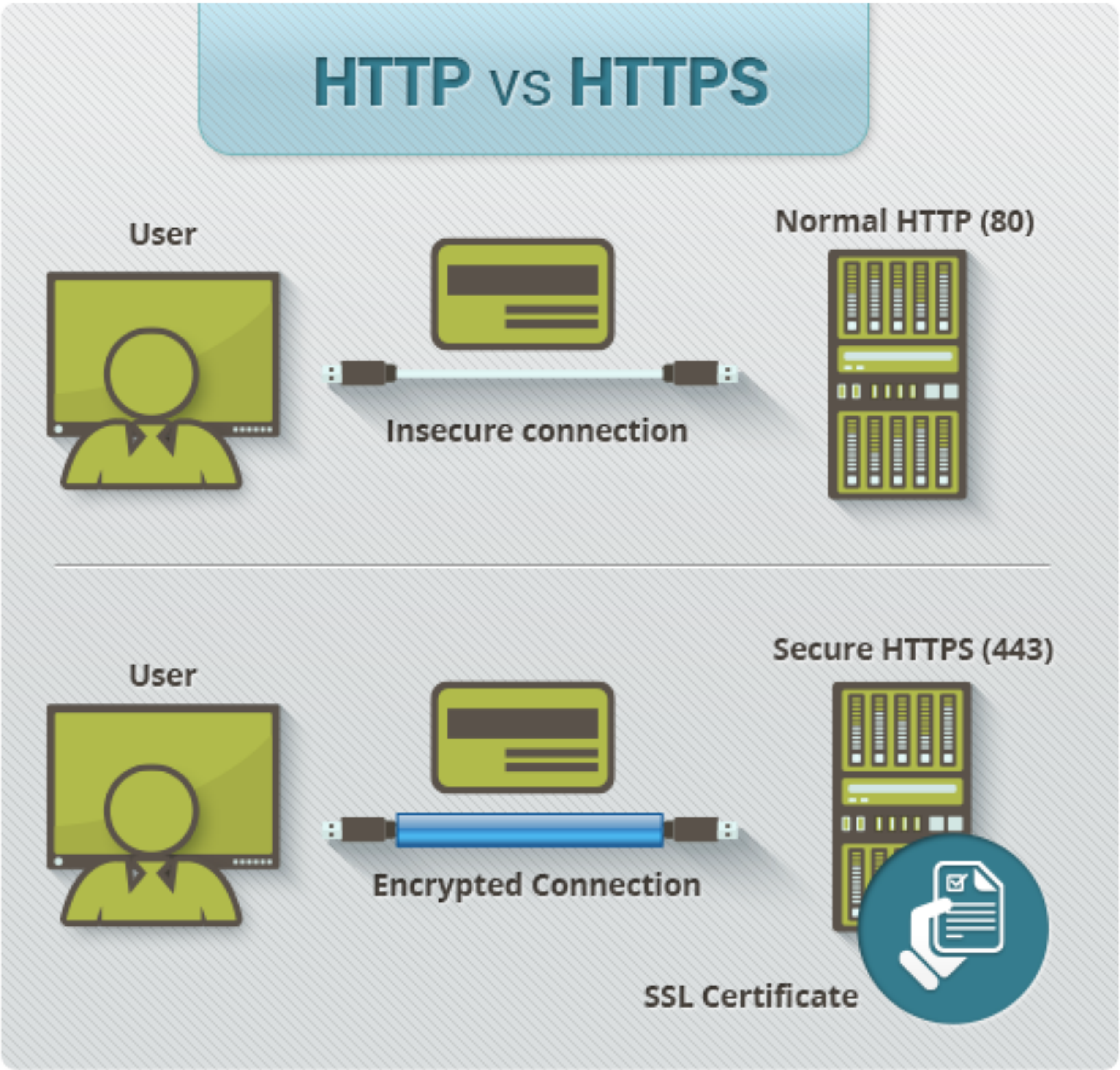
HTTPS

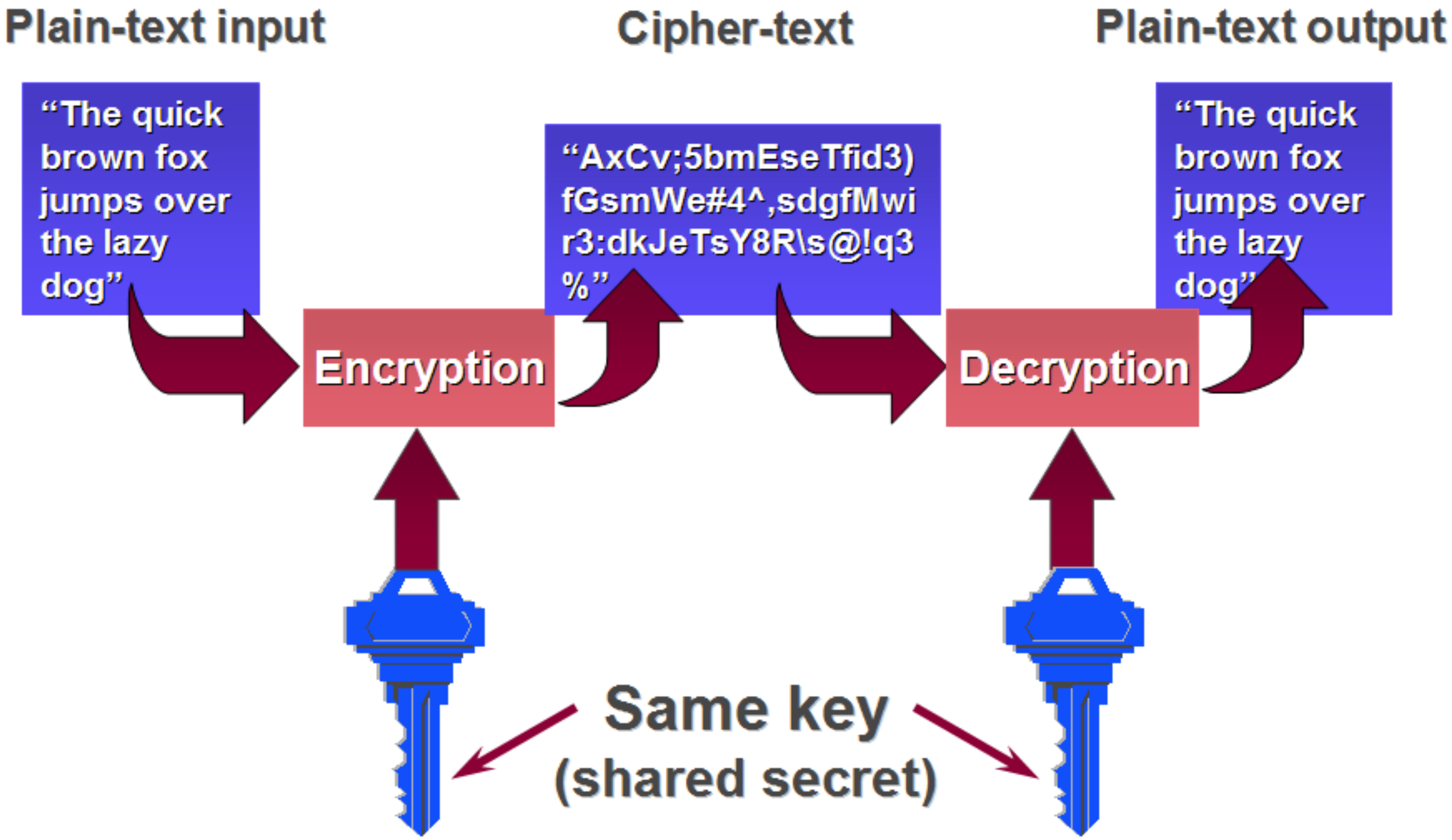
(the s stands for secure)

We do not want people reading our messages



How does it work?

Symmetric encryption



Plain-text input

Cipher-text

Plain-text output

“The quick brown fox jumps over the lazy dog”

“AxCv;5bmEseTfid3)fGsmWe#4^,sdgfMwir3:dkJeTsY8R\s@!q3%”

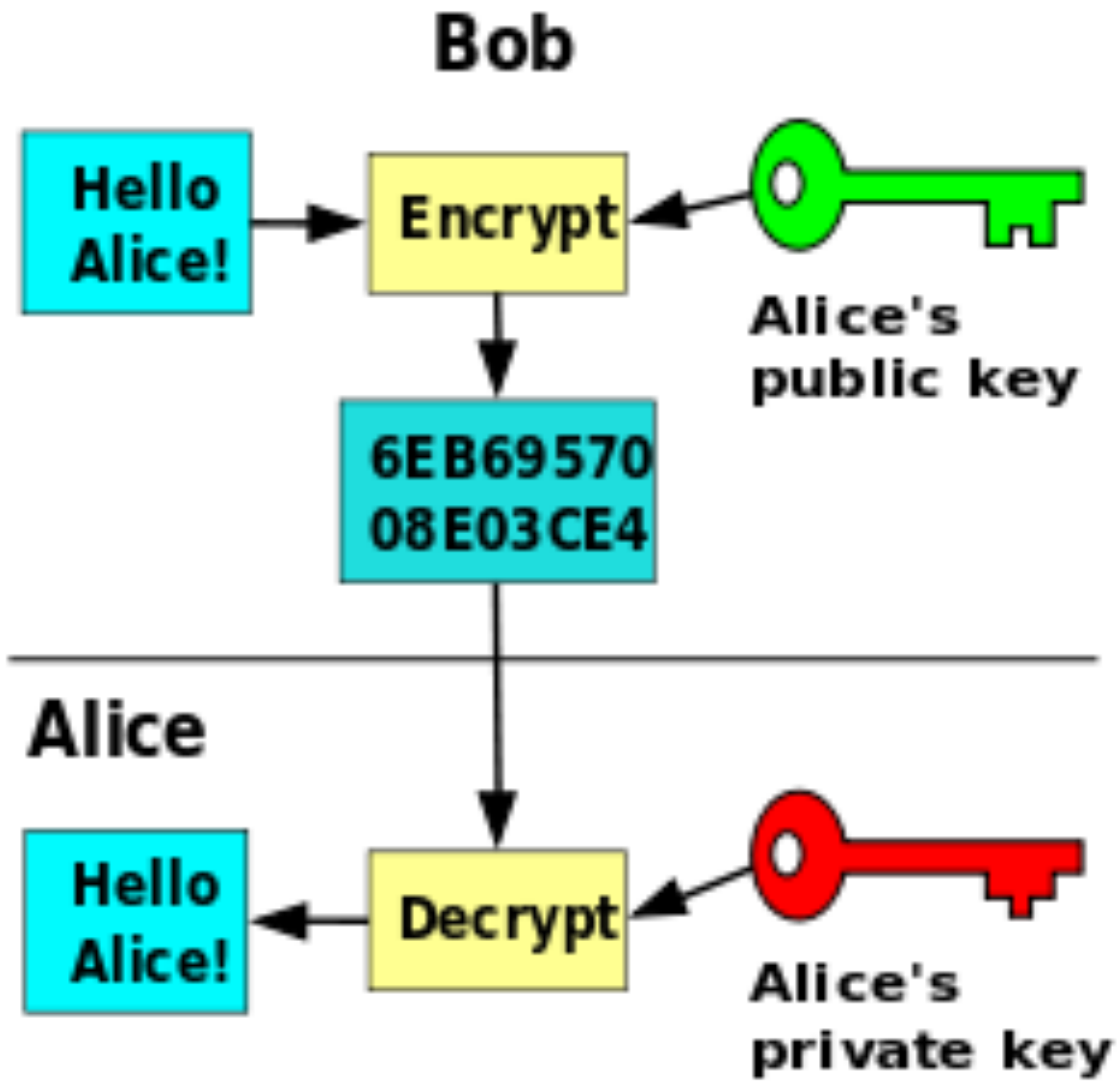
“The quick brown fox jumps over the lazy dog”

Encryption

Decryption

Same key
(shared secret)

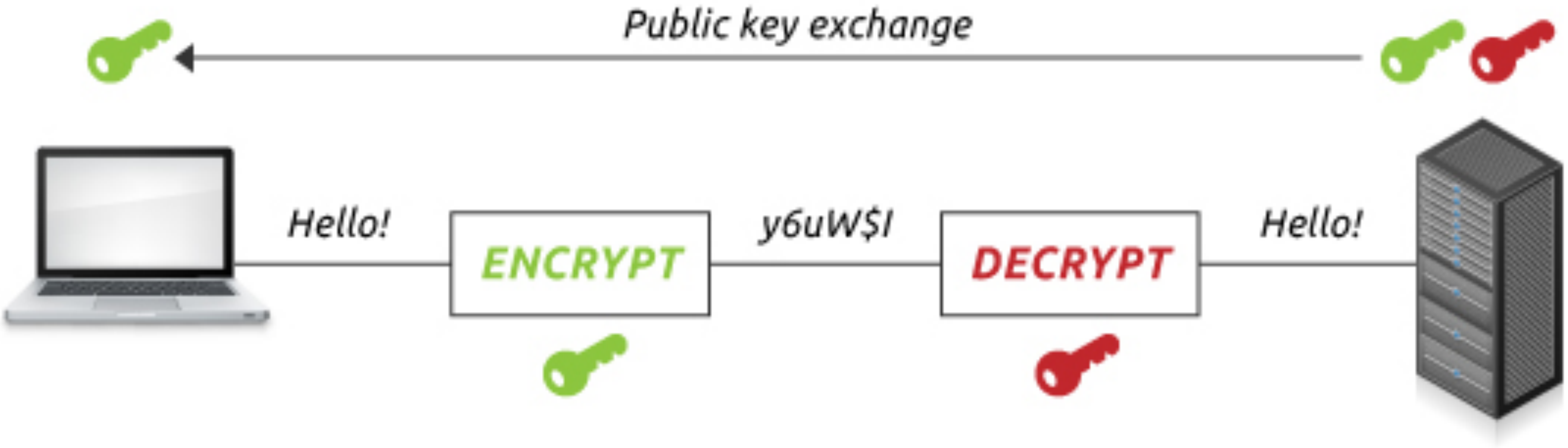
Asymmetric encryption



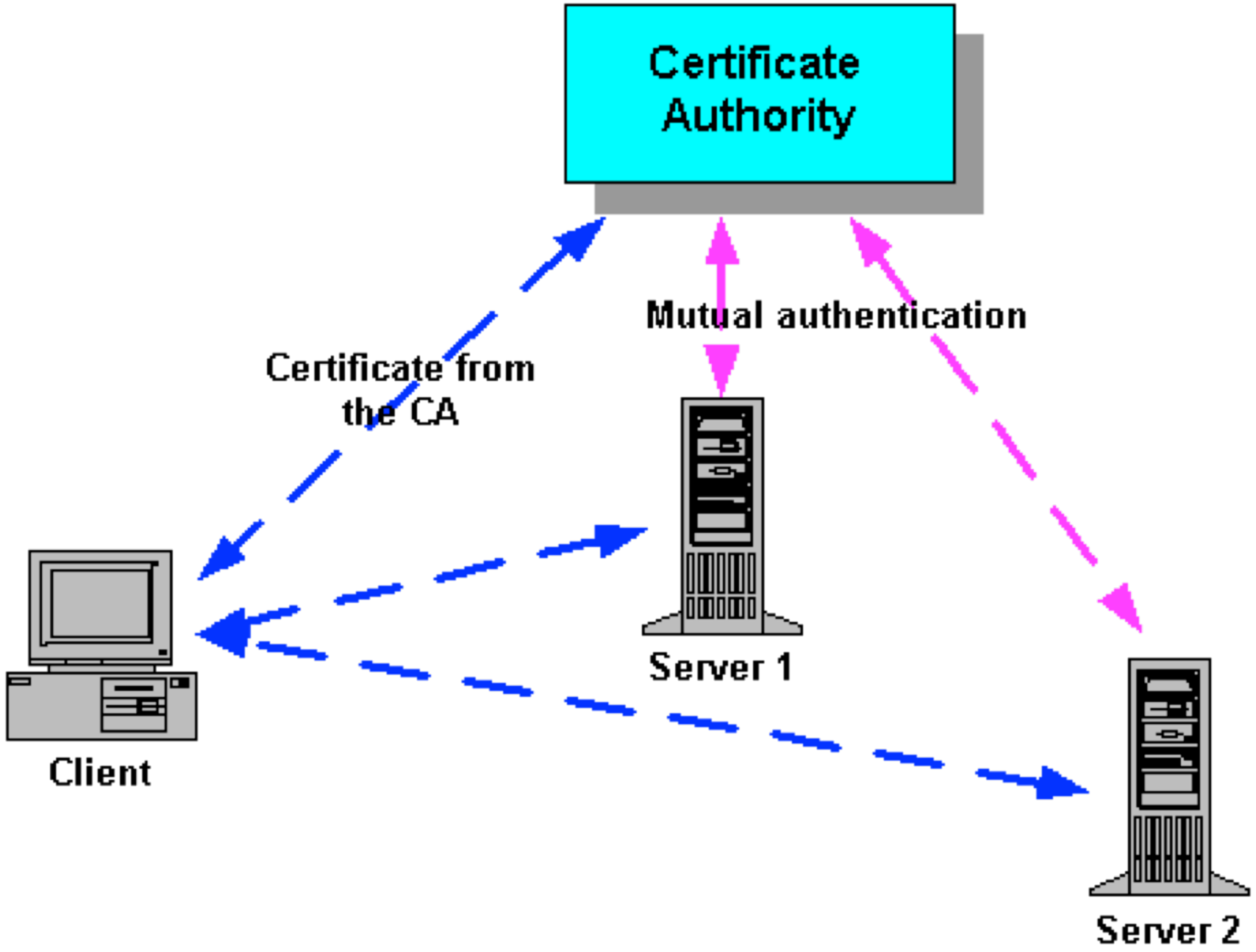
SSL handshake

Asymmetric encryption to create session

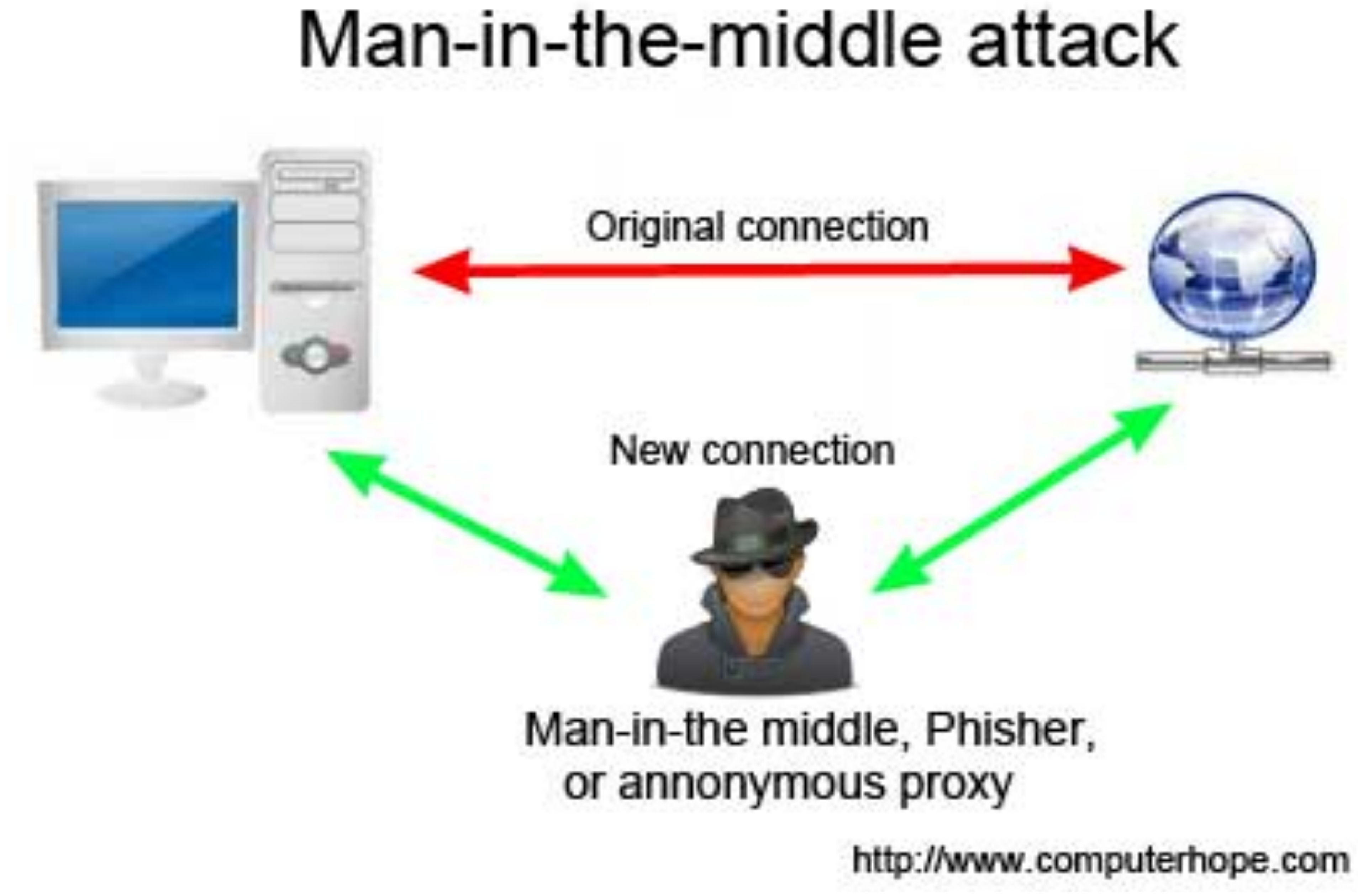
Symmetric encryption to transfer messages (faster)



Certificate Verification

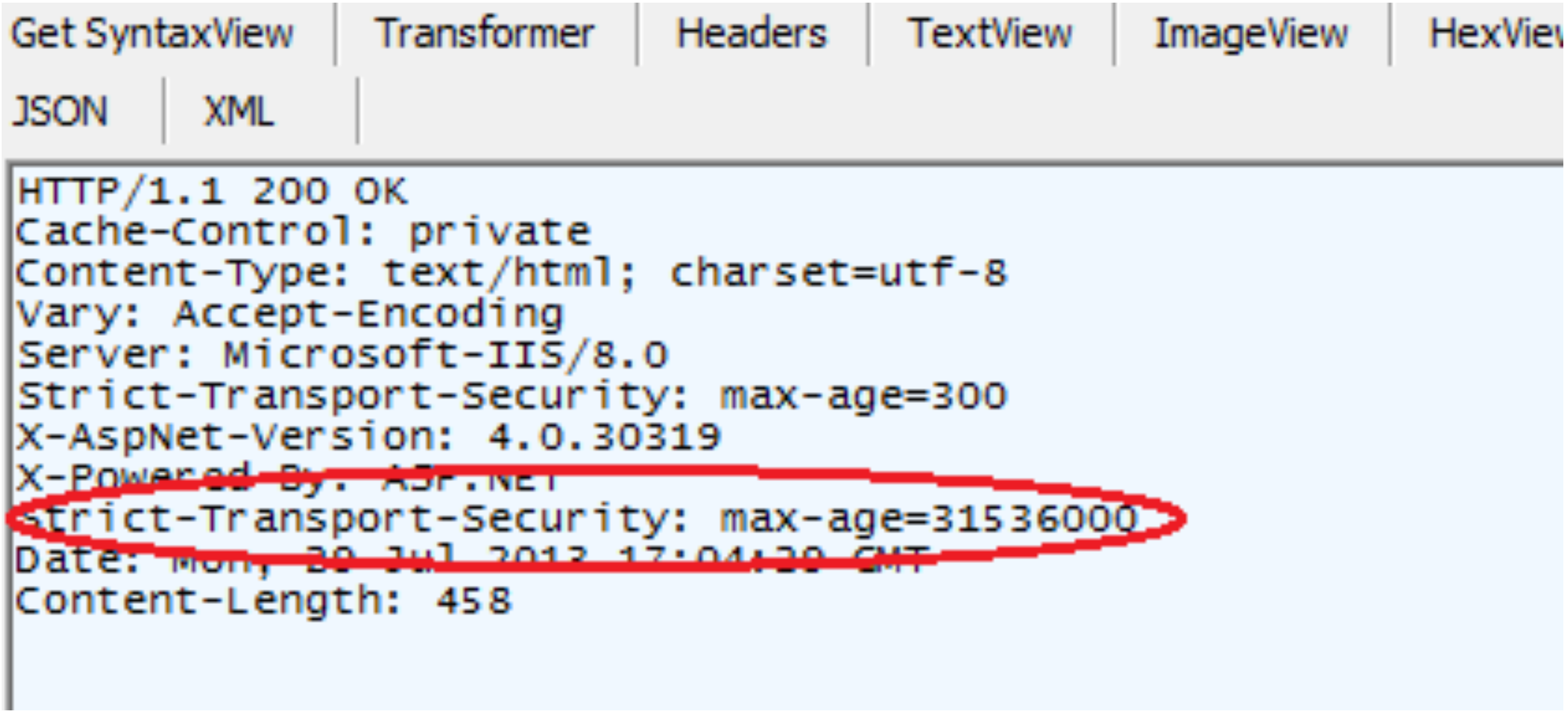


HTTPS reduces Man in the Middle Attacks



HTTP Strict Transport Security

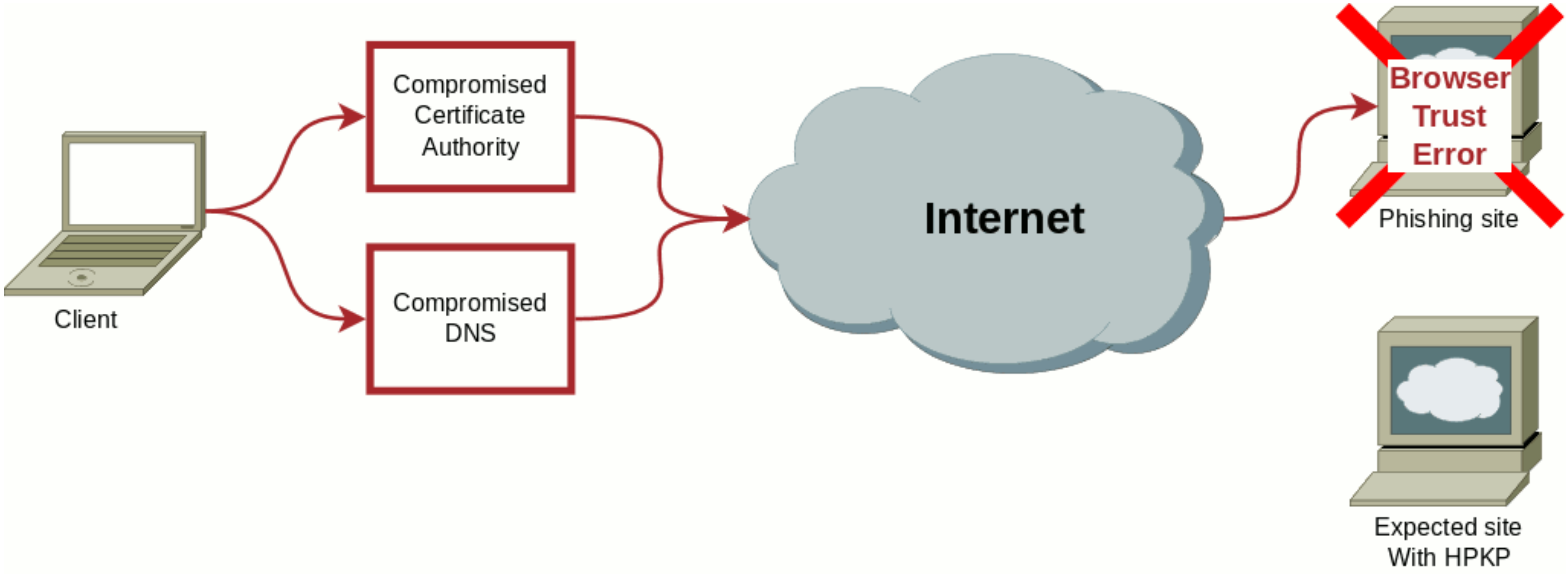
Requires browsers to use HTTPS with site



```
HTTP/1.1 200 OK
Cache-Control: private
Content-Type: text/html; charset=utf-8
Vary: Accept-Encoding
Server: Microsoft-IIS/8.0
Strict-Transport-Security: max-age=300
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Strict-Transport-Security: max-age=31536000
Date: Mon, 29 Jul 2013 17:04:29 GMT
Content-Length: 458
```

HTTP Public Key Pinning

Binds certificate to site


Compromised Certificate Authority
Compromised DNS
Client
Internet
Browser Trust Error
Phishing site
Expected site With HPKP