

1 Analyse von Zertifikaten

1.1 Was fällt Ihnen beim folgenden Zertifikat 01 auf ?

Certificate:

Data:

```
Version: 3 (0x2)
Serial Number:
    e2:c8:fd:55:82:7b:55:32:d9:34:a9:7f:3b:cd:41:fc
Signature Algorithm: sha256WithRSAEncryption
Issuer: O = Acme Co, CN = Kubernetes Ingress Controller Fake Certificate
Validity
    Not Before : Oct 26 20:29:59 2020 GMT
    Not After: Oct 27 20:29:59 2019 GMT
Subject: O = Acme Co, CN = Kubernetes Ingress Controller Fake Certificate
Subject Public Key Info:
    Public Key Algorithm: rsaEncryption
    RSA Public-Key: (2048 bit)
    Modulus:
        00:c9:...
    Exponent: 65537 (0x10001)
    X509v3 extensions:
        X509v3 Key Usage: critical
            Digital Signature, Key Encipherment
        X509v3 Extended Key Usage:
            TLS Web Server Authentication
        X509v3 Basic Constraints: critical
            CA:FALSE
        X509v3 Subject Alternative Name:
            DNS:ingress.local
    Signature Algorithm: sha256WithRSAEncryption
    bd:48:...
```

-----BEGIN CERTIFICATE-----

...

-----END CERTIFICATE-----

1.2 Warum ist das Zertifikat 02 nicht für die Domain google.com gültig ?

Certificate:

Data:

```
Version: 3 (0x2)
Serial Number:
    e2:c8:fd:55:82:7b:55:32:d9:34:a9:7f:3b:cd:41:fc
Signature Algorithm: sha256WithRSAEncryption
Issuer: O = Google Trust Services, CN = GTS CA 101, C = US
Validity
    Not Before: Oct 27 20:29:59 2019 GMT
    Not After : Oct 26 20:29:59 2020 GMT
Subject: O = Google Trust Services, CN = GTS CA 101, C = US
Subject Public Key Info:
    Public Key Algorithm: rsaEncryption
    RSA Public-Key: (2048 bit)
    Modulus:
        00:c9:...
    Exponent: 65537 (0x10001)
    X509v3 extensions:
        X509v3 Key Usage: critical
        Digital Signature, Key Encipherment
        X509v3 Extended Key Usage:
            TLS Web Server Authentication
        X509v3 Basic Constraints: critical
        CA:FALSE
        X509v3 Subject Alternative Name:
            DNS:bing.com
    Signature Algorithm: sha256WithRSAEncryption
    bd:48:...
```

-----BEGIN CERTIFICATE-----

...

-----END CERTIFICATE-----

2 Analyse von Quellcode

Warum akzeptiert der folgende Code auch fehlerhafte Zertifikate ?

3 Weitere Fragen

3.1 Warum war die Ausstellung eines Test Zertifikats für einige Domains von Google durch Symantec ein großes Problem?

3.2 Warum wird der Zweck eines Zertifikats validiert ?