

# Solutions: Sheet 7

## 1. X.509 Certificates in HTTPS

Analyze the X.509 certificate, which your browser obtains when you access <https://www.frankfurt-university.de>. Make sure that you really analyze the certificate of the Frankfurt University of Applied Sciences, and not e.g. a certificate from an intermediate firewall.

(a) What is the public key of the certificate holder (applicant)?

Go to website → Click on lock → View certificates → Go to section **Miscellaneous** → download **PEM (cert)** (file name: **www-frankfurt-university-de.pem**)

```
$ cd Downloads
$ openssl x509 -in www-frankfurt-university-de.pem -pubout
-----BEGIN CERTIFICATE-----
MIIBBjCCBu6gAwIBAgIMIuxme0k+7aBTHr9XMA0GCSqGSIb3DQEBCwUAMIGNMQsw
CQYDVQQGEwJERTFFMEMGA1UECgw8VmVyZWluIHplciBGb2VyZGVydW5nIGVpbmVz
IERldXRzY2h1biBGb3JzY2h1bmdzbmV0emVzIGUuIFYuMRAwDgYDVQQLDAdERk4t
UEtJMSUwIwYDVQQDDDBxERk4tVmVyZWluIEdsb2JhbCBJc3N1aW5nIENBMB4XDTEw
MDUyNjEwMDEyN1oXDTEyMDgyODEwMDEyN1owZGMxMzA0BjNVBAYTAkRFRMQ8wDQYD
VQIDAZIZXNzZW4xGjAYBgNVBACMEUZYyW5rZnVydCBhbSBNYWluMTEwLwYDVQQK
DChGcmFua2Z1cnQgVW5pdmdVyc2l0eSBvZiBBChBsawVkiFNjaWVuY2VzMSQwIgYD
VQDDDBt3d3cuZnJhbmtmdXJ0LXVuaXZlcnNpdHkuZGUwgGEiMA0GCSqGSIb3DQEB
AQUAA4IBDwAwggEKAoIBAQCrcR6vZc8rWsowd1VLEJExfgKEL4H7Q+R2vPdNnZ8h
jtndPtz7LCU796oA2dmZG9nAv9Kw5pcU0vWYAZUpzY63gKhVx1L824iSu/DiG97R
Jn1fSUwF5y/TzwWsQpGUBUFXBnQRp3QFBPMkMYpzJh6lHR4lTHzJJqMJ4hoJ8Qae
p/EREIDBPC07Ca9BBv+Mi3MrGlVWLuGc/IAx+vmCwz+B54uXiurXMWkdMQ+Br7IQ
UwdtKBqz7jvouWExwQuE2CNtUrNA5m0uK7b+JsoC3rtIMS3QI2e9QCmP4L3/9N6N
fgiI4eXu6cmdBmWoM8RzTIK1j0PEkLfhlfmkZ9tjR2aXAgMBAAGjggRcMIIEWDBX
BgNVHSAEUDB0MAgGBmeBDAECAjANBgSRBgEEAYGtIYIsHjAPBg0rBgEEAYGtIYIs
AQEEMBAGDisGAQQBGA0hgiwBAQQGMBAGDisGAQQBGA0hgiwCAQQGMAKGA1UdEwQC
MAAwDgYDVROPAQH/BAQDAgWgMBMGA1UdJQQMMAoGCCsGAQUFBwMBMB0GA1UdDgQW
BBQLwA6vADJtsJlm4+uDCJz4pp3J0jAfBgNVHSMEGDAWgBRrOpil+fJTidrgbIy
Hgkf6Ko7dDAmbGvNHREEHzAdght3d3cuZnJhbmtmdXJ0LXVuaXZlcnNpdHkuZGUw
gY0GA1UdHwSBhTCBgjA/oD2g04Y5aHR0cDovL2NkcDEucGNhLmRmbi5kZS9kZm4t
Y2EtZ2xvYmFsLWcyL3B1Yi9jcmVwY2FjcmVwY3JzSMD+gPaA7hjlodHRwOi8vY2Rw
Mi5wY2EuZGZuLmRlL2Rmbi1jYS1nbG9iYWwtZzIvcHVlL2Nybc9jYWNybC5jcmVw
gdsGCCsGAQUFBwEBBIHOMIHLMDMGCCsGAQUFBzABhidodHRwOi8vb2Nzc5wY2Eu
ZGZuLmRlL09DU1AtU2VydmVyL09DU1AwSQYIKwYBBQUHMAKGPWh0dHA6Ly9jZHAx
LnBjYS5kZm4uZGUvZGZuLWNhLWdsb2JhbC1nMi9wdWIvY2FjZXJ0L2NhY2VydmVz
cnQwSQYIKwYBBQUHMAKGPWh0dHA6Ly9jZHAyLnBjYS5kZm4uZGUvZGZuLWNhLWds
```

```
b2JhbClnMi9wdWIvY2FjZXJ0L2NhY2VydC5jcnQwggH1BgorBgEEAdZ5AgQCBIIB
5QSCAeEB3wB2ALvZ37wfinG1k5Qjl6qSe0c4V5UKq1LoGpCWZDa0HtGFAAABclBt
6AQAAAQDAEcwRQIhAMKZYBDeFbmJniLWNrZx4ewK/mZxatQL3IBoB4fqPuJIAiBG
/Zv/kC4ykT0xg7mtwHGBRh0/SdwF6tthmHn1aF09PgB2AEalVet1+pEgMLWiiWn0
830RLEF0vv1JuIW8vxxw/m1HAAABclBt6H8AAAQDAEcwRQIgZ3Kin0SVdJ62hJVc
fVWZiLVQNYfrblnKQZP0lpJaVw8CIQD2x6Jc845Jg20g1yxP4z6zRX+v/t1n7W/N
CuCK6vfoRwB1AG9Tdqwx8DEZ2JkApFEV/3cVHBHZAseAKQaNsgiaN9kTAAABclBt
6B4AAAQDAEYwRAIgYHGPPxEPqg+QcUb+cIAtMy6LpMYaqfctEPwK09Un0cICICfC
IEYCVk2w12vTJX55awuVhLgh5iTlCfw3o0QNRihaAHYAVYHUwhaQNgFK6gubVzxT
8MDk0HhwJQgXL60qHqcT0wwAAAFyUG3pCgAABAMARzBFAiEAxluGQlwJRW5WNHM8
y+0IR+94QzZLT5G0ctRQ48jtjccCIGMIz2dv6qXnwHomSNJHEKxM0sd+bFJTUV53
Fo+uz6nkMA0GCSqGSIb3DQEBCwUAA4IBAQCvBQSVJ81DfNQLME1CVsmNZYtHmJX
dBDpEjD0TJWFB0QBAKQKDSMFCScUaBvMJDWqi7sLou2doU/F+wEANewGRip/VaUL
oBo+UwCfcjKl16bBRxVKo982F06NMFwGFqP8UyP6KvAHxwefc7tgFJzVN+VSS426
rNWTHb20U131lf47gpK4qMn7m0xojSFvne4GJZDdUrDg4Y3+0bFV0fS8tLBUYAR4
QvWzU0V+z3jtDGAWjJvb5hYlok+c8NviWXYT/BPCet6MnSY3sk1b/6KZXym1s7J8
dWIJGzur99ZG1wJhSS0epMoZE0uAmEFhSt4sBMwj03bJPPrBhoPJQVqZJ
-----END CERTIFICATE-----
```

(b) What is the subject name of the certificate holder (applicant)?

Go to website → Click on lock → View certificates → Go to section **Subject Name**

www.frankfurt-university.de	DFN-Verein Global Issuing CA	DFN-Verein Certification Authority 2	T-TeleSec GlobalRoot Class 2
<b>Subject Name</b>			
Country	DE		
State/Province	Hessen		
Locality	Frankfurt am Main		
Organization	Frankfurt University of Applied Sciences		
Common Name	www.frankfurt-university.de		

(c) Which signature algorithm was used to sign the certificate?

Go to website → Click on lock → View certificates → Go to section **Public Key Info**

<b>Public Key Info</b>	
Algorithm	RSA
Key Size	2048
Exponent	65537
Modulus	AB:71:1E:AF:65:CF:2B:5A:CA:30:77:55:65:10:91:31:7E:02:84:2F:81:FB:43:E4:...

(d) Which CA (Certification Authority) issued the certificate?

Go to website → Click on lock → View certificates → Go to section **Issuer Name**

Issuer Name	
Country	DE
Organization	Verein zur Foerderung eines Deutschen Forschungsnetzes e. V.
Organizational Unit	DFN-PKI
Common Name	DFN-Verein Global Issuing CA

(e) How far can the certification bodies be traced back?

Go to website → Click on lock → View certificates → Select **T-TeleSec GlobalRoot Class**

Validity	
Not Before	Wed, 01 Oct 2008 10:40:14 GMT
Not After	Sat, 01 Oct 2033 23:59:59 GMT

(f) Describe the process for checking the certification chain based on the root certificate using the X.509 certificate from Frankfurt UAS as an example.

## 2. Asymmetrical Email Encryption

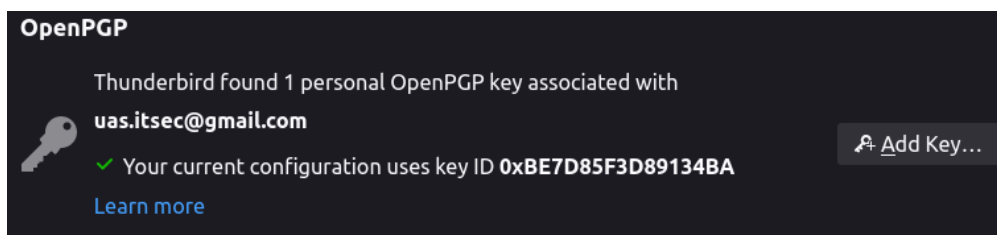
(a) Install an extension for an e-mail client of your choice that allows you to encrypt and decrypt e-mails according to the OpenPGP standard (RFC 4880).

OpenPGP implemented by default since Thunderbird version 78.

(b) Generate a key pair for your e-mail address and upload your public key to a so-called keyserver.

### Creation:

Click **Account Settings** → Choose Email (**uas.itsec@gmail.com**) → Open section **End-To-End Encryption** → Click **+ Add Key...**



Select **Create a new OpenPGP Key** and click **Continue**

Add a Personal OpenPGP Key for uas.itsec@gmail.com

**i** If you have an existing personal key for this email address, you should import it. Otherwise you will not have access to your archives of encrypted emails, nor be able to read incoming encrypted emails from people who are still using your existing key. [Learn more](#)

☒ Create a new OpenPGP Key

☐ Import an existing OpenPGP Key

☐ Use your external key through GnuPG (e.g. from a smartcard)

Cancel Continue

Adjust settings (optional) → Click **Generate Key**

Add a Personal OpenPGP Key for uas.itsec@gmail.com

### Generate OpenPGP Key

**Identity** "Max Semdner (itsec)" <uas.itsec@gmail.com> - uas.itsec@gmail.com

**Key expiry**  
Define the expiration time of your newly generated key. You can later control the date to extend it if necessary.

☒ Key expires in 1 years

☐ Key does not expire

**Advanced settings**  
Control the advanced settings of your OpenPGP Key.

Key type: RSA

Key size: 3072

Go back Cancel Generate key

Generated Public Key:

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
xsDNBGKmBoQBDACon4aqE5LDZymNzECfLLbP4kTa5tRZ1aE+PkFz7D0Awo3sDfV3
xHorTCwSQj7cos+pVJ2PbhWRr0a5fBt4UPZ2CaDBmcc94CSyM7RpXfARKZt5hC8W
Mrh2tT/Vx0UQjdNRLUD+C1HR3FJ1tdI0RoXpu40m0rzTFZA4b0B4UHLDGpK0qh3r
dgmL8yRL/zmfCG2mI06ZjZHmjScbEJZ3qcztDzuLGy/NDLBSNyhCpgcR1bt0HfC+
```


```
aFPSoNG9/RM6xxH/2m4E8DsDJ4X32Moo5mecUjXQ/b0bPkEF+lK1N0qeeAKPEzmJ
c/YjX/b+9nyq0n/ZSZEDr+YAdjy0t80SDGE/Nwh7c6MjCbmTlSYGaSIInMBV7LVG
MN9VmHlEsgf8BQaSJ6za8j6Z06Gkj3fCo9By2XtvoGJwMSQtQwsFkCUi/8GrfH/F
E+ex636cSYMAGcq0qzJ1KdFpDHvF28x6Jpgk+qaEzK2q9Ud5kXRZ60XI65RVGux7
uwiMzbReTRAVdBcAEQEAAcOpTWF4IFNlBWruZXIqKGl0c2VjKSA8dWFzLml0c2Vj
QGdtYWlsLmNvbT7CwQ0EEwEIADcWIQR8BoGsr5kVaLu1IgG+fYXz2JE0ugUCYqYG
hAUJAeEzgAIbAwQLCQgHBRUICQoLBRYCAwEAAAJEL59hfPYkTS6NvcL/0xr070E
cTrYqFhnL8HlaXEB9lJuk+a9NxxHgAMukDLVd6LxCK+cibIBIV9quj fphcmiuAcr
5TnDiagAyJPN2Pow0MhVtRiDg6IwHLZythgw4ZIzQGBE9AtgJBHQPElBo5Wyj3PS
DKGoE090E61bwYK3meYYP3nHD+FKDnYayaJB3xXJEXU3mRq3fV4z3u3woY9Tbaqd
btuQitwF4MMc9aKn03xp2mxw8GkPTxUsA2wXM4Xow2gC115SjlnhivWan0zFrRp
fWLuK68A6vGBX3TroEBQz3iQ6s3b267f7BY876qvE8lw5w2xvhnNwxomh0ybyq917
wzZ76xLIpQ4szMgRQCRw0e3ZT1qQ20ZFRW53oBW8dHbYW6FfBzy7ZgADotKJK0av
ze33fRjW8K4xBRcrlA8J4I3rpgwyAz99y87q2xeY2fHhiLu1PDfxtxRDsDQIk7
LfpK+fAlLIcNm2B8U/7quxSpnlKZWMAyceRi0A08B2gnTspKPvbGjGWys7AzQRi
pgaFAQwAuZ/VxqtVc1Fa00kf7ZhriEXhAfJvaUrki9ePVVVUKnVdjySPoS2KKXP+
mK2fsrC82s0hjkhttrtM0kn/kBpnN/BZe0jdEqdc9RYi0Sfa/le3UPKfMFvgZiI7A
Is0iMNBPlYcnkM10yW3lSYnKHCskIXlqPQV0339eo6aDnFPtqxf7qcup6p6z6ZmP
RIsuxmp5KLTz294oyZsmvHex2i0BJv8U9GvQjZHnuQddUKpV+2giYvjy1UiXVqki
9qT3oHLSvNlIYdjka4l+kpeJ500UQy56ANDcx60ziRv6Ua+T0QpxPJNDGz78dD3G
/aTv71bwEcwqQhqcxy4oaPt+85c/03hw47ZMfFNSgbem73TXKDkozrxMQGVt50c
1cgQ0l5qaC0aR4fuSi9yzrEJ88dtem0Q7rgSJgnsPazuAMJ3e8KQ7QmIaq0+jdsC
T4T+IzYs4yFP9swmN8fs1Byipcx059rPg3X+Fi2k6RFhgFyWurCE8tqjoHH906Kz
Xp/qZwcXABEBAAHCwPwEGAEIACYWIQR8BoGsr5kVaLu1IgG+fYXz2JE0ugUCYqYG
hQUJAeEzgAIbDAAKCRC+fYXz2JE0ustaC/sHemGMzWo1lS2rfIlepWtQeyz+GIlu
eCwMM3+8xZxVFlcqhwR9vUXBRUJ047MqXAvvsaIoQBldoI/T75Bzk9EE+xQ2E6Tv
ADijVm59fxU75QI4A0MhluUwdYFS/QGWExBno0zJXcjBcq0W2l2Dk0T+uDiwzwjN
bNAiIL2/uj4IV2tuKdN52n8mZPRE5V3uy9Yj0e6YRE6qEDaYKiqsVQcvV01hndqs
aECfVx1enWXJediVq/ZI4nouHpneF3/QwetbcMIW6Q6w4Xnz+c0JQXS05vsLb3TR
YhsdghLKoe1l5EE7LMwCWTPpSIwS3WCutWQAuT4ikfF/1GYsW/Ilb/rXh9gd4B4
2+uDys5HR8uzVKU0ZsgWtd+rqlcomLlp9SGMhEzQHCSY0170N0jFNPpGZxX+D0Xc
Xo8AfKMRDedTA99+JmaqX3Uft/zA+tE1ll7P/aMcV0oLfuyACldi7yUajauEBCCD
NXVs5dulq9420vcgBGRQkfRYZhUWniw4yjk=
=hBU1
-----END PGP PUBLIC KEY BLOCK-----
```

## Upload:


Select [More](#) → export public key to file

0xBE7D85F3D89134BA

Expires on: 12.6.2023

 **Fingerprint**

 7C06 81AC AF99 1568 BBB5 2201 BE7D 85F3 D891 34BA

 **Created**

 12.6.2022

Key Properties

More

Upload file to <https://keys.openpgp.org/upload>

keys.openpgp.org

Upload your key

Browse...

Max Semdner (itsec)\_uas.its....0xBE7D85F3D89134BA-pub.asc

Upload

Need more info? Check our [intro](#) and [usage guide](#).

Send verification mail

keys.openpgp.org

You uploaded the key [7C0681ACAF991568BBB52201BE7D85F3D89134BA](#).

This key is now published with only non-identity information. ([What does this mean?](#))

To make the key available for search by email address, you can verify it belongs to you:

uas.itsec@gmail.com

Send Verification Email

**Note:** Some providers delay emails for up to 15 minutes to prevent spam. Please be patient.

Accept mail (then it's public accessible)

keys.openpgp.org

Your key [7C0681ACAF991568BBB52201BE7D85F3D89134BA](#) is now published for the identity [uas.itsec@gmail.com](#).

**Validation:**

Can be validated by others on <https://keys.openpgp.org/>

# keys.openpgp.org

Q Search

You can also [upload](#) or [manage](#) your key.

Find out more [about this service](#).

---

**News:** [Celebrating 100.000 verified addresses!](#) 📈 (2019-11-12)

# keys.openpgp.org

We found an entry for `uas.itsec@gmail.com`.

<https://keys.openpgp.org/vks/v1/by-fingerprint/7C0681ACAF991568BBB52201BE7D85F3D89134BA>

**Hint:** It's more convenient to use `keys.openpgp.org` from your OpenPGP software.

Take a look at our [usage guide](#) for details.

(c) Make the public keys of your team members known to your e-mail client by importing them from a keyserver.

(d) Send an encrypted and signed email to your team members.