Streng geheim!

Verschlüsselung im Alltag

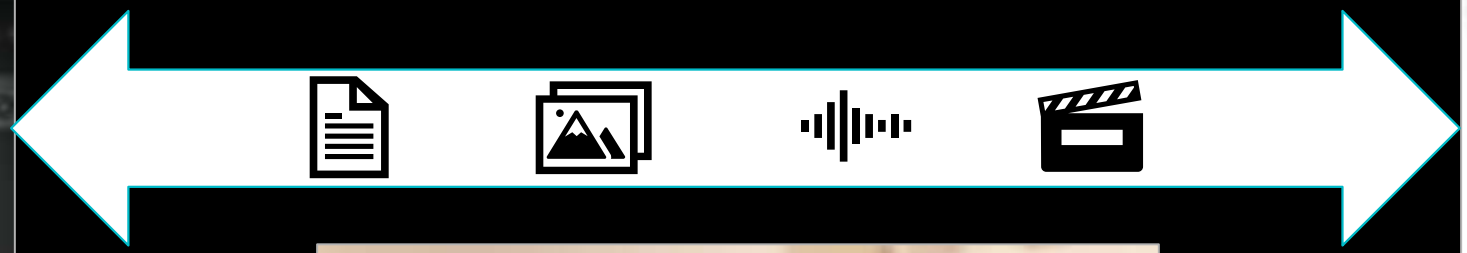
@stephanius@chaos.social

@w1ntermute@23.social

CRYPTO PARTY

Quelle Fotos: flickr.com

Streng geheime Kommunikation



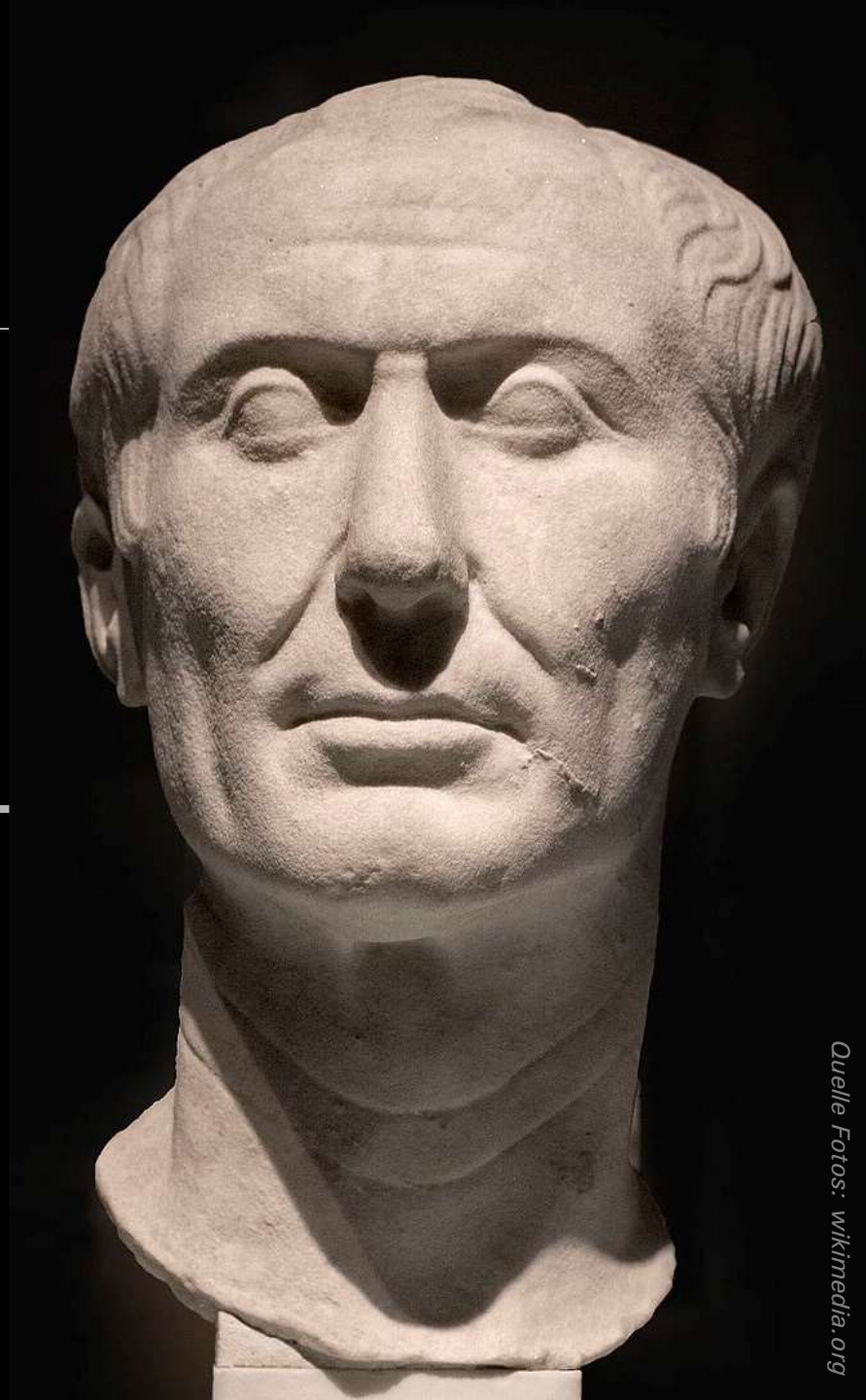
Quelle Fotos: unsplash.com

Caesar Chiffre

```
ABCDEFGHIJKLMNOPQR...
|   |   |   |
ABCDEFGHIJKLMNOPQ...
```

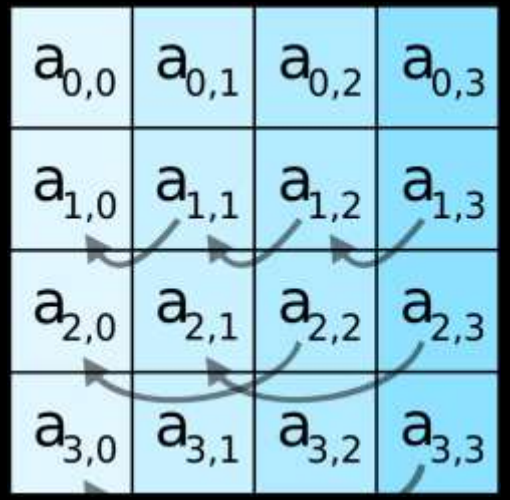

```
HALLO WELT    >>    MFQQT BJQY

HELLO WELT    >>    MJQQT BJQY
```



Quelle Fotos: wikimedia.org

Rijndael (AES)



21blaue_wale_AES

128 Bit

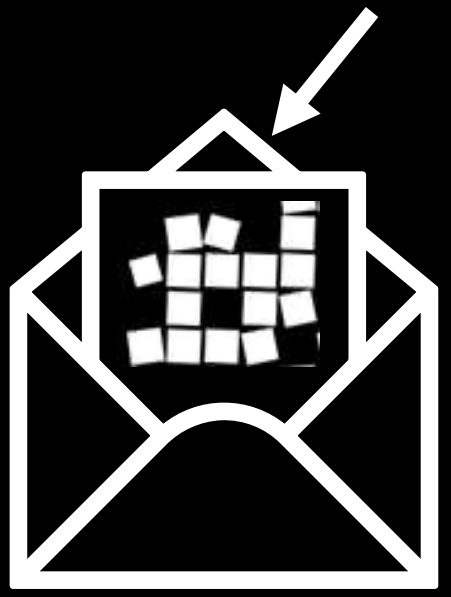
Quelle Foto: krypterix.com

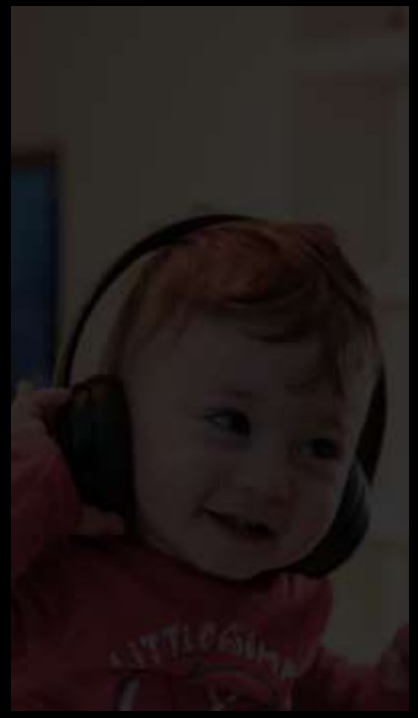
```
HALLO WELT      >>    kz0eo0Zia+Thegxe2ieRdA==

HELLO WELT      >>    iYRPVHoJXwT+OFWpnGs+cw==

HELLO           >>    G+nD+qhIjh63uI2ovqtkgA==
```

Schlüsseltausch (RSA)



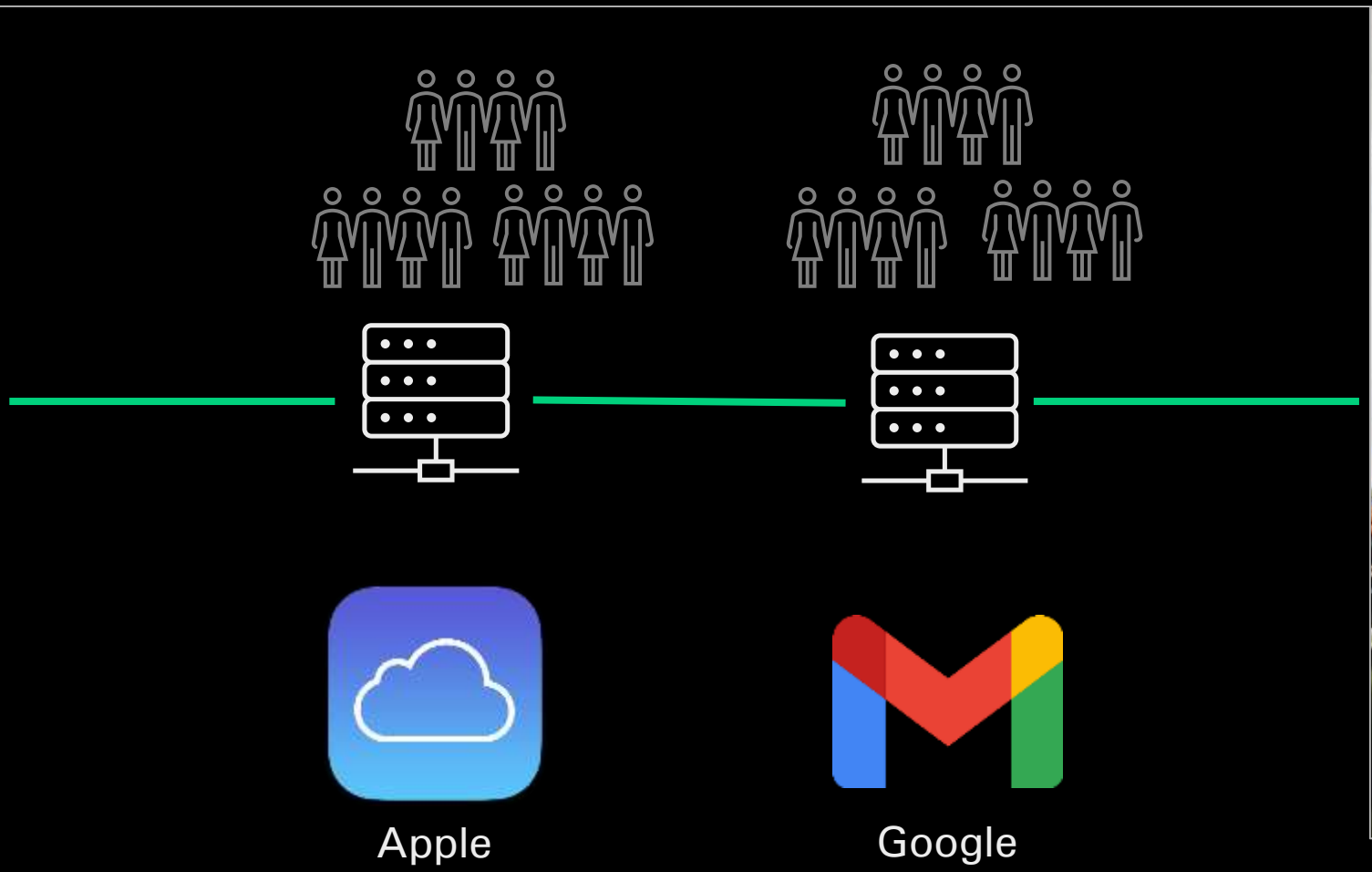


public

private

Quelle Fotos: unsplash.com

Email Verschlüsselung



Quelle Fotos: unsplash.com

Echtheit der Schlüssel (Zertifikate)

public

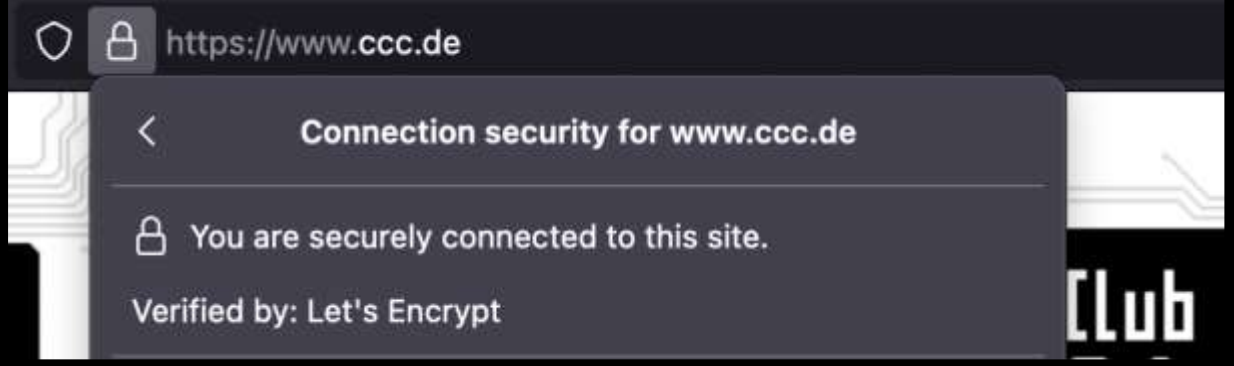
private

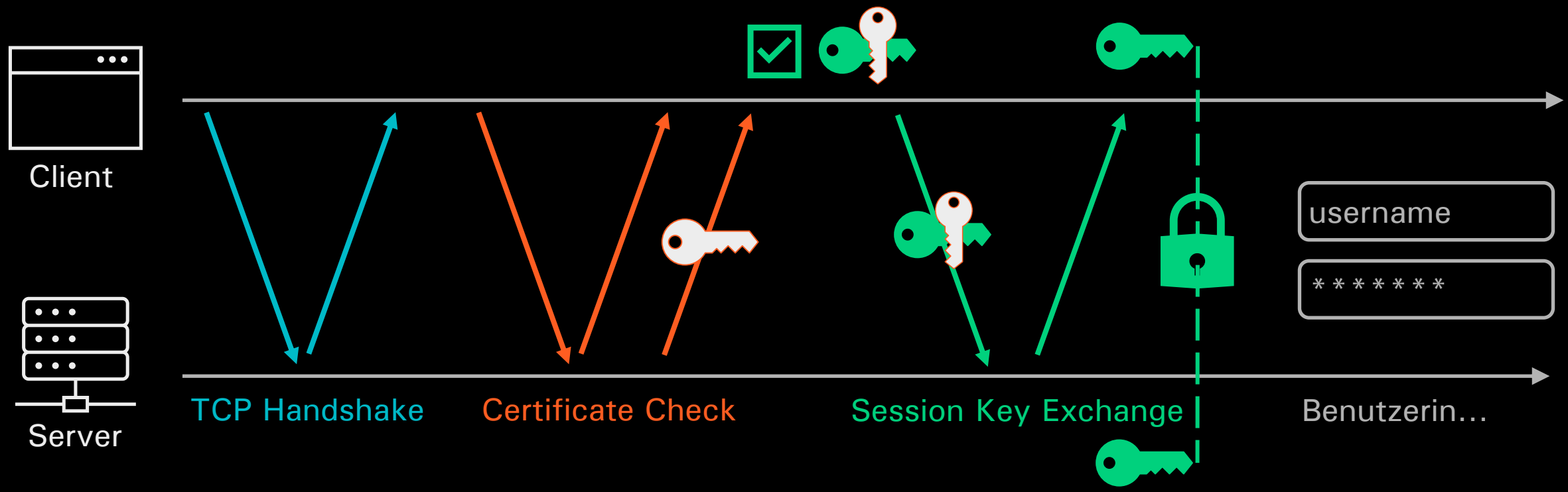
alice@icloud.com

bob@gmail.com

Quelle Fotos: unsplash.com

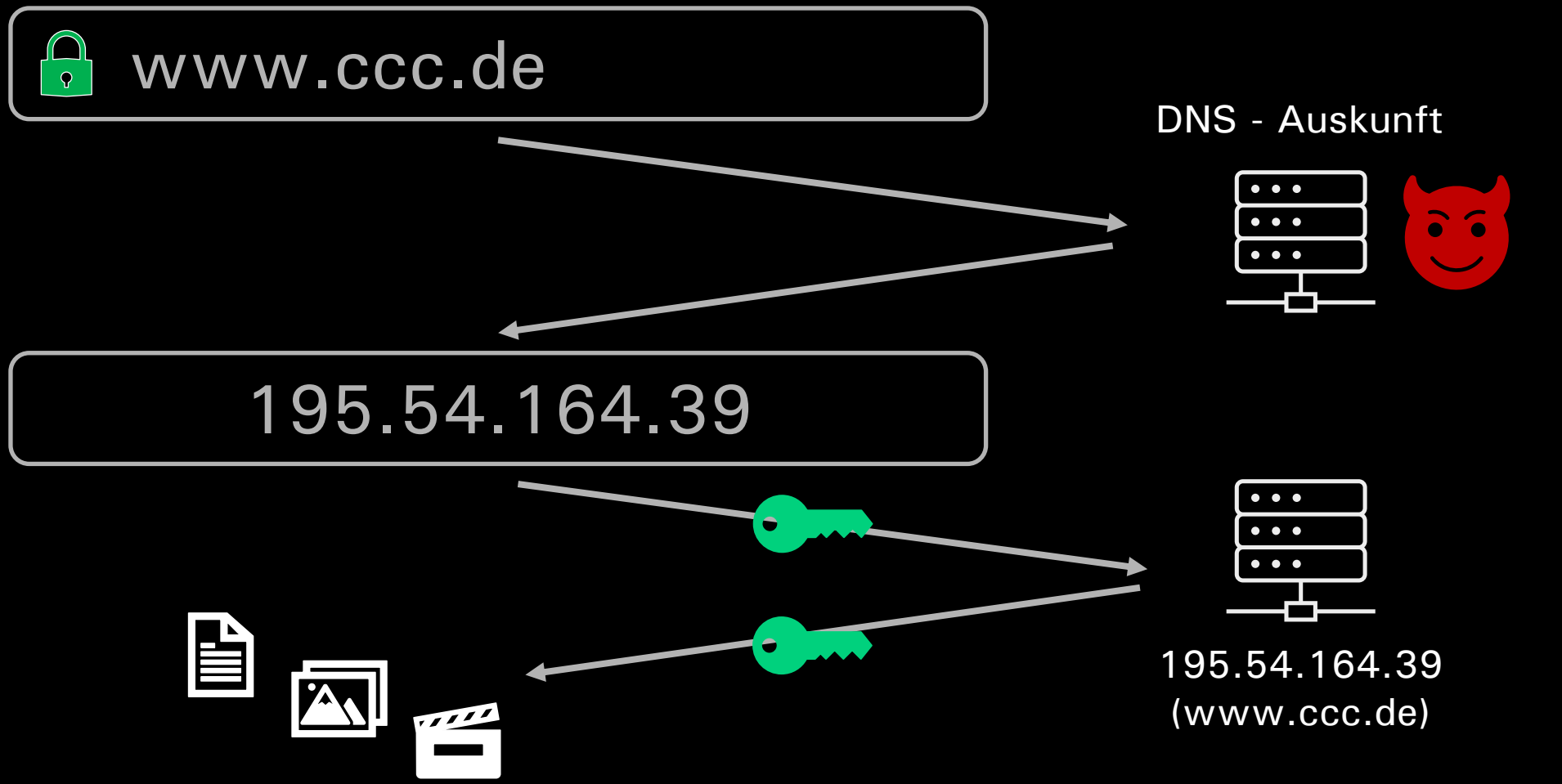
HTTPS


https://www.ccc.de
Connection security for www.ccc.de
You are securely connected to this site.
Verified by: Let's Encrypt


Client
Server
TCP Handshake
Certificate Check
Session Key Exchange
username
* * * * * * *
Benutzerin…

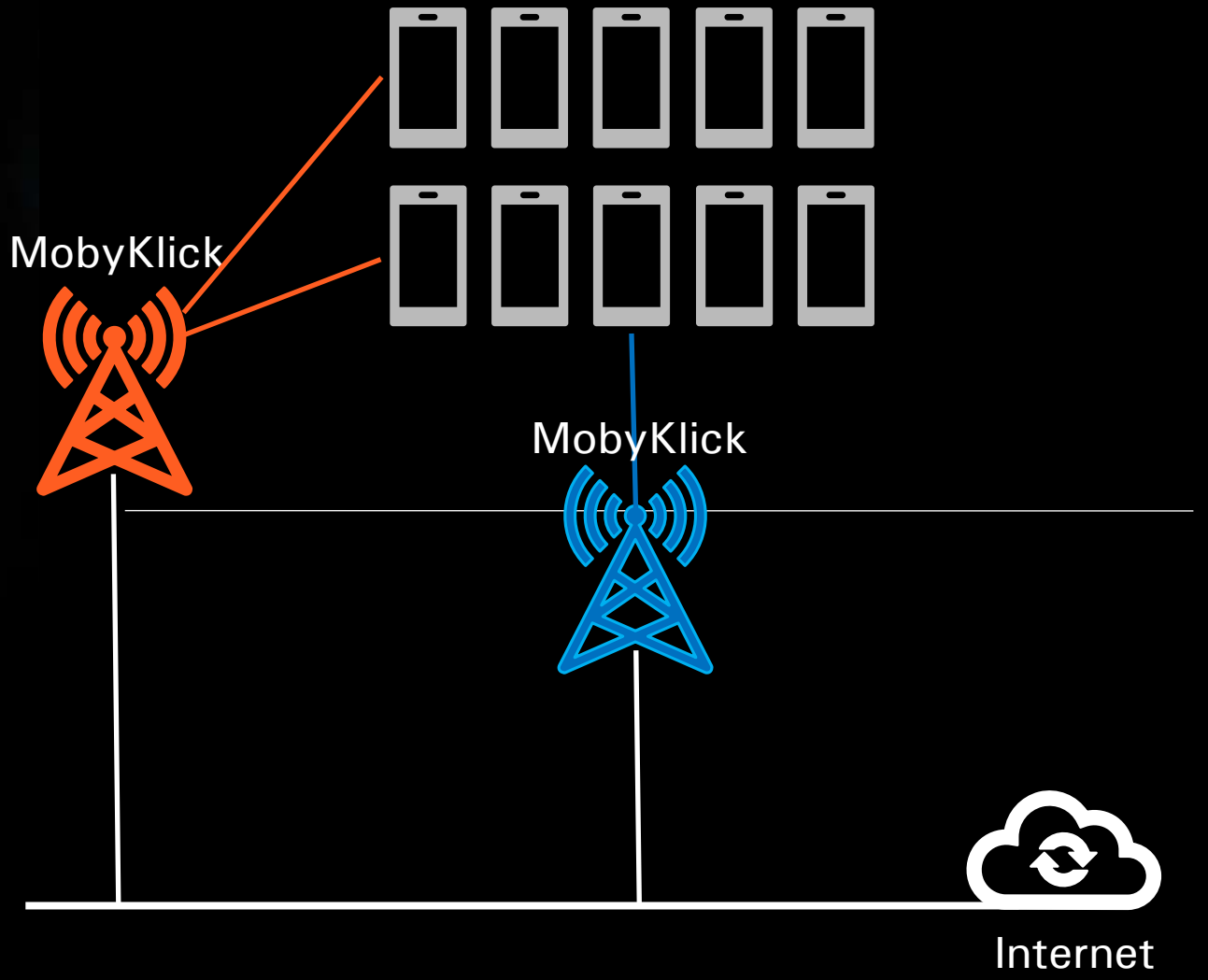

DE
BUNDESREPUBLIK DEUTSCHLAND
FEDERAL REPUBLIC OF GERMANY / REPUBLIQUE FEDERALE D'ALLEMAGNE
PERSONALAUSWEIS
IDENTITY CARD / CARTE D'IDENTITE
L01XJJRH8
[a] Name/Surname/Nom
[b] Geburtsname/Name at birth/Nom de naissance
[a]MUSTERMANN
[b]GABLER
Vornamen/Given names/Prénoms
ERIKA
Geburtstag/Date of birth/ Date de naissance
12.08.1983
Staatsangehörigkeit/Nationality/ Nationalité
DEUTSCH
Geburtsort/Place of birth/Lieu de naissance
BERLIN
Gültig bis/Date of expiry/ Date d'expiration
01.08.2031
045253
MUSTER

Internet Telefonbuch (DNS)



Quelle Fotos: unsplash.com

Man-in-the-middle



Links, Folien, Tipps & Tricks

@stephanius@chaos.social

@w1ntermute@23.social