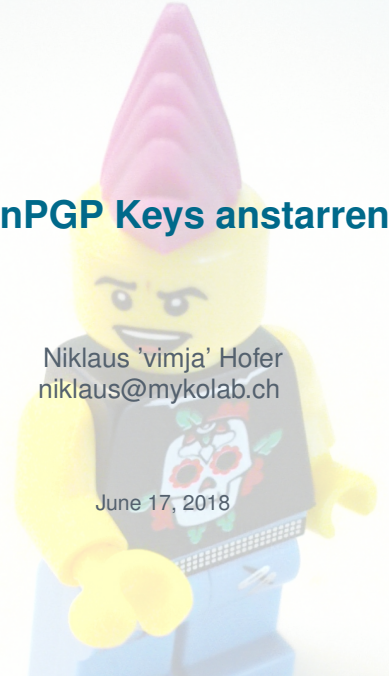
OpenPGP Keys anstarren

Niklaus 'vimja' Hofer
niklaus@mykolab.ch

June 17, 2018



/me

- Founding member of the Chaostreff Bern
- Studiert an der BFH
  - IT / Infosec

/me und OpenPGP

- Keine Assoziation mit...
  - OpenPGP
  - GnuPG
  - PeP
  - ...
- Regelmässig Keysignings organisiert
- Krypto Grundlagen bekannt aus Studium

Content I

Einführung

OpenPGP Zertifikate

Tools
- pgpgdump
- hopenpgp

Inhalt

Einführung

OpenPGP Zertifikate

Tools

All computers are broken

Meiner Erfahrung nach ist Dokumentation:

- nicht vorhanden / inexistent
- unvollständig
- outdated
- unpräzise
- schlicht falsch

Ausserdem ist Software in der Regel Buggy...

Kontrolle geht über vertrauen

... Zumindest bei Computern.

- Kein blindes vertrauen in
  - Dokumentation
  - Ratschläge online
  - Den Output des ausführenden Programmes
- Kontrolliere das Ergebnis
- Insbesondere bei Crypto

Inhalt

Einführung

OpenPGP Zertifikate

Tools

GnuPG Keys erstellen

- Viele Anleitungen online
- In der Regel nur die Anweisungen, keine Kontrollmöglichkeiten

Disclaimer

- Der in dieser Präsentation verwendete Schlüssel ist unsicher
- erstellt zu Demonstrationszwecken

Zielsetzung

- analysieren des Zertifikates
- Analog zu `openssl x509` output

OpenSSL x509


```
openssl x509 \
    -noout \
    -text \
    -in cert.pem
```

OpenSSL x509


```
[...]

    Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
        Validity
            Not Before: Mar 27 14:08:00 2018 GMT
            Not After : Jun 25 14:08:00 2018 GMT
                Subject: CN=xmpp.honet.ch

[...]

            X509v3 Subject Alternative Name:
                DNS:jabber.honet.ch, DNS:xmpp.honet.ch

[...]
```

OpenSSL x509


```
X509v3 extensions:
    X509v3 Subject Alternative Name:
        othername:<unsupported>, othername:<unsupported>
```

GnuPG Bordmittel


```
gpg \
    --keyid-format LONG \
        --fingerprint \
        --with-keygrip \
        --list-secret-keys
```

GnuPG Bordmittel

Ausgabe:

```
sec    rsa4096/93D3F6873020F6EB 2018-05-08 [C] [expires: 2018-07-01]
       Key fingerprint = F1CC 6A0D 12BD DDEA 4C46  2B0D 93D3 F687 3020
           F6EB
       Keygrip = 58A4A9A839B089A9A6AD45D07A724028E63A3B07
uid                  [ultimate] vimja <demo@honet.ch>
uid                  [ultimate] vimja <vimja@example.com>
ssb    ed25519/F48A34AB5D92BD2C 2018-05-08 [A] [expires: 2018-07-01]
       Keygrip = 945028EBEC67F8B313956AC97629DD33B98D1D93
ssb    dsa1024/EE41AAB9C4E3FFFC 2018-05-08 [S] [expires: 2018-07-01]
       Keygrip = 1B7520ABB7AE1FFEB590B149F05F68D6269C74EE
ssb    elg2048/6B3F9652BF6E7FA1 2018-05-08 [E] [expires: 2018-07-01]
       Keygrip = E945803708D76444E4A037C95226DEF151D7008F
```

GnuPG Bordmittel

keyid (Erstellt aus dem letzten Stellen des Fingerprint)

```
sec    rsa4096/93D3F6873020F6EB 2018-05-08 [C] [expires: 2018-07-01]
       Key fingerprint = F1CC 6A0D 12BD DDEA 4C46  2B0D 93D3 F687 3020
           F6EB
       Keygrip = 58A4A9A839B089A9A6AD45D07A724028E63A3B07
uid                  [ultimate] vimja <demo@honet.ch>
uid                  [ultimate] vimja <vimja@example.com>
ssb    ed25519/F48A34AB5D92BD2C 2018-05-08 [A] [expires: 2018-07-01]
       Keygrip = 945028EBEC67F8B313956AC97629DD33B98D1D93
ssb    dsa1024/EE41AAB9C4E3FFFC 2018-05-08 [S] [expires: 2018-07-01]
       Keygrip = 1B7520ABB7AE1FFEB590B149F05F68D6269C74EE
ssb    elg2048/6B3F9652BF6E7FA1 2018-05-08 [E] [expires: 2018-07-01]
       Keygrip = E945803708D76444E4A037C95226DEF151D7008F
```

GnuPG Bordmittel

fingerprint

```
sec    rsa4096/93D3F6873020F6EB 2018-05-08 [C] [expires: 2018-07-01]
       Key fingerprint = F1CC 6A0D 12BD DDEA 4C46  2B0D 93D3 F687 3020
           F6EB
       Keygrip = 58A4A9A839B089A9A6AD45D07A724028E63A3B07
uid                  [ultimate] vimja <demo@honet.ch>
uid                  [ultimate] vimja <vimja@example.com>
ssb    ed25519/F48A34AB5D92BD2C 2018-05-08 [A] [expires: 2018-07-01]
       Keygrip = 945028EBEC67F8B313956AC97629DD33B98D1D93
ssb    dsa1024/EE41AAB9C4E3FFFC 2018-05-08 [S] [expires: 2018-07-01]
       Keygrip = 1B7520ABB7AE1FFEB590B149F05F68D6269C74EE
ssb    elg2048/6B3F9652BF6E7FA1 2018-05-08 [E] [expires: 2018-07-01]
       Keygrip = E945803708D76444E4A037C95226DEF151D7008F
```

GnuPG Bordmittel

keygrip (unique identifier for a keypair)

```
sec    rsa4096/93D3F6873020F6EB 2018-05-08 [C] [expires: 2018-07-01]
       Key fingerprint = F1CC 6A0D 12BD DDEA 4C46  2B0D 93D3 F687 3020
           F6EB
       Keygrip = 58A4A9A839B089A9A6AD45D07A724028E63A3B07
uid                  [ultimate] vimja <demo@honet.ch>
uid                  [ultimate] vimja <vimja@example.com>
ssb    ed25519/F48A34AB5D92BD2C 2018-05-08 [A] [expires: 2018-07-01]
       Keygrip = 945028EBEC67F8B313956AC97629DD33B98D1D93
ssb    dsa1024/EE41AAB9C4E3FFFC 2018-05-08 [S] [expires: 2018-07-01]
       Keygrip = 1B7520ABB7AE1FFEB590B149F05F68D6269C74EE
ssb    elg2048/6B3F9652BF6E7FA1 2018-05-08 [E] [expires: 2018-07-01]
       Keygrip = E945803708D76444E4A037C95226DEF151D7008F
```

GnuPG Bordmittel

Element Typ identifier

```
sec    rsa4096/93D3F6873020F6EB 2018-05-08 [C] [expires: 2018-07-01]
       Key fingerprint = F1CC 6A0D 12BD DDEA 4C46  2B0D 93D3 F687 3020
           F6EB
       Keygrip = 58A4A9A839B089A9A6AD45D07A724028E63A3B07
uid                  [ultimate] vimja <demo@honet.ch>
uid                  [ultimate] vimja <vimja@example.com>
ssb    ed25519/F48A34AB5D92BD2C 2018-05-08 [A] [expires: 2018-07-01]
       Keygrip = 945028EBEC67F8B313956AC97629DD33B98D1D93
ssb    dsa1024/EE41AAB9C4E3FFFC 2018-05-08 [S] [expires: 2018-07-01]
       Keygrip = 1B7520ABB7AE1FFEB590B149F05F68D6269C74EE
ssb    elg2048/6B3F9652BF6E7FA1 2018-05-08 [E] [expires: 2018-07-01]
       Keygrip = E945803708D76444E4A037C95226DEF151D7008F
```

GnuPG Bordmittel

Key type

```
sec    rsa4096/93D3F6873020F6EB 2018-05-08 [C] [expires: 2018-07-01]
       Key fingerprint = F1CC 6A0D 12BD DDEA 4C46  2B0D 93D3 F687 3020
           F6EB
       Keygrip = 58A4A9A839B089A9A6AD45D07A724028E63A3B07
uid                  [ultimate] vimja <demo@honet.ch>
uid                  [ultimate] vimja <vimja@example.com>
ssb    ed25519/F48A34AB5D92BD2C 2018-05-08 [A] [expires: 2018-07-01]
       Keygrip = 945028EBEC67F8B313956AC97629DD33B98D1D93
ssb    dsa1024/EE41AAB9C4E3FFFC 2018-05-08 [S] [expires: 2018-07-01]
       Keygrip = 1B7520ABB7AE1FFEB590B149F05F68D6269C74EE
ssb    elg2048/6B3F9652BF6E7FA1 2018-05-08 [E] [expires: 2018-07-01]
       Keygrip = E945803708D76444E4A037C95226DEF151D7008F
```

GnuPG Bordmittel

Key usage

```
sec    rsa4096/93D3F6873020F6EB 2018-05-08 [C] [expires: 2018-07-01]
       Key fingerprint = F1CC 6A0D 12BD DDEA 4C46  2B0D 93D3 F687 3020
           F6EB
       Keygrip = 58A4A9A839B089A9A6AD45D07A724028E63A3B07
uid                  [ultimate] vimja <demo@honet.ch>
uid                  [ultimate] vimja <vimja@example.com>
ssb    ed25519/F48A34AB5D92BD2C 2018-05-08 [A] [expires: 2018-07-01]
       Keygrip = 945028EBEC67F8B313956AC97629DD33B98D1D93
ssb    dsa1024/EE41AAB9C4E3FFFC 2018-05-08 [S] [expires: 2018-07-01]
       Keygrip = 1B7520ABB7AE1FFEB590B149F05F68D6269C74EE
ssb    elg2048/6B3F9652BF6E7FA1 2018-05-08 [E] [expires: 2018-07-01]
       Keygrip = E945803708D76444E4A037C95226DEF151D7008F
```

GnuPG Bordmittel

UID trust

```
sec    rsa4096/93D3F6873020F6EB 2018-05-08 [C] [expires: 2018-07-01]
       Key fingerprint = F1CC 6A0D 12BD DDEA 4C46  2B0D 93D3 F687 3020
           F6EB
       Keygrip = 58A4A9A839B089A9A6AD45D07A724028E63A3B07
uid                  [ultimate] vimja <demo@honet.ch>
uid                  [ultimate] vimja <vimja@example.com>
ssb    ed25519/F48A34AB5D92BD2C 2018-05-08 [A] [expires: 2018-07-01]
       Keygrip = 945028EBEC67F8B313956AC97629DD33B98D1D93
ssb    dsa1024/EE41AAB9C4E3FFFC 2018-05-08 [S] [expires: 2018-07-01]
       Keygrip = 1B7520ABB7AE1FFEB590B149F05F68D6269C74EE
ssb    elg2048/6B3F9652BF6E7FA1 2018-05-08 [E] [expires: 2018-07-01]
       Keygrip = E945803708D76444E4A037C95226DEF151D7008F
```

GnuPG Bordmittel

Creation date

```
sec    rsa4096/93D3F6873020F6EB 2018-05-08 [C] [expires: 2018-07-01]
       Key fingerprint = F1CC 6A0D 12BD DDEA 4C46  2B0D 93D3 F687 3020
           F6EB
       Keygrip = 58A4A9A839B089A9A6AD45D07A724028E63A3B07
uid                  [ultimate] vimja <demo@honet.ch>
uid                  [ultimate] vimja <vimja@example.com>
ssb    ed25519/F48A34AB5D92BD2C 2018-05-08 [A] [expires: 2018-07-01]
       Keygrip = 945028EBEC67F8B313956AC97629DD33B98D1D93
ssb    dsa1024/EE41AAB9C4E3FFFC 2018-05-08 [S] [expires: 2018-07-01]
       Keygrip = 1B7520ABB7AE1FFEB590B149F05F68D6269C74EE
ssb    elg2048/6B3F9652BF6E7FA1 2018-05-08 [E] [expires: 2018-07-01]
       Keygrip = E945803708D76444E4A037C95226DEF151D7008F
```

GnuPG Bordmittel

Expiration date

```
sec    rsa4096/93D3F6873020F6EB 2018-05-08 [C] [expires: 2018-07-01]
       Key fingerprint = F1CC 6A0D 12BD DDEA 4C46  2B0D 93D3 F687 3020
           F6EB
       Keygrip = 58A4A9A839B089A9A6AD45D07A724028E63A3B07
uid                  [ultimate] vimja <demo@honet.ch>
uid                  [ultimate] vimja <vimja@example.com>
ssb    ed25519/F48A34AB5D92BD2C 2018-05-08 [A] [expires: 2018-07-01]
       Keygrip = 945028EBEC67F8B313956AC97629DD33B98D1D93
ssb    dsa1024/EE41AAB9C4E3FFFC 2018-05-08 [S] [expires: 2018-07-01]
       Keygrip = 1B7520ABB7AE1FFEB590B149F05F68D6269C74EE
ssb    elg2048/6B3F9652BF6E7FA1 2018-05-08 [E] [expires: 2018-07-01]
       Keygrip = E945803708D76444E4A037C95226DEF151D7008F
```

–list-secred-keys Bonus

Keys können für verschiedene Zwecke verwendet werden

```
sec>   rsa4096/0xB8A370B45E3400FC 2012-04-02 [SC] [revoked: 2017-11-14]
       55B3E8E659B09F1F754E3967B8A370B45E3400FC
       Card serial no. = 0006 04136111
```

–list-secred-keys Bonus

Master key auf smartcard

```
sec>   rsa4096/0xB8A370B45E3400FC 2012-04-02 [SC] [revoked: 2017-11-14]
       55B3E8E659B09F1F754E3967B8A370B45E3400FC
       Card serial no. = 0006 04136111
```

–list-secred-keys Bonus

Nicht vorhandener master key

```
sec#   rsa4096/0xC2763A151BA30BAE 2017-11-04 [C] [expires: 2022-12-31]
       18E95BC7C8F55DBB1CE9CEFBC2763A151BA30BAE
uid                    [ unknown] Niklaus Manuel Hofer <niklaus@mykolab
    .ch>
ssb>   rsa4096/0xE670951C874F0B08 2017-11-04 [S] [expires: 2019-12-31]
ssb>   rsa4096/0x77B300C55E7280EE 2017-11-04 [E] [expires: 2019-12-31]
ssb>   rsa4096/0xA6FB4048313C40A7 2017-11-04 [A] [expires: 2019-12-31]
ssb>   ed25519/0x3DE8BF457D826CBD 2017-11-04 [A] [expires: 2019-12-31]
ssb>   ed25519/0xCE02C97E745697D2 2017-11-04 [S] [expires: 2019-12-31]
ssb>   cv25519/0xB31120454E8DF234 2017-11-04 [E] [expires: 2019-12-31]
```

–list-secred-keys Bonus

Subkeys auf smartcard

```
sec#   rsa4096/0xC2763A151BA30BAE 2017-11-04 [C] [expires: 2022-12-31]
       18E95BC7C8F55DBB1CE9CEFBC2763A151BA30BAE
uid                    [ unknown] Niklaus Manuel Hofer <niklaus@mykolab
    .ch>
ssb>   rsa4096/0xE670951C874F0B08 2017-11-04 [S] [expires: 2019-12-31]
ssb>   rsa4096/0x77B300C55E7280EE 2017-11-04 [E] [expires: 2019-12-31]
ssb>   rsa4096/0xA6FB4048313C40A7 2017-11-04 [A] [expires: 2019-12-31]
ssb>   ed25519/0x3DE8BF457D826CBD 2017-11-04 [A] [expires: 2019-12-31]
ssb>   ed25519/0xCE02C97E745697D2 2017-11-04 [S] [expires: 2019-12-31]
ssb>   cv25519/0xB31120454E8DF234 2017-11-04 [E] [expires: 2019-12-31]
```

OpenPG Zertifikats Struktur

- Wir wollen mehr Details
- Verständnis für den Aufbau des Zertifikates

  An OpenPGP message is constructed from a number of records that are traditionally called packets. [...] An OpenPGP message, keyring, certificate, and so forth consists of a number of packets.

– RFC4880, Kapitel 4

list packets 1


```
gpg \
    --export \
    --armor \
    55B3E8E659B09F1F754E3967B8A370B45E3400FC \
    | gpg \
    --list-packets
```

list packets 1


```
[...]
# off=1791 ctb=89 tag=2 hlen=3 plen=540
:signature packet: algo 1, keyid A97A7702BAF91EF5
        version 4, created 1375701634, md5len 0, sigclass 0x10
        digest algo 10, begin of digest d0 35
        hashed subpkt 2 len 4 (sig created 2013-08-05)
        subpkt 16 len 8 (issuer key ID A97A7702BAF91EF5)
        data: [4094 bits]
# off=2334 ctb=88 tag=2 hlen=2 plen=70
:signature packet: algo 17, keyid C932807B37901254
        version 4, created 1333743630, md5len 0, sigclass 0x10
        digest algo 2, begin of digest 04 e8
        hashed subpkt 2 len 4 (sig created 2012-04-06)
        subpkt 16 len 8 (issuer key ID C932807B37901254)
        data: [160 bits]
        data: [159 bits]
[...]
```

list packets 2


```
gpg \
    --export \
    --armor \
    --export-options export-minimal \
    F1CC6A0D12BDDDEA4C462B0D93D3F6873020F6EB \
    | gpg \
    --list-packets
```

list packets 2


```
# off=0 ctb=99 tag=6 hlen=3 plen=525
:public key packet:
        version 4, algo 1, created 1525801707, expires 0
        pkey[0]: [4096 bits]
        pkey[1]: [17 bits]
        keyid: 93D3F6873020F6EB
```

Algorithmen

- Problem: Algorithmen nummeriert
- Lookup im RFC4880, Kapitel 9.1 bis 9.4
- GnuPG Source Code `common/openpgpdefs.h`

Zertifikatsaufbau (user ID)


```
# off=528 ctb=b4 tag=13 hlen=2 plen=21
:user ID packet: "vimja <demo@honet.ch>"
```

Zertifikatsaufbau (user ID)


```
# off=551 ctb=89 tag=2 hlen=3 plen=591
:signature packet: algo 1, keyid 93D3F6873020F6EB
        version 4, created 1525802354, md5len 0, sigclass 0x13
        digest algo 10, begin of digest c7 9d
        hashed subpkt 33 len 21 (issuer fpr v4
            F1CC6A0D12BDDDEA4C462B0D93D3F6873020F6EB)
        hashed subpkt 2 len 4 (sig created 2018-05-08)
        hashed subpkt 27 len 1 (key flags: 01)
        hashed subpkt 9 len 4 (key expires after 53d16h11m)
        hashed subpkt 11 len 2 (pref-sym-algos: 7 2)
        hashed subpkt 21 len 2 (pref-hash-algos: 2 3)
        hashed subpkt 22 len 3 (pref-zip-algos: 2 3 0)
        hashed subpkt 30 len 1 (features: 01)
        hashed subpkt 23 len 1 (keyserver preferences: 80)
        subpkt 16 len 8 (issuer key ID 93D3F6873020F6EB)
        data: [4095 bits]
```

Zertifikatsaufbau (user ID)


```
# off=551 ctb=89 tag=2 hlen=3 plen=591
:signature packet: algo 1, keyid 93D3F6873020F6EB
        version 4, created 1525802354, md5len 0, sigclass 0x13
        digest algo 10, begin of digest c7 9d
        hashed subpkt 33 len 21 (issuer fpr v4
            F1CC6A0D12BDDDEA4C462B0D93D3F6873020F6EB)
        hashed subpkt 2 len 4 (sig created 2018-05-08)
        hashed subpkt 27 len 1 (key flags: 01)
        hashed subpkt 9 len 4 (key expires after 53d16h11m)
        hashed subpkt 11 len 2 (pref-sym-algos: 7 2)
        hashed subpkt 21 len 2 (pref-hash-algos: 2 3)
        hashed subpkt 22 len 3 (pref-zip-algos: 2 3 0)
        hashed subpkt 30 len 1 (features: 01)
        hashed subpkt 23 len 1 (keyserver preferences: 80)
        subpkt 16 len 8 (issuer key ID 93D3F6873020F6EB)
        data: [4095 bits]
```

Zertifikatsaufbau (user ID)


```
# off=551 ctb=89 tag=2 hlen=3 plen=591
:signature packet: algo 1, keyid 93D3F6873020F6EB
        version 4, created 1525802354, md5len 0, sigclass 0x13
        digest algo 10, begin of digest c7 9d
        hashed subpkt 33 len 21 (issuer fpr v4
            F1CC6A0D12BDDDEA4C462B0D93D3F6873020F6EB)
        hashed subpkt 2 len 4 (sig created 2018-05-08)
        hashed subpkt 27 len 1 (key flags: 01)
        hashed subpkt 9 len 4 (key expires after 53d16h11m)
        hashed subpkt 11 len 2 (pref-sym-algos: 7 2)
        hashed subpkt 21 len 2 (pref-hash-algos: 2 3)
        hashed subpkt 22 len 3 (pref-zip-algos: 2 3 0)
        hashed subpkt 30 len 1 (features: 01)
        hashed subpkt 23 len 1 (keyserver preferences: 80)
        subpkt 16 len 8 (issuer key ID 93D3F6873020F6EB)
        data: [4095 bits]
```

Zertifikatsaufbau (user ID)


```
# off=551 ctb=89 tag=2 hlen=3 plen=591
:signature packet: algo 1, keyid 93D3F6873020F6EB
        version 4, created 1525802354, md5len 0, sigclass 0x13
        digest algo 10, begin of digest c7 9d
        hashed subpkt 33 len 21 (issuer fpr v4
            F1CC6A0D12BDDDEA4C462B0D93D3F6873020F6EB)
        hashed subpkt 2 len 4 (sig created 2018-05-08)
        hashed subpkt 27 len 1 (key flags: 01)
        hashed subpkt 9 len 4 (key expires after 53d16h11m)
        hashed subpkt 11 len 2 (pref-sym-algos: 7 2)
        hashed subpkt 21 len 2 (pref-hash-algos: 2 3)
        hashed subpkt 22 len 3 (pref-zip-algos: 2 3 0)
        hashed subpkt 30 len 1 (features: 01)
        hashed subpkt 23 len 1 (keyserver preferences: 80)
        subpkt 16 len 8 (issuer key ID 93D3F6873020F6EB)
        data: [4095 bits]
```

Zertifikatsaufbau (user ID)


```
# off=551 ctb=89 tag=2 hlen=3 plen=591
:signature packet: algo 1, keyid 93D3F6873020F6EB
        version 4, created 1525802354, md5len 0, sigclass 0x13
        digest algo 10, begin of digest c7 9d
        hashed subpkt 33 len 21 (issuer fpr v4
            F1CC6A0D12BDDDEA4C462B0D93D3F6873020F6EB)
        hashed subpkt 2 len 4 (sig created 2018-05-08)
        hashed subpkt 27 len 1 (key flags: 01)
        hashed subpkt 9 len 4 (key expires after 53d16h11m)
        hashed subpkt 11 len 2 (pref-sym-algos: 7 2)
        hashed subpkt 21 len 2 (pref-hash-algos: 2 3)
        hashed subpkt 22 len 3 (pref-zip-algos: 2 3 0)
        hashed subpkt 30 len 1 (features: 01)
        hashed subpkt 23 len 1 (keyserver preferences: 80)
        subpkt 16 len 8 (issuer key ID 93D3F6873020F6EB)
        data: [4095 bits]
```

Zertifikatsaufbau (subkeys)


```
# off=1769 ctb=b8 tag=14 hlen=2 plen=51
:public sub key packet:
        version 4, algo 22, created 1525803019, expires 0
        pkey[0]: [80 bits] ed25519 (1.3.6.1.4.1.11591.15.1)
        pkey[1]: [263 bits]
        keyid: F48A34AB5D92BD2C
```

Zertifikatsaufbau (subkeys)


```
# off=1822 ctb=89 tag=2 hlen=3 plen=572
:signature packet: algo 1, keyid 93D3F6873020F6EB
        version 4, created 1525803019, md5len 0, sigclass 0x18
        digest algo 8, begin of digest fc 97
        hashed subpkt 33 len 21 (issuer fpr v4
            F1CC6A0D12BDDDEA4C462B0D93D3F6873020F6EB)
        hashed subpkt 2 len 4 (sig created 2018-05-08)
        hashed subpkt 27 len 1 (key flags: 20)
        hashed subpkt 9 len 4 (key expires after 53d15h49m)
        subpkt 16 len 8 (issuer key ID 93D3F6873020F6EB)
        data: [4095 bits]
```

Inhalt

Einführung

OpenPGP Zertifikate

Tools
- pgpgdump
- hopenpgp

Inhalt

Einführung

OpenPGP Zertifikate

Tools
- pgpgdump
- hopenpgp

pgpdump introduction

- Besser formatiert
- Beannte Algorithmen
- Trotzdem unübersichtlich
- Zeigt auch signature packets

pgpdump Output


```
gpg \
    --export \
    --armor \
    --export-options export-minimal \
    F1CC6A0D12BDDDEA4C462B0D93D3F6873020F6EB \
    | pgpdump
```

pgpdump Output


```
Old: Public Key Packet(tag 6)(525 bytes)
        Ver 4 - new
        Public key creation time - Tue May  8 19:48:27 CEST 2018
        Pub alg - RSA Encrypt or Sign(pub 1)
        RSA n(4096 bits) - ...
        RSA e(17 bits) - ...
```

pgpdump Output


```
Old: User ID Packet(tag 13)(21 bytes)
        User ID - vimja <demo@honet.ch>
```

pgpdump Output


```
Old: Signature Packet(tag 2)(591 bytes)
        Ver 4 - new
        Sig type - Positive certification of a User ID and Public Key
            packet(0x13).
        Pub alg - RSA Encrypt or Sign(pub 1)
        Hash alg - SHA512(hash 10)
        Hashed Sub: unknown(sub 33)(21 bytes)
        Hashed Sub: signature creation time(sub 2)(4 bytes)
                Time - Tue May  8 19:59:14 CEST 2018
        Hashed Sub: key flags(sub 27)(1 bytes)
                Flag - This key may be used to certify other keys
        Hashed Sub: key expiration time(sub 9)(4 bytes)
                Time - Sun Jul  1 12:00:00 CEST 2018
        Hashed Sub: preferred symmetric algorithms(sub 11)(2 bytes)
                Sym alg - AES with 128-bit key(sym 7)
                Sym alg - Triple-DES(sym 2)

                                [...]
```

pgpdump Output


```
Old: Signature Packet(tag 2)(591 bytes)
        Ver 4 - new
        Sig type - Positive certification of a User ID and Public Key
            packet(0x13).
        Pub alg - RSA Encrypt or Sign(pub 1)
        Hash alg - SHA512(hash 10)
        Hashed Sub: unknown(sub 33)(21 bytes)
        Hashed Sub: signature creation time(sub 2)(4 bytes)
                Time - Tue May  8 19:59:14 CEST 2018
        Hashed Sub: key flags(sub 27)(1 bytes)
                Flag - This key may be used to certify other keys
        Hashed Sub: key expiration time(sub 9)(4 bytes)
                Time - Sun Jul  1 12:00:00 CEST 2018
        Hashed Sub: preferred symmetric algorithms(sub 11)(2 bytes)
                Sym alg - AES with 128-bit key(sym 7)
                Sym alg - Triple-DES(sym 2)

                                [...]
```

pgpdump Output


```
[...]

Hashed Sub: preferred hash algorithms(sub 21)(2 bytes)
        Hash alg - SHA1(hash 2)
        Hash alg - RIPEMD160(hash 3)
Hashed Sub: preferred compression algorithms(sub 22)(3 bytes)
        Comp alg - ZLIB <RFC1950>(comp 2)
        Comp alg - BZip2(comp 3)
        Comp alg - Uncompressed(comp 0)
Hashed Sub: features(sub 30)(1 bytes)
        Flag - Modification detection (packets 18 and 19)
Hashed Sub: key server preferences(sub 23)(1 bytes)
        Flag - No-modify
Sub: issuer key ID(sub 16)(8 bytes)
        Key ID - 0x93D3F6873020F6EB
Hash left 2 bytes - c7 9d
RSA m^d mod n(4095 bits) - ...
        -> PKCS-1
```

pgpdump Output


```
[...]

Hashed Sub: preferred hash algorithms(sub 21)(2 bytes)
        Hash alg - SHA1(hash 2)
        Hash alg - RIPEMD160(hash 3)
Hashed Sub: preferred compression algorithms(sub 22)(3 bytes)
        Comp alg - ZLIB <RFC1950>(comp 2)
        Comp alg - BZip2(comp 3)
        Comp alg - Uncompressed(comp 0)
Hashed Sub: features(sub 30)(1 bytes)
        Flag - Modification detection (packets 18 and 19)
Hashed Sub: key server preferences(sub 23)(1 bytes)
        Flag - No-modify
Sub: issuer key ID(sub 16)(8 bytes)
        Key ID - 0x93D3F6873020F6EB
Hash left 2 bytes - c7 9d
RSA m^d mod n(4095 bits) - ...
        -> PKCS-1
```

Inhalt

Einführung

OpenPGP Zertifikate

Tools
- pgpgdump
- hopenpgp

hopenpgp

- OpenPGP Implementation in Haskell
- Unvollständig
- Super analysetools

hkt und GnuPG 2.1


```
hkt \
    export-pubkeys F1CC6A0D12BDDDEA4C462B0D93D3F6873020F6EB \
    | hokey lint
```

hkt und GnuPG 2.1


```
hkt (hopenpgp-tools) 0.20
Copyright (C) 2012-2018  Clint Adams
hkt comes with ABSOLUTELY NO WARRANTY. This is free software, and you
    are welcome to redistribute it under certain conditions.
hokey (hopenpgp-tools) 0.20
Copyright (C) 2012-2018  Clint Adams
hokey comes with ABSOLUTELY NO WARRANTY. This is free software, and
    you are welcome to redistribute it under certain conditions.
hkt: /home/pgptest/.gnupg/pubring.gpg: openBinaryFile: does not exist
    (No such file or directory)
hokey: Unexpected finalization failure
CallStack (from HasCallStack):
  error, called at ./Codec/Encryption/OpenPGP/KeyringParser.hs:55:33
      in hOpenPGP-2.5.5-7yNpuvQFfipH5zYNxJg4qw:Codec.Encryption.
      OpenPGP.KeyringParser
```

hkt und GnuPG 2.1

- GnuPG 2.1 und neuer verwenden kein `pubring.gpg`
  - Gilt nur für Neuinstallation
- Neues `pubring.kbx` Format
- von hopenpgp nicht unterstützt

hkt trotz GnuPG 2.1


```
gpg \
    --output .gnupg/pubring.gpg \
    --export F1CC6A0D12BDDDEA4C462B0D93D3F6873020F6EB
```

hkt trotz GnuPG 2.1


```
hkt \
    export-pubkeys F1CC6A0D12BDDDEA4C462B0D93D3F6873020F6EB \
    | hokey lint
```

hopenpgp output


```
Key has potential validity: good
Key has fingerprint: F1CC 6A0D 12BD DDEA 4C46  2B0D 93D3 F687 3020
    F6EB
Checking to see if key is OpenPGPv4: V4
Checking to see if key is RSA or DSA (>= 2048-bit): RSA 4096
Checking user-ID- and user-attribute-related items:
```

hopenpgp output


```
vimja <demo@honet.ch>:
  Self-sig hash algorithms: [SHA-512]
  Preferred hash algorithms: [SHA-1, RIPEMD-160]
  Key expiration times: [1m23d20493s = Sun Jul  1 10:00:00 UTC 2018]
  Key usage flags: [[certify-keys]]
```

hopenpgp output


```
vimja <vimja@example.com>:
  Self-sig hash algorithms: [SHA-512]
  Preferred hash algorithms: [SHA-512, SHA-384, SHA-256]
  Key expiration times: [1m23d20493s = Sun Jul  1 10:00:00 UTC 2018]
  Key usage flags: [[certify-keys]]
```

hopenpgp output


```
Checking subkeys:
  one of the subkeys is encryption-capable: True
  fpr: 2A94 31D8 8D8D 6866 5F14  B5A3 F48A 34AB 5D92 BD2C
    version: v4
    timestamp: 20180508-181019
    algo/size: unknown pubkey algorithm type 22 unknown
    binding sig hash algorithms: [SHA-256]
    usage flags: [[auth]]
    embedded cross-cert: False
    cross-cert hash algorithms: [SHA-256]
```

hopenpgp output


```
fpr: 6A76 710E 2A34 74A4 D13A  278B EE41 AAB9 C4E3 FFFC
  version: v4
  timestamp: 20180508-181156
  algo/size: DSA 1024
  binding sig hash algorithms: [RIPEMD-160]
  usage flags: [[sign-data]]
  embedded cross-cert: True
  cross-cert hash algorithms: [RIPEMD-160]
```

hopenpgp output


```
fpr: DBAA F271 F8A9 8DB7 86C4  CDEF 6B3F 9652 BF6E 7FA1
  version: v4
  timestamp: 20180508-181206
  algo/size: Elgamal encrypt-only 2048
  binding sig hash algorithms: [SHA-1]
  usage flags: [[encrypt-storage, encrypt-communications]]
  embedded cross-cert: False
  cross-cert hash algorithms: [SHA-1]
```

But why ...?


```
gpg \
    --edit-key \
        F1CC6A0D12BDDDEA4C462B0D93D3F6873020F6EB
```

But why ...?


```
gpg> showpref
```

But why ...?


```
[ultimate] (1). vimja <demo@honet.ch>
     Cipher: AES, 3DES
     Digest: SHA1, RIPEMD160
     Compression: ZLIB, BZIP2, Uncompressed
     Features: MDC, Keyserver no-modify
[ultimate] (2)  vimja <vimja@example.com>
     Cipher: AES256, CAMELLIA256, TWOFISH, AES, CAMELLIA128, 3DES
     Digest: SHA512, SHA384, SHA256, SHA1
     Compression: ZLIB, ZIP, Uncompressed
     Features: MDC, Keyserver no-modify
```

But why ...?

g10/keyedit.c

```
/*
 * Show preferences of a public keyblock.
 */
static void
show_prefs (PKT_user_id * uid, PKT_signature * selfsig, int verbose) {
[...]
  for (i = any = 0; prefs[i].type; i++) {
       [...]
       if (prefs[i].value == DIGEST_ALGO_SHA1)
         sha1_seen = 1;
       [...]
    } if (!sha1_seen) {
       if (any)
         tty_printf (", ");
       tty_printf ("%s", gcry_md_algo_name (DIGEST_ALGO_SHA1));
    }
[...]
```

Questions?

Ask them now or contact me:

email

- niklaus@mykolab.ch

XMPP

- vimja@xmpp.honet.ch

Copyright

- This presentation is licensed under a Creative Commons Attribution 4.0 International License `http://creativecommons.org/licenses/by/4.0/`
  - Find the sources at `https://git.chaostreffbern.ch/vimja/OpenPGP-Keys-anstarren`
- In the creation of this presentation, I used the Feather Beamer Theme by "Lilyana Vankova" which is released under the GPLv3 license.
  - As required by the GPLv3, I make the exact sources of the theme, as used by me, including all modifications I made, available to you. You can download them from `https://gitlab.honet.ch/vimja/beamer_template`