EU Digital COVID Certificate

Keine schwarze Magie



Your proposals

Title	State
Von Null auf root in 120 Minuten - Einführung ins Website Hacking	confirmed
Besser leben mit SSH	confirmed
Moderne Linux Kommandozeilenwerkzeuge - Edition "Allein zu Haus"	confirmed
"EU Digital COVID Certificate" - Keine schwarze Magie	confirmed
Die unterhaltsamsten österreichischen IT Fails der letzen Jahre und was wir daraus lernen können	confirmed

Helft mir !!!

- Reicht Talks und Workshops ein
- Ich helfe gerne
  - Themenfindung
  - CfP Formulierung
  - Präsentation bauen
  - Präsentation Testlauf
- haecksen.org et.al. helfen

#gpn20

@LEYRER [@chaos.social]
https://martin.leyrer.priv.at



EU Digital COVID Certificate

Keine schwarze Magie



Ich mag das “EU Digital COVID Certificate” (EU DCC)

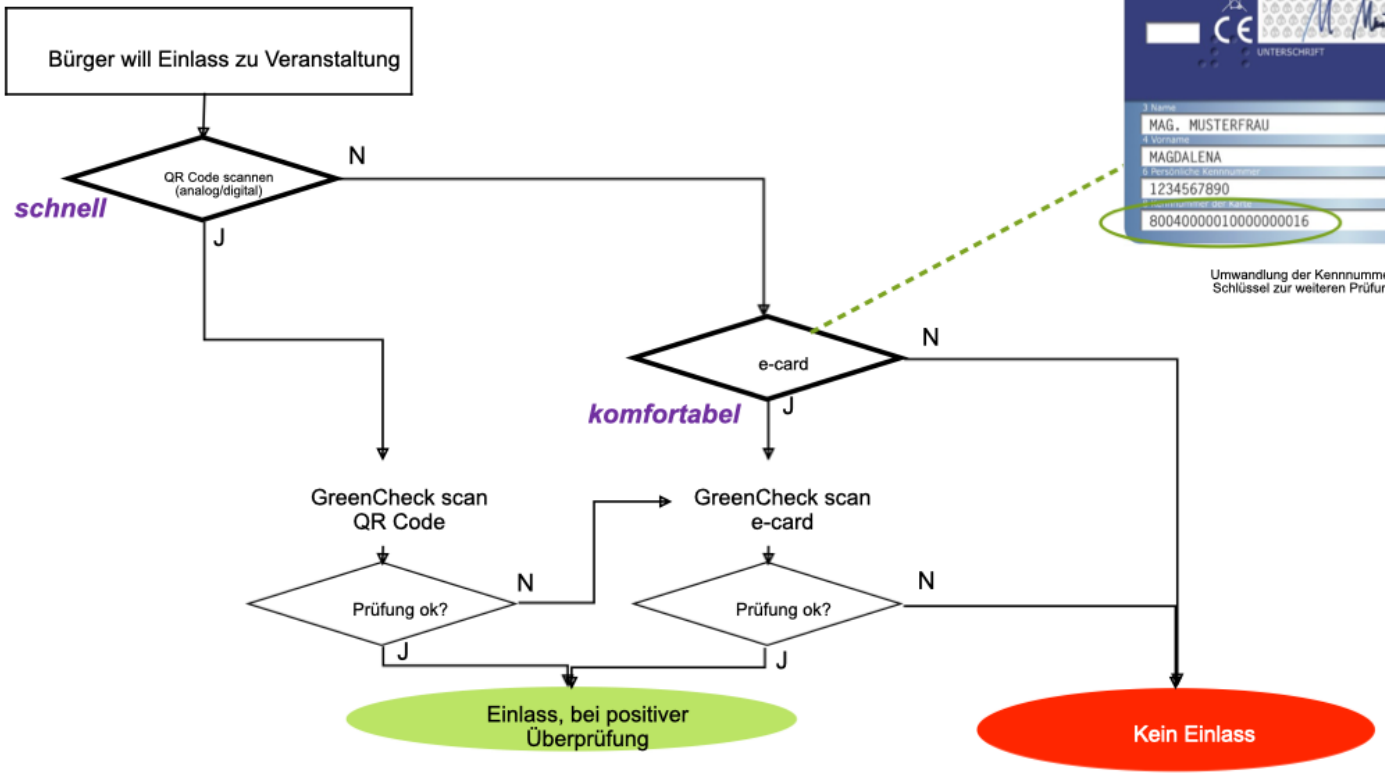
https://futurezone.at/netzpolitik/ecard-ist-sicherheitsluecke-beim-gruenen-pass/401374445


ecard
Kartenfolgenummer
004
1234 567890
Mag.
Magdalena
Musterfrau
e-card Serviceline 050124 33 11
Wenn's weh tut! 1450


EUROPÄISCHE KRANKENVERSICHERUNGSKARTE
UNTERSCHRIFT
AUSTRIACARD
AT
3 Name
MAG. MUSTERFRAU
4 Vorname
MAGDALENA
5 Geburtsdatum
01/01/1970
6 Persönliche Kennnummer
1234567890
7 Kennnummer des Trägers
1100 - OEGK
8 Kennnummer der Karte
80040000010000000016
9 Ablaufdatum
31/12/2025

ANWENDUNGSABLAUF GREENCHECK

ITSV GmbH





Umwandlung der Kennnummer in einen eGovernment konformen Schlüssel zur weiteren Prüfung. Diese Umwandlung ist nur durch sie SV möglich.

Kopfrechnen

- 10 Stellen mit Wiederholung
- Littledata, May 2022: 416 ms average server response time



Datenhandel

- “Sogar mit reinem Durchprobieren hätte man den Namen, das Geburtsdatum und den Status des Covid-Nachweises aller Sozialversicherten bei einer niedrigen Geschwindigkeit und wenigen IP-Adressen in unter einem Monat kopiert.“ – epicenter.works



Zertifikatsimport

- "Grüner Pass" App
  - Kartennummer
  - Postleitzahl
- Profit!



UNTERSCHIEDLICHE ANWENDUNGEN

ITSV GmbH

	Smartphone mit Prüfer WebApp	Smartphone mit Bürger APP
	Green Check	impf → Grüner Pass (Der „Grüne Pass" ist die erste Funktion des elektronischen Impfpasses.)
Verwendet von	Prüferinnen bei zB. Gastro, Friseur, Kulturveranstalter, etc. …	Bürgerinnen zum vorweisen des QR Code
Input	QR Codes aus Teststraßen, Alles Gurgelt und e-Impfpass, Rückseite der e-card	Identifikation der Bürgerinnen (Handysignatur, E-ID / ID Austria), Rückseite der e-card plus PIN (PLZ)
Output	Grün/Rot, Vorname, Nachname, Geburtsdatum	QR Code für COVID19-Impfzertifikat und ggf. andere Zertifikate (später Abruf der e-Impfpassdaten der authentifizierten Bürgerin)

TIMELINE

04.06.2021
Umstellung auf EU-QR-Codes

Bis 04.06.2021 ist die Überprüfung der nationalen Zertifikate mit QR-Code über einen Standard-QR-Code Reader möglich. Ausgestellt werden diese wie bisher von Labore und Teststraßen.

Ab 04.06.2021 ist durch die Umstellung auf EU-weit einheitliche QR-Codes der Einsatz von "greenCheck und grünerPass" notwendig. Ein Nachweis ist weiterhin sowohl analog als auch digital möglich.

! Die Regeln für die Zutrittsberechtigungen werden vom Gesetz und EU Verordnung festgelegt und gelten für Papier und elektronische Nachweise und Umsetzung der Überprüfungsmaßnahmen.

Danke, EU DCC

- 2021-05-06: Durch die Kartennummer auf der eCard kann man mit geringem technischen Aufwand den Corona-Status aller Personen in Österreich abfragen.
- 2021-05-07: Ministerium streicht eCard als Nachweis für Grünen Pass

Identifikation der Bürgerinnen (Handysignatur, E-ID / ID Austria), Rückseite der e-card plus PIN (PLZ)
QR Code für COVID19-Impfzertifikat und ggf. andere Zertifikate (später Abruf der e-Impfpassdaten der authentifizierten Bürgerin)

“Grüner Pass”

vs.

(EU) Digital COVID Certificate

Grüner Pass

- Israel: Erster!
- Rot/Grün Anzeige
- EU im Zugzwang
- Politischer Begriff
- Reisepass-Abgrenzung



Digital COVID Certificate (DCC)

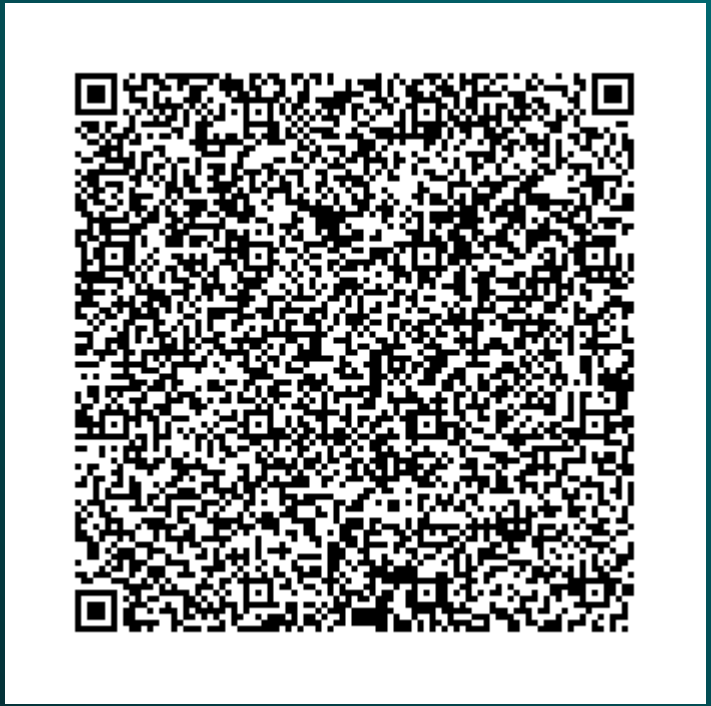
- EU eHealth Network
- Commission Implementing Decision (EU) 2021/1073
- multiple amendments



DURCHFÜHRUNGSBESCHLUSS (EU) 2021/1073

Es sollte [...] ein Transportverschlüsselungs-mechanismus in einem maschinenlesbaren optischen Format (QR) festgelegt werden, das auf dem Bildschirm eines mobilen Geräts angezeigt oder auf Papier ausgedruckt werden kann.

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2021.230.01.0032.01.ENG



https://github.com/ehn-dcc-development/dcc-testdata/tree/main/AT

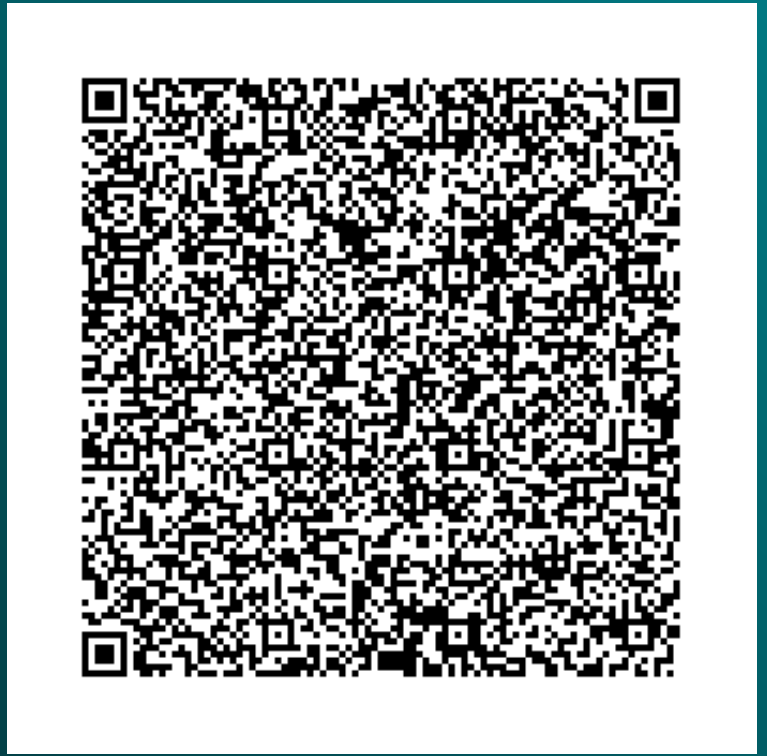
Deutsche Doku

Es sollten eine Spezifikation der Datenstruktur und Verschlüsselungsmechanismen sowie ein **Transportverschlüsselungsmechanismus** in einem maschinenlesbaren optischen Format (QR) festgelegt werden ...

A data structure specification and encoding mechanisms should be specified, as well as a **transport encoding** mechanism in a machine-readable optical format (QR)...

Besser

Es sollten eine Spezifikation der Datenstruktur und Ver-schlüsselungsmechanismen sowie eine **Enkodierung für die Übertragung** in einem maschinenlesbaren optischen Format (QR) festgelegt werden ...



Schei Encoding

- Enkodieren: Zahlenwert entspricht Zeichen

- Ü im ISO-8859-1 Zeichensatz: 220 (11011100)
- 220 im EBCDIC Zeichensatz: }
- 220 im ASCII/ CP437 Zeichensatz: ▄

7 bit ASCII

- American National Standards Institute (ANSI)
- 1967 spezifiziert
- basiert auf den 5 Bit Telegraphie Codes von Émile Baudot (pat. 1874)
- 7 Bit reichen für 128 versch. Zeichen “US-Englisch”
- 1 Bit “gespart”



QR-Code

- Code: Datendarstellung, nicht Verschlüsselung
- Japan, 1994
- automatische Fehlerkorrektur
- optoelektronisch lesbar
- ISO/IEC 18004



QR-Code Eigenschaften

- mehr als 4.000 Zeichen Kapazität
- Binärformat
- 45 unterschiedliche Zeichen (Buchstaben, Ziffern, Satzzeichen)
- Beschädigungen von 7 bis zu 30 % reparierbar

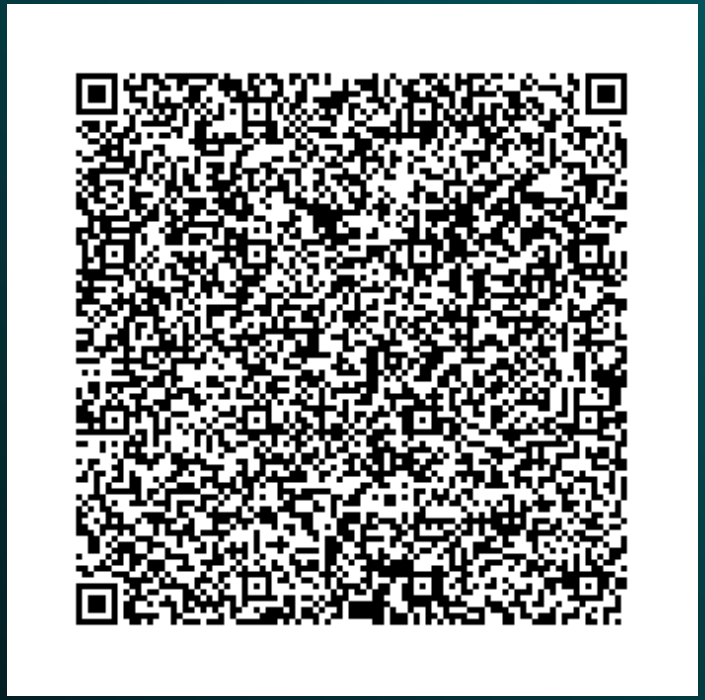


QR Dekodierer

- ZXing ("zebra crossing")
  - 1D/2D barcode image processing library
  - Java, in maintenance mode
- Online-Version: https://zxing.org/w/decode.jspx
- Linux: http://zbar.sourceforge.net/



Dekodieren 01/07



```
48 43 31 3A 4E 43 46 54 57 32 48 3A 37 2A 49 30
36 52 33 57 2F 4A 3A 4F 36 3A 50 34 51 42 33 2B
37 52 4B 46 56 4A 57 56 36 36 55 42 43 45 2F 2F
55 58 44 54 3A 2A 4D 4C 2D 34 44 2E 4E 42 58 52
2B 53 52 48 4D 4E 49 59 36 45 42 38 49 35 39 35
2B 36 55 59 39 2D 2B 30 44 50 49 4F 36 43 35 25
30 53 42 48 4E 2D 4F 57 4B 43 4A 36 42 4C 43 32
4D 2E 4D 2F 4E 50 4B 5A 34 46 33 57 4E 48 45 49
45 36 49 4F 32 36 4C 42 38 3A 46 34 3A 4A 56 55
47 56 59 38 2A 45 4B 43 4C 51 2E 2E 51 43 53 54
53 2B 46 24 3A 30 50 4F 4E 3A 2E 4D 4E 44 34 5A
30 49 39 3A 47 55 2E 4C 42 4A 51 37 2F 32 49 4A
50 52 3A 50 41 4A 46 4F 38 30 4E 4E 30 54 52 4F
...
```

Dekodieren 02/07

```
48 43 31 3A 4E 43 46 54 57 32 48 3A 37 2A 49 30    H C 1 : N C F T W 2 H : 7 * I 0
36 52 33 57 2F 4A 3A 4F 36 3A 50 34 51 42 33 2B    6 R 3 W / J : O 6 : P 4 Q B 3 +
37 52 4B 46 56 4A 57 56 36 36 55 42 43 45 2F 2F    7 R K F V J W V 6 6 U B C E / /
...
```


Barcode Scanner
SHARE
HISTORY
HC1:NCFTW2H:7*I06R3W/
J:O6:P4QB3+7RKFVJWV66UBCE//UXDT:*
ML-4D.NBXR+SRHMNIY6EB8I595+6UY9-+
0DPIO6C5%0SBHN-OWKCJ6BLC2M.M/
NPKZ4F3WNHEIE6IO26LB8:F4:JVUGVY8*
EKCLQ..QCSTS+F$:0PON:.MND4Z0I9:G
U.LBJQ7/2IJPR:PAJFO80NN0TRO1IB:
44:N2336-:KC6M*2N*41C42CA5KCD555O/
A46F6ST1JJ9D0:.MMLH2/G9A7ZX4DCL*0
10LGDFI$MUD82QXSVH6R.CLIL:T4Q312
Format QR_CODE
Type TEXT
Time 17/05/2022 16:56
Metadata Q
Web search
Share via email
Share via SMS
motorola

HC1:NCFTW2H:7*I06R3W/J:O6:P4QB3+7RKFVJWV66UBCE//
UXDT:*ML-4D.NBXR+SRHMNIY6EB8I595+6UY9-+0DPIO6C5%0SBHN-
OWKCJ6BLC2M.M/
NPKZ4F3WNHEIE6IO26LB8:F4:JVUGVY8*EKCLQ..QCSTS+F$:0PON:
.MND4Z0I9:GU.LBJQ7/2IJPR:PAJFO80NN0TRO1IB:44:N2336-:KC
6M*2N*41C42CA5KCD555O/A46F6ST1JJ9D0:.MMLH2/
G9A7ZX4DCL*010LGDFI$MUD82QXSVH6R.CLIL:T4Q3129HXB8WZI8R
ASDE1LL9:9NQDC/O3X3G+A:2U5VP:IE+EMG40R53CG9J3JE1KB
KJA5*$4GW54%LJBIWKE*HBX+4MNEIAD$3NR E228Z9SS4E
R3HUMH3J%-B6DRO3T7GJBU6O URY858P0TR8MDJ$6VL8+7B5$G
CIKIPS2CPVDK%K6+N0GUG+TG+RB5JGOU55HXDR.TL-
N75Y0NHQTZ3XNQMTF/ZHYBQ$8IR9MIQHOSV%9K5-7%ZQ/.15I0*-
J8AVD0N0/0USH.3

NCFTW2H:7*I06R3W/J:O6:P4QB3+7RKFVJWV66UBCE//UXDT:*ML-4D.NBXR+SRHMNIY6EB8I595+6UY9-+0DPIO6C5%0SBHN-OWKCJ6BLC2M.M/
NPKZ4F3WNHEIE6IO26LB8:F4:JVUGVY8*EKCLQ..QCSTS+F$:0PON:.MND4Z0I9:GU.LBJQ7/2IJPR:PAJFO80NN0TRO1IB:44:N2336-:KC
6M*2N*41C42CA5KCD555O/A46F6ST1JJ9D0:.MMLH2/
G9A7ZX4DCL*010LGDFI$MUD82QXSVH6R.CLIL:T4Q3129HXB8WZI8R
ASDE1LL9:9NQDC/O3X3G+A:2U5VP:IE+EMG40R53CG9J3JE1KB
KJA5*$4GW54%LJBIWKE*HBX+4MNEIAD$3NR E228Z9SS4E
R3HUMH3J%-B6DRO3T7GJBU6O URY858P0TR8MDJ$6VL8+7B5$G
CIKIPS2CPVDK%K6+N0GUG+TG+RB5JGOU55HXDR.TL-N75Y0NHQTZ3XNQMTF/ZHYBQ$8IR9MIQHOSV%9K5-7%ZQ/.15I0*-J8AVD0N0/0USH.3

baseX Enkodierung

- Übersetzt 8 Bit Binärdaten in 7 Bit “druckbare” ASCII Zeichen
- baseX definiert den “Zahlenraum” des Ziels
- Base16, Base32, Base64: RFC 4648

base45

- QR-Code: 45 unterschiedliche Zeichen
- "Hello" → “%69 VDL2”

- https://datatracker.ietf.org/doc/html/draft-faltstrom-base45-06

base45 Dekodierer

- Online
  - https://dencode.com/string/base45
- Python
  - https://github.com/kirei/python-base45
- Python 3.7
  - sudo pip install base45

Dekodieren 03/07

```
78 DA 15 8F 3F 2C 03 51 1C 80 9D FA 33 DA 24 35    x . . . ? , . Q . . . . 3 . $ 5
19 C4 D6 F6 F7 EE FA EA EE 62 70 E5 F5 08 E7 CF    . . . . . . . . . b p . . . . .
B5 0D 26 EE BD 5E DB 6B DA A7 B9 DE 35 82 41 45    . . & . . ^ . k . . . . 5 . A E
48 24 36 83 4D 49 07 31 92 D4 60 12 06 B3 88 84    H $ 6 . M I . 1 . . ` . . . . .
...
```

Dekodieren 04/07

```
D2 84 4D A2 04 48 D9 19 37 5F C1 E7 B6 B2 01 26    . . M . . H . . 7 _ . . . . . &
A0 59 01 24 A4 04 1A 61 81 7C A0 06 1A 60 94 2E    . Y . $ . . . a . | . . . ` . .
A0 01 62 41 54 39 01 03 A1 01 A4 61 76 81 AA 62    . . b A T 9 . . . . . a v . . b
64 6E 01 62 6D 61 6D 4F 52 47 2D 31 30 30 30 33    d n . b m a m O R G - 1 0 0 0 3
30 32 31 35 62 76 70 6A 31 31 31 39 33 30 35 30    0 2 1 5 b v p j 1 1 1 9 3 0 5 0
30 35 62 64 74 6A 32 30 32 31 2D 30 32 2D 31 38    0 5 b d t j 2 0 2 1 - 0 2 - 1 8
62 63 6F 62 41 54 62 63 69 78 30 75 72 6E 3A 75    b c o b A T b c i x 0 u r n : u
...
```

Concise Binary Object Representation (CBOR)

- RFC 8949
- binäres Datenformat
- kompakt
- Für Datenaustausch zwischen Anwendungen
- keine Klartextlesbarkeit



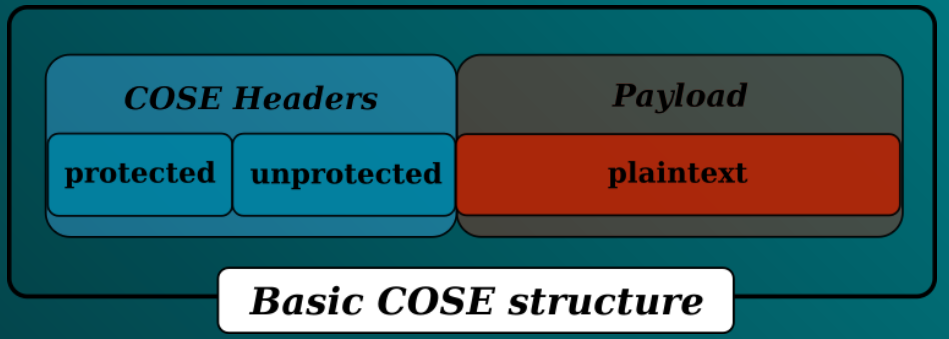
Dekodieren 05/07

```
D2 84 4D A2 04 48 D9 19 37 5F C1 E7 B6 B2 01 26    . . M . . H . . 7 _ . . . . . &
```

- Das erste Byte ist “D2”:
  - most significant 3 Bits == 6 (das ist ein “tag”)
  - least significant 5 Bits == 18 == 0x12
- Concise Binary Object Representation (CBOR) Tag Registratur der IANA: https://www.iana.org/assignments/cbor-tags/cbor-tags.xhtml

CBOR Object Signing and Encryption (COSE)

- RFC 8949
- Erweitert CBOR um
  - Signaturen
  - Message Authentication Codes
  - Verschlüsselung



CBOR Web Token (CWT)

- RFC 8392
- Claim Austausch
  - Info über ein “Subject”
  - Name/Wert Pärchen
- Abgleitet von JWT, nutzt aber CBOR

```
// Example: CBOR Web Token (RFC 8392)
type coseHeader struct {
   Alg int     `cbor:"1,keyasint,omitempty"`
   Kid []byte `cbor:"4,keyasint,omitempty"`
}
type signedCWT struct {
   _           struct{} `cbor:",toarray"`
   Protected   []byte
   Unprotected coseHeader
   Payload     []byte
   Signature   []byte
}

 // Decode []byte into signedCWT struct
 var v signedCWT
 err := cbor.Unmarshal(b, &v)
```

Dekodieren 06/07


```
{
    "dob": "1998-02-26",
    "nam": {
        "fn": "Musterfrau-Gößinger",
        "fnt": "MUSTERFRAU<GOESSINGER",
        "gn": "Gabriele",
        "gnt": "GABRIELE"
    },
"v": [
        {
            "ci":
"urn:uvci:01:AT:10807843F94AEE0EE5093FBC25
4BD813P",
            "co": "AT",
            "dn": 1,
            "dt": "2021-02-18",
            "is": "BMSGPK Austria",
            "ma": "ORG-100030215",
            "mp": "EU/1/20/1528",
            "sd": 2,
            "tg": "840539006",
            "vp": "1119305005"
        }
    ],
    "ver": "1.0.0"
}
```

DCC JSON schema

- upporting the serialization and deserialization of the DCC payload
- focus on generation of a 2D barcode (QR Code)
- Übersetzt Feld-IDs in Feldnamen

https://ec.europa.eu/health/system/files/2021-06/covid-certificate_json_specification_en_0.pdf

Dekodieren 07/07

Last name: Musterfrau-Gößinger

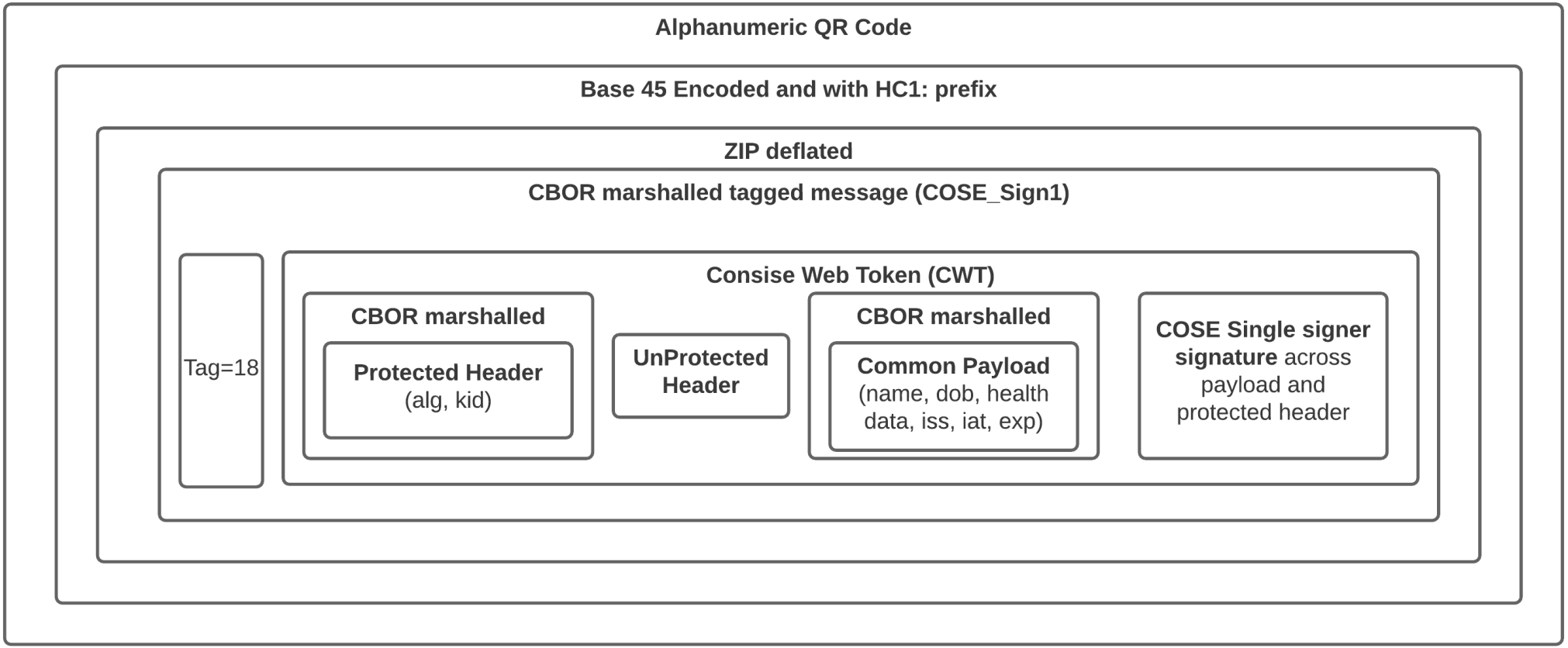
First name: Gabriele

Name as in passport (ICAO 9303 transliteration): MUSTERFRAU<GOESSINGER<<GABRIELE

Birth date: 1998-02-26

Vaccine for COVID-19

- Vaccine name: Comirnaty by Biontech Manufacturing GmbH
- Dose: 1 out of 2 taken on 2021-02-18 in Austria by BMSGPK Austria


Alphanumeric QR Code
Base 45 Encoded and with HC1: prefix
ZIP deflated
CBOR marshalled tagged message (COSE_Sign1)
Tag=18
Consise Web Token (CWT)
CBOR marshalled
Protected Header
(alg, kid)
UnProtected Header
CBOR marshalled
Common Payload
(name, dob, health data, iss, iat, exp)
COSE Single signer signature across payload and protected header

Linux CLI

QR code reader

$ sudo apt-get install zbar-tools

base45 decoder. You need Python3.7 installed (https://www.python.org/downloads/)

$ sudo pip install base45

CBOR analyser. You need Rust installed

$ sudo cargo install cbor-diag-cli

https://www.corentindupont.info/blog/posts/Programming/2021-08-13-GreenPass.html

Python

```
#! /usr/bin/env python3
import json
import sys
import zlib

import base45
import cbor2
from cose.messages import CoseMessage

payload = sys.argv[1][4:]
print("decoding payload: "+ payload)

# decode Base45 (remove HC1: prefix)
decoded = base45.b45decode(payload)

# decompress using zlib
decompressed = zlib.decompress(decoded)
# decode COSE message (no signature verification done)
cose = CoseMessage.decode(decompressed)
# decode the CBOR encoded payload and print as json
print(json.dumps(cbor2.loads(cose.payload), indent=2))
```

```
pip3 install cryptography==2.8

pip3 install cose

pip3 install cbor2

pip3 install base45
```

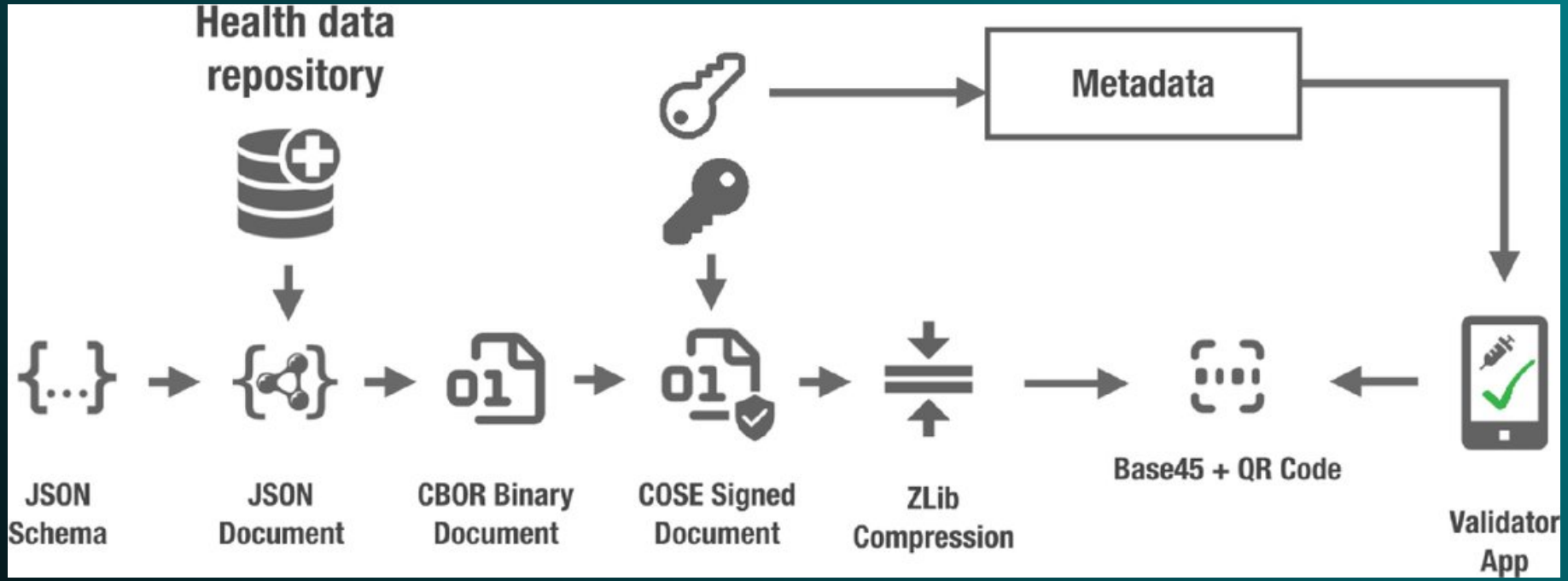
https://hackernoon.com/how-to-decode-your-own-eu-vaccination-green-pass-with-a-few-lines-of-python-9v2c37s1

DCC Online Decoder

Simple decoder of the QR-code, it displays all the information in the Health Certificate QR-code with many technical explanations on the steps.

https://ehealth.vyncke.org/

DURCHFÜHRUNGSBESCHLUSS (EU) 2021/1073



DCC Online Encoder

- A simple encoder of the QR-code, it describes also the many technical explanations on the steps.
- The only purpose of this page is to show that there is no magic behind the QR-code itself.
- The generated QR will be detected as invalid by any good validator because:
  - a human being will notice the 'FAKE' logo in the middle of the QR code
  - the COSE claims are expired since yesterday
  - the key used to sign the COSE Web Token is not trusted
  - the date of birth is in the XIXth century
  - this issuer name will please Harry Potter's fans

https://ehealth.vyncke.org/generate.php

⑤ Bescheinigung über die gesetzliche Pockenschutz-Erstimpfung

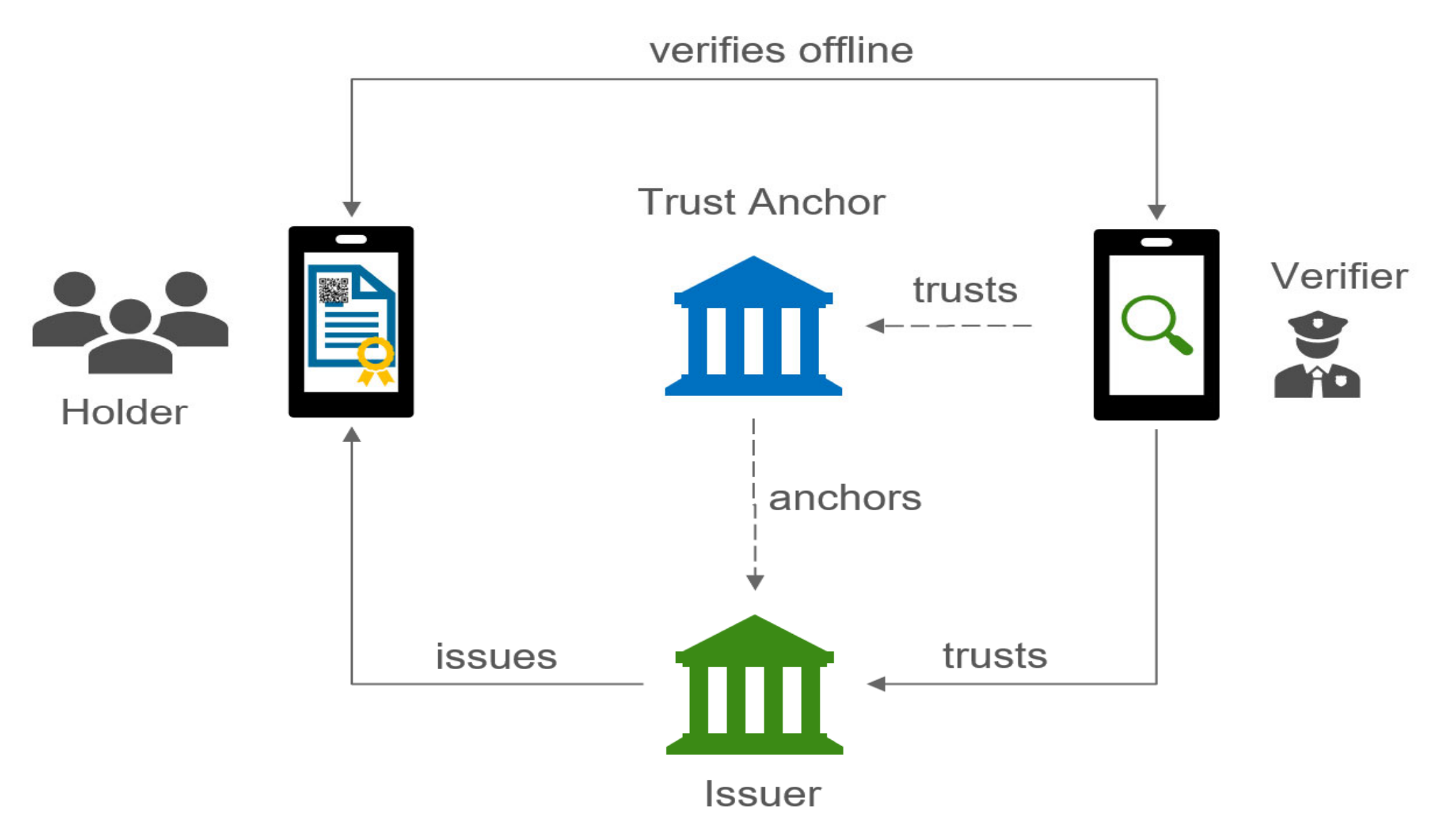
Impfbezirk Impflisten-Nr.	Datum der Impfung	Erfolg mit/ohne*)	An- und Unterschrift des Arztes
Kirchseeon	22.7 1966	mit Erfolg	Dr. med. G. Ebner

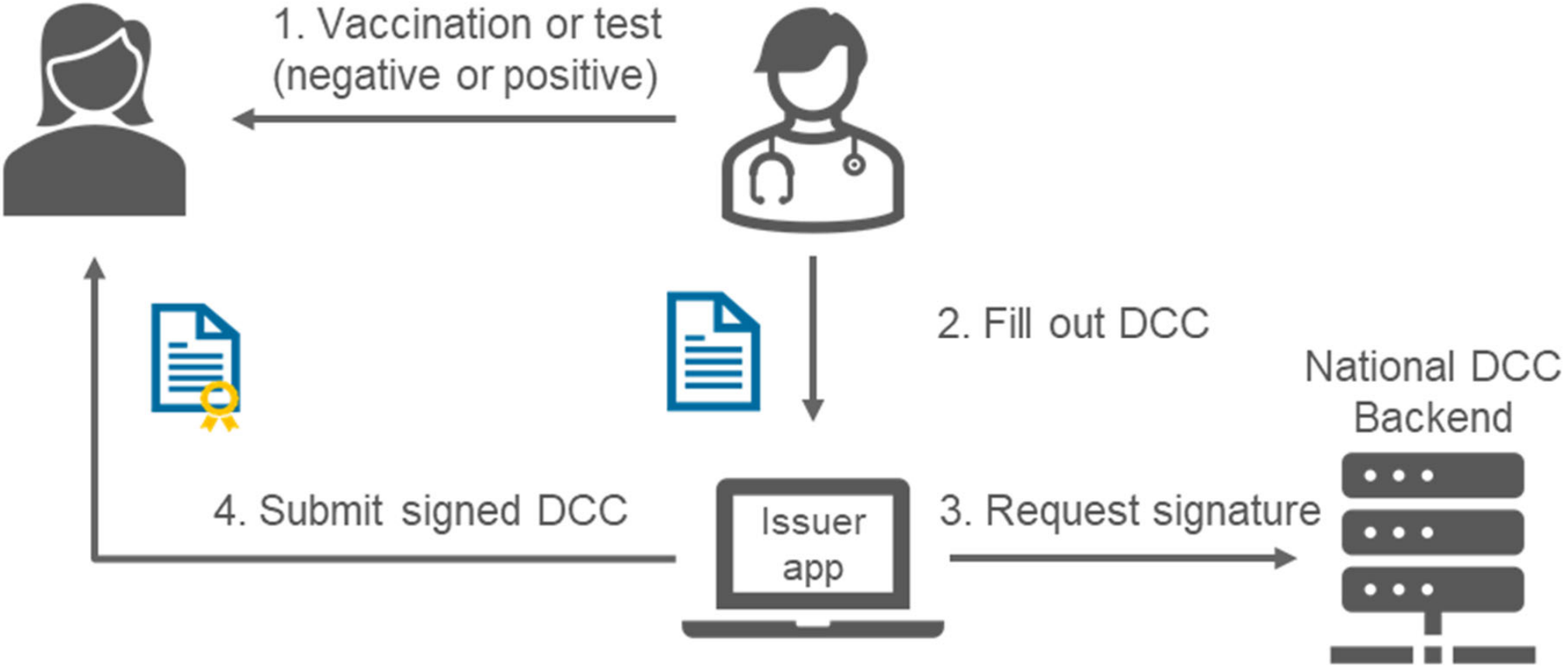
Der gesetzlichen Impfpflicht ist damit genügt **)

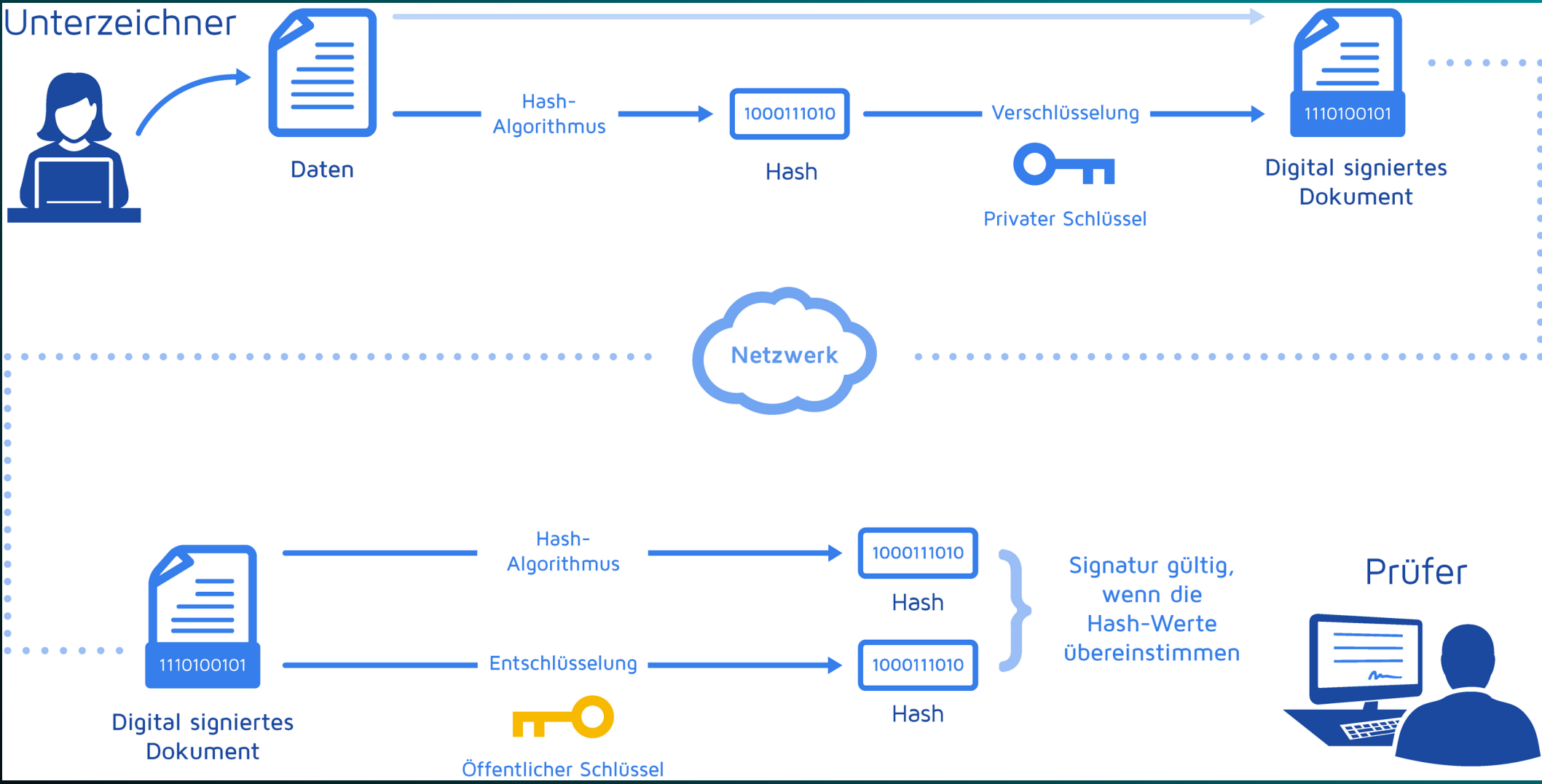
Dr. med. Gregor Ebner
prakt. Arzt

(Unterschrift des Arztes) **)
Eigenschaft: Arzt — Impfarzt

*) Wiederholung möglichst spätestens im folgenden Jahr.
**) Bestätigung erst nach positiver oder dreimaliger negativer Impfung


verifies offline
Trust Anchor
Holder
trusts
Verifier
anchors
issues
trusts
Issuer

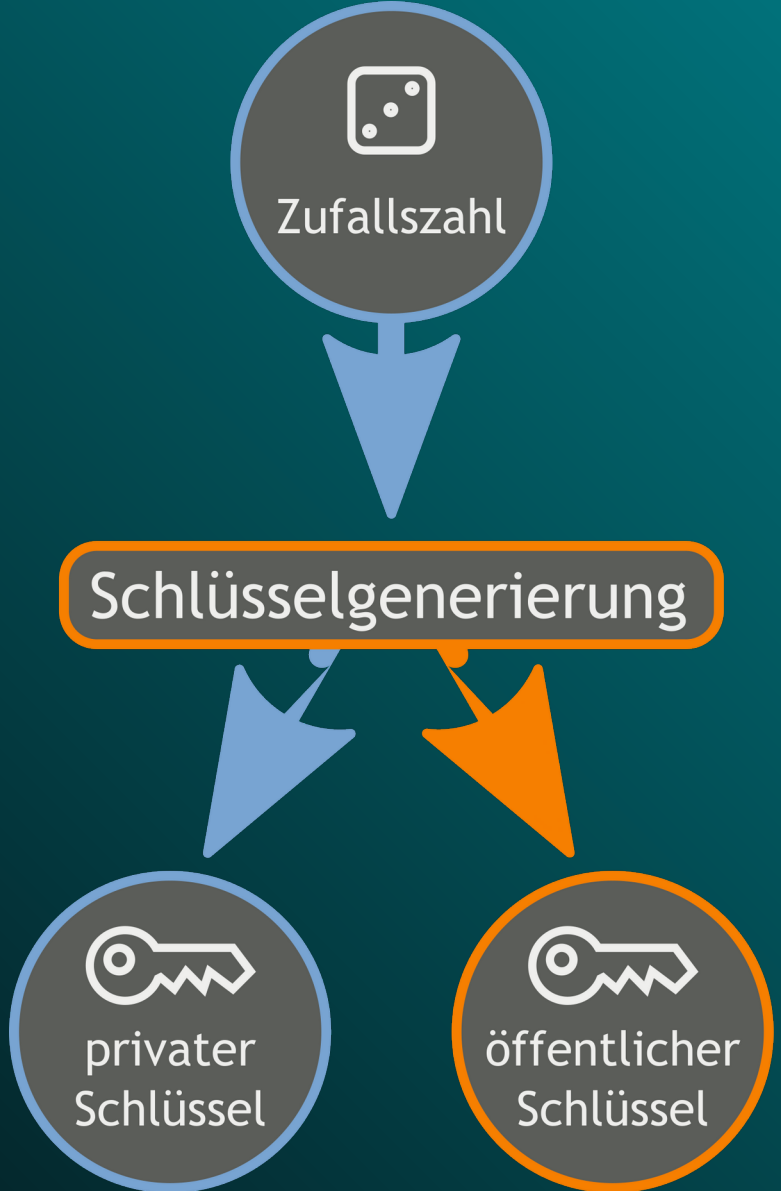

1. Vaccination or test
(negative or positive)
2. Fill out DCC
National DCC
Backend
Issuer
app
3. Request signature
4. Submit signed DCC

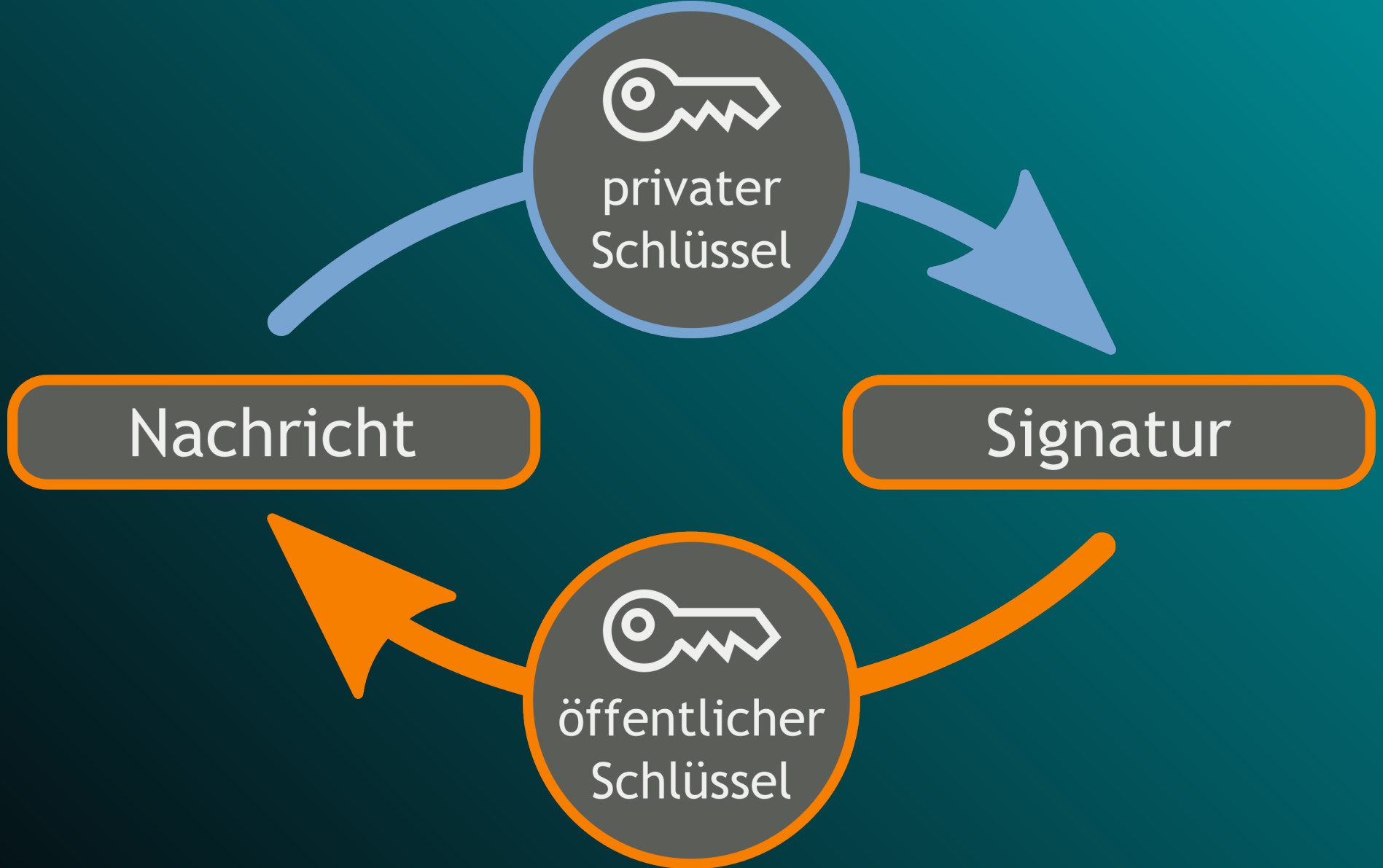

Unterzeichner
Daten
Hash-
Algorithmus
1000111010
Hash
Verschlüsselung
Privater Schlüssel
1110100101
Digital signiertes
Dokument
Netzwerk
1110100101
Digital signiertes
Dokument
Hash-
Algorithmus
1000111010
Hash
Entschlüsselung
Öffentlicher Schlüssel
1000111010
Hash
Signatur gültig,
wenn die
Hash-Werte
übereinstimmen
Prüfer

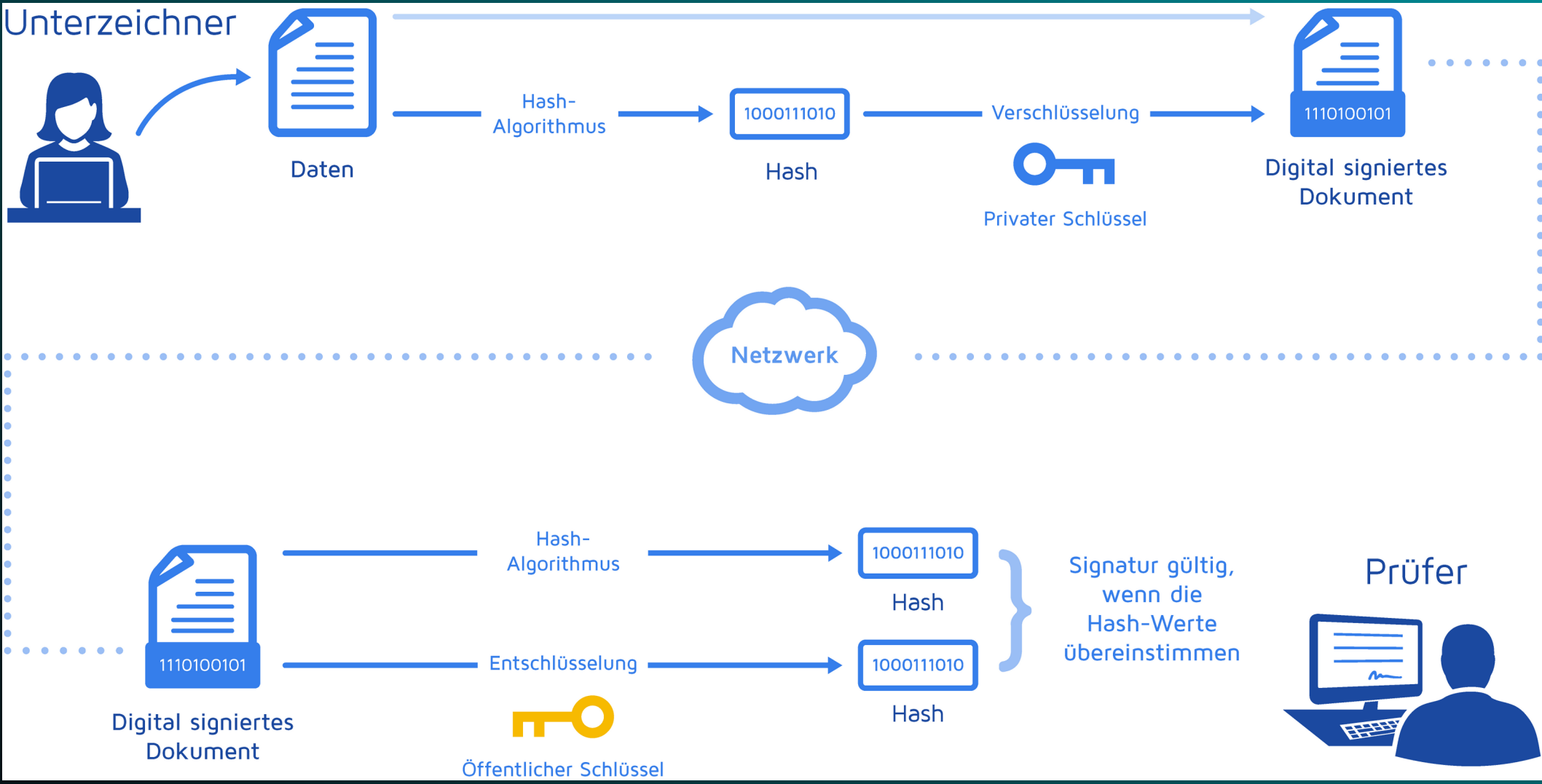
sha256

- “20. Gulaschprogrammiernacht”

- `7c25d7dd373bfed2930cf44893e7e2a29fbf1985eecbd59ae855736acd80fe8a`


Zufallszahl
Schlüsselgenerierung
privater Schlüssel
öffentlicher Schlüssel

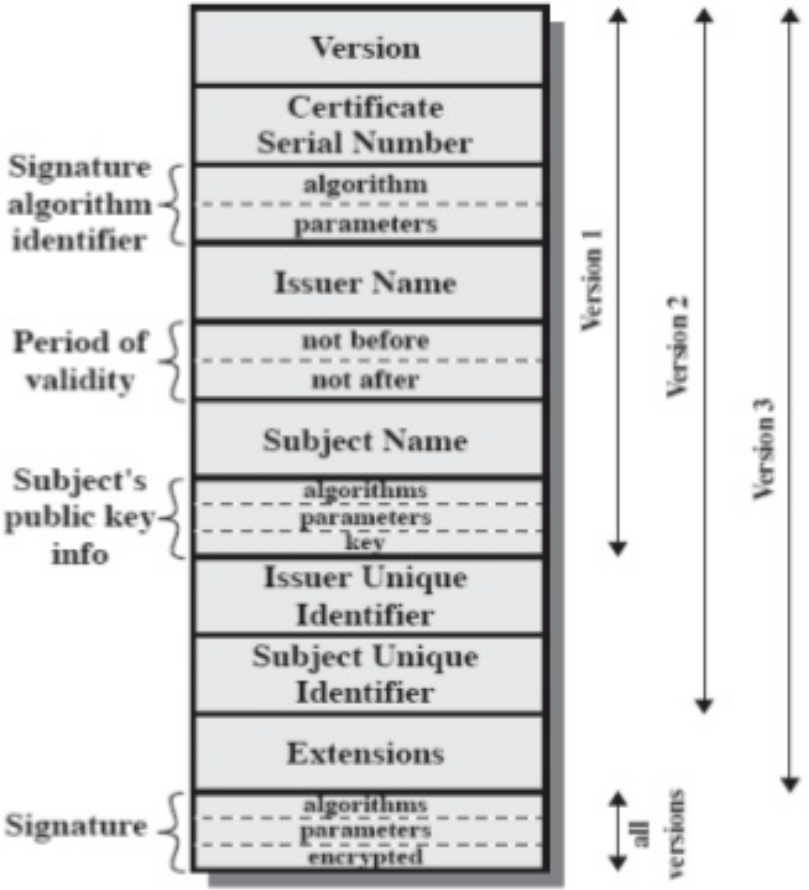

privater
Schlüssel
Nachricht
Signatur
öffentlicher
Schlüssel

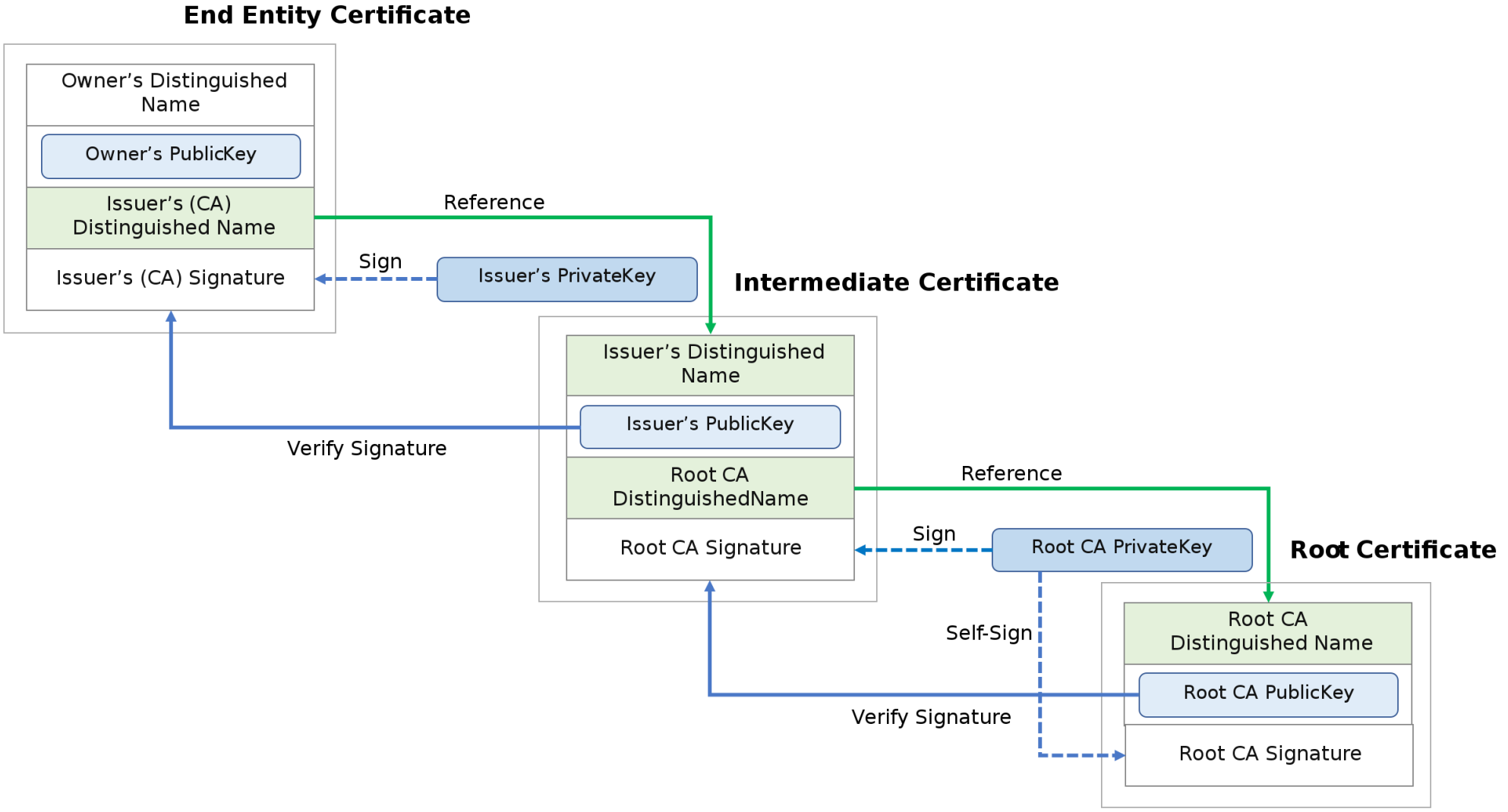

Unterzeichner
Daten
Hash-
Algorithmus
1000111010
Hash
Verschlüsselung
Privater Schlüssel
1110100101
Digital signiertes
Dokument
Netzwerk
1110100101
Digital signiertes
Dokument
Hash-
Algorithmus
1000111010
Hash
Entschlüsselung
Öffentlicher Schlüssel
1000111010
Hash
Signatur gültig,
wenn die
Hash-Werte
übereinstimmen
Prüfer

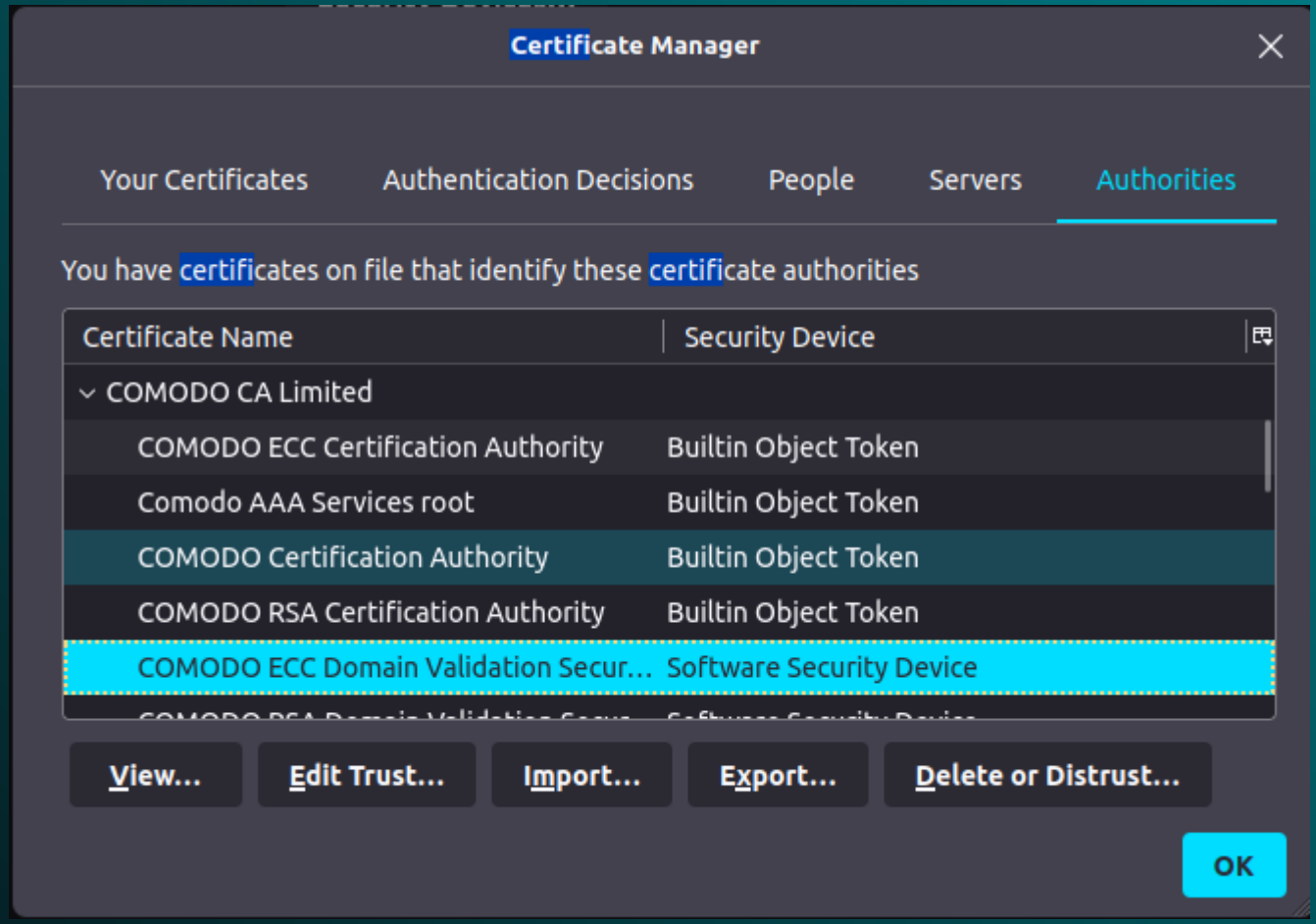
Zertifikate

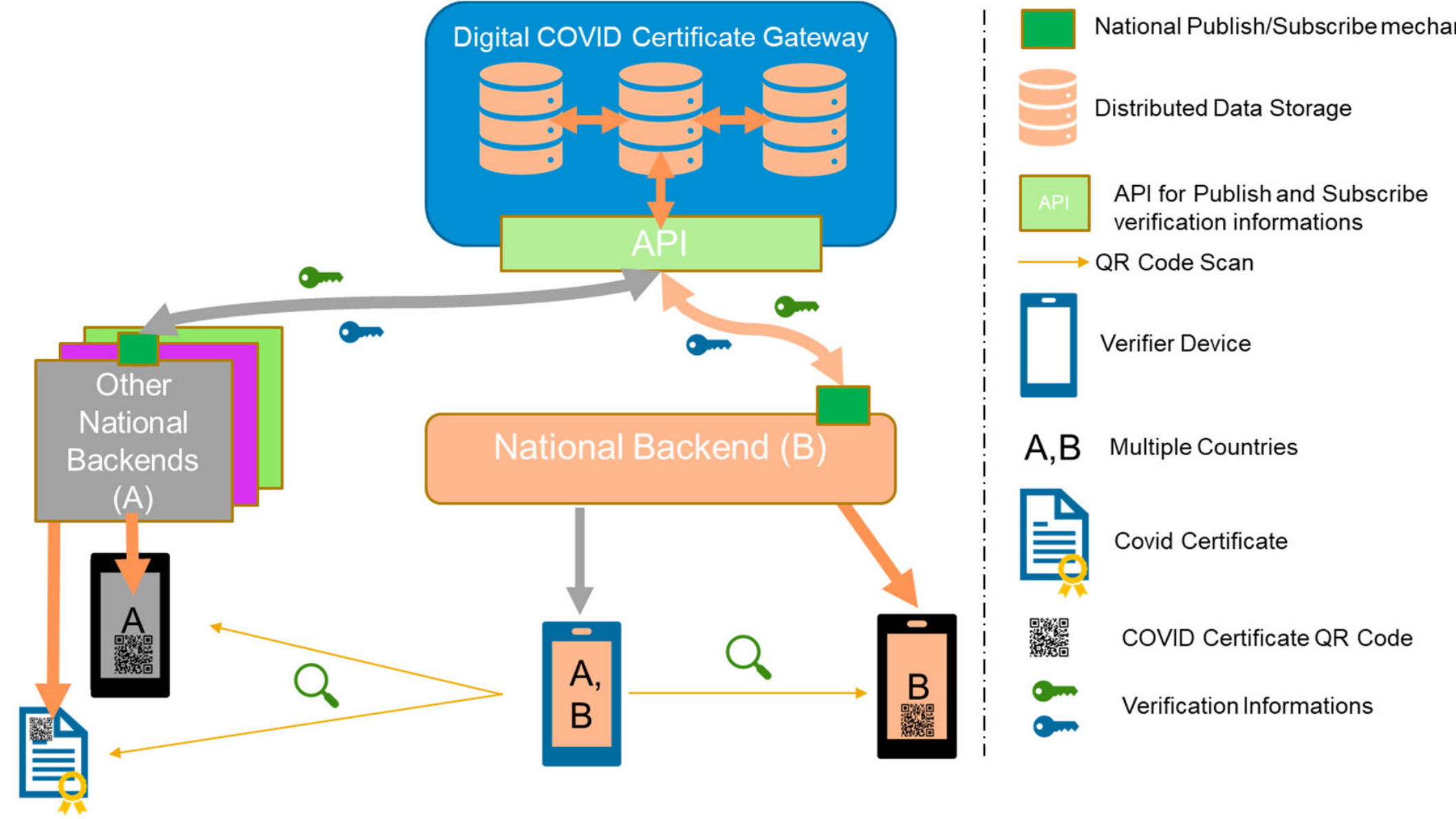
- In zertifikatbasierten Systemen erhält jeder Benutzer ein digitales Zertifikat, welches Angaben zu seiner Identität und den öffentlichen Schlüssel enthält.
- Jedes Zertifikat ist von einer ausgebenden Stelle beglaubigt, die ihrerseits wieder von höheren Stellen beglaubigt sein kann.
- Das Vertrauenssystem dieser PKI ist streng hierarchisch.

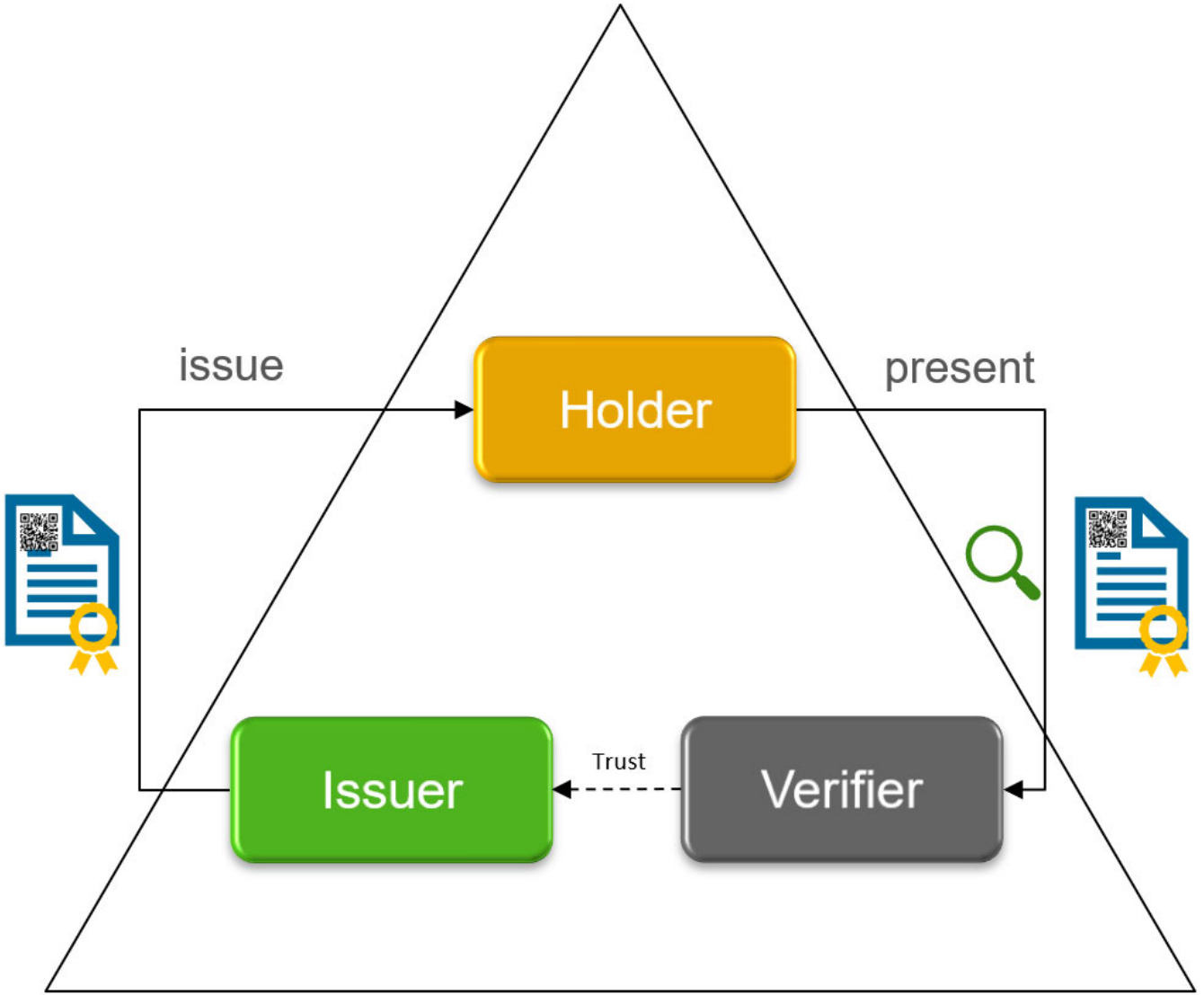
X.509 Certificate Format

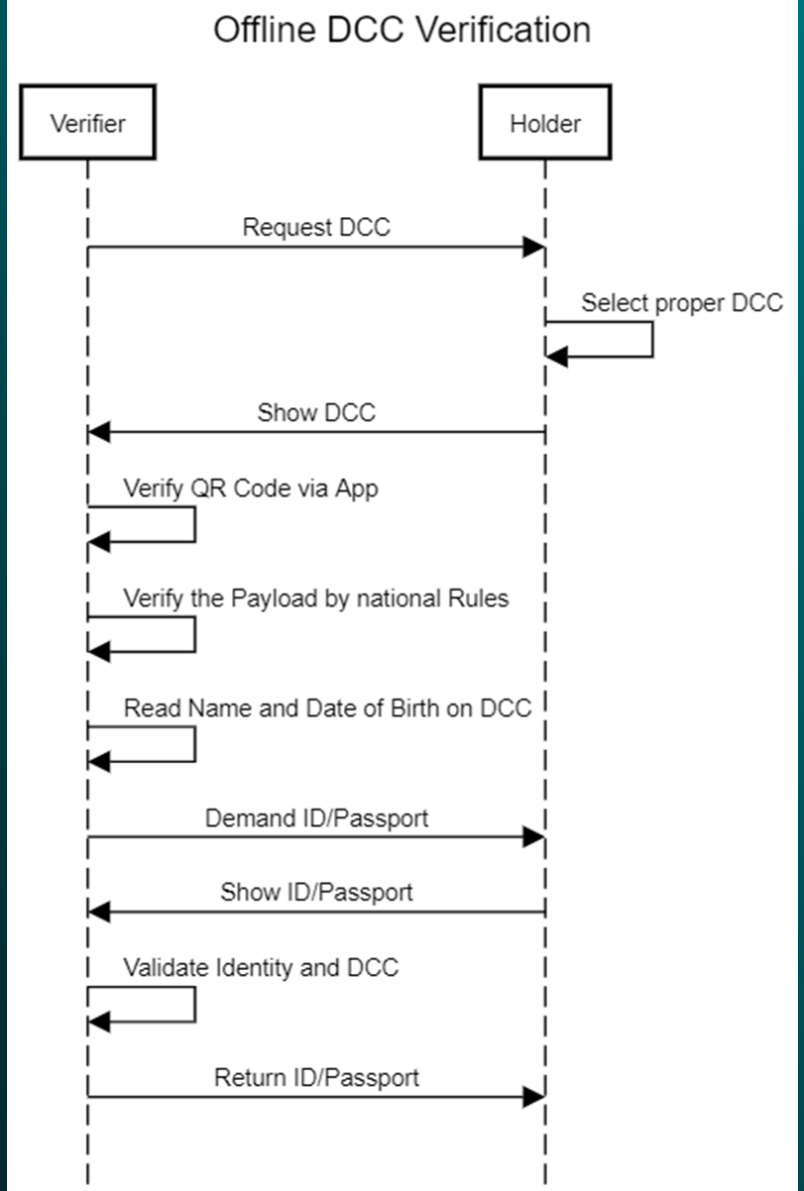


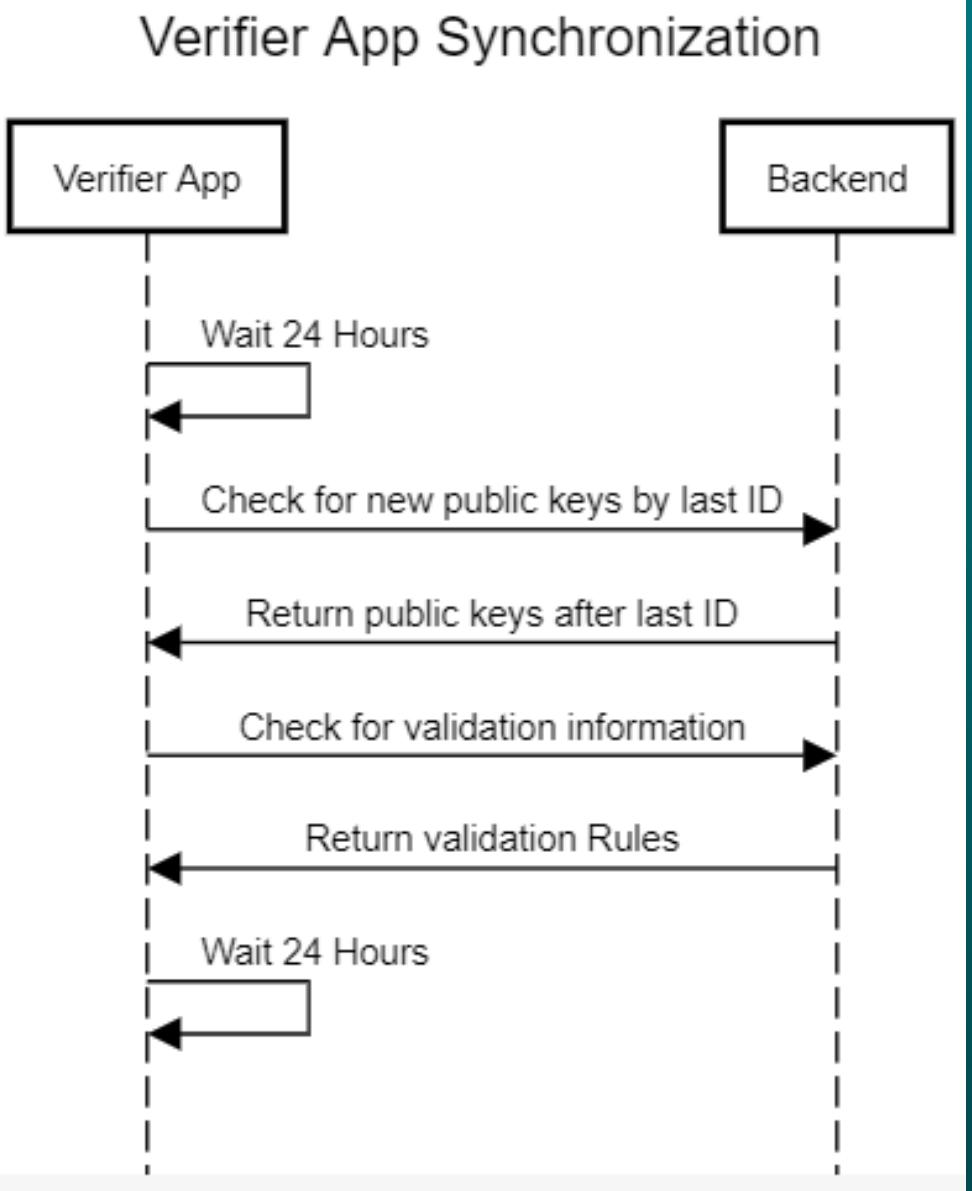

End Entity Certificate
Owner's Distinguished Name
Owner's PublicKey
Issuer's (CA) Distinguished Name
Issuer's (CA) Signature
Reference
Sign
Issuer's PrivateKey
Intermediate Certificate
Issuer's Distinguished Name
Issuer's PublicKey
Root CA DistinguishedName
Root CA Signature
Verify Signature
Reference
Sign
Root CA PrivateKey
Root Certificate
Self-Sign
Root CA Distinguished Name
Root CA PublicKey
Root CA Signature
Verify Signature


Certificate Manager
Your Certificates
Authentication Decisions
People
Servers
Authorities
You have certificates on file that identify these certificate authorities
Certificate Name
Security Device
COMODO CA Limited
COMODO ECC Certification Authority
Builtin Object Token
Comodo AAA Services root
Builtin Object Token
COMODO Certification Authority
Builtin Object Token
COMODO RSA Certification Authority
Builtin Object Token
COMODO ECC Domain Validation Secur…
Software Security Device
View…
Edit Trust…
Import…
Export…
Delete or Distrust…
OK


Digital COVID Certificate Gateway
API
Other National Backends (A)
National Backend (B)
A
A, B
B
National Publish/Subscribe mechan
Distributed Data Storage
API
API for Publish and Subscribe verification informations
QR Code Scan
Verifier Device
A,B
Multiple Countries
Covid Certificate
COVID Certificate QR Code
Verification Informations


issue
Holder
present
Issuer
Trust
Verifier


Offline DCC Verification
Verifier
Holder
Request DCC
Select proper DCC
Show DCC
Verify QR Code via App
Verify the Payload by national Rules
Read Name and Date of Birth on DCC
Demand ID/Passport
Show ID/Passport
Validate Identity and DCC
Return ID/Passport


Verifier App Synchronization
Verifier App
Backend
Wait 24 Hours
Check for new public keys by last ID
Return public keys after last ID
Check for validation information
Return validation Rules
Wait 24 Hours

Revocation

- The incident has no impact on the security and integrity of the EU Gateway managed by the Commission
- The fact that anybody is able to forge cryptographically-valid COVID certificates brings into question the authenticity of even legitimate certificates issued by EU government bodies.
- Should this be the case, the private key would need to be revoked by the government authorities for the entire EU, thereby invalidating both forged and legitimate COVID certificates.



https://www.bleepingcomputer.com/news/security/eu-investigating-leak-of-private-key-used-to-forge-covid-passes/

Implementing Decision (EU) 2021/1073, Annex IV

- In general, digital certificates can be revoked by their issuing CA using certificate revocation lists or Online Certificate Status Protocol Responder (OCSP).
- CSCAs for the DCC system should provide certificate revocation lists (CRLs).
- Even if these CRLs are currently not used by other Member States, they should be integrated for future applications.

Revocation

eHealth Network Guidelines on EU DCC Revocation - B2A

Communication between the Backend and the Applications

Version 1.1

2022-03-30

Danke schön!

Fragen ?

