Metadata Signing Key

All SAML Metadata documents published by ACOnet for the eduID.at service are signed with a 2048-bit sized private key that corresponds to the public key contained in the self-issued X.509 certificate reproduced below in Base64-encoded DER format:

```
-----BEGIN CERTIFICATE-----
MIID6jCCAtKgAwIBAgIJANITq5P0ezzOMA0GCSqGSIb3DQEBCwUAMIGJMQswCQYD
VQQGEwJBVDEPMA0GA1UECgwGQUNPbmV0MSMwIQYDVQQLDBpBQ09uZXQgSWRlbnRp
dHkgRmVkZXJhdGlvbjEmMCQGA1UEAwwdZWR1SUQuYXQgTWV0YWRhdGEgU2lnbmlu
ZyBLZXkxHDAaBgkqhkiG9w0BCQEWDWVkdWlkQGFjby5uZXQwHhcNMTgwNDExMTIw
MDA2WhcNMzcxMjMxMTIwMDA2WjCBiTELMAkGA1UEBhMCQVQxDzANBgNVBAoMBkFD
T25ldDEjMCEGA1UECwwaQUNPbmV0IElkZW50aXR5IEZlZGVyYXRpb24xJjAkBgNV
BAMMHWVkdUlELmF0IE1ldGFkYXRhIFNpZ25pbmcgS2V5MRwwGgYJKoZIhvcNAQkB
Fg1lZHVpZEBhY28ubmV0MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA
wSDLS25Y5spmrB8fykSqzXbTaEssR/cD12foFIDoLwN5PUEwXWWPsl8zXyoFw2nW
lrORK47Z8wjU1QlO4BcZRt8ix52GJXs9Q5xgBs4zE/Xp6hgUBa0if2PxOWoA2UTq
UgBj8L6joVkz5rBeiY7J2CkfvRw+QSzkMm+YEsmAcwpyghavKfDvYSOxubuYBacq
kwGa0J8AkDuiG3kfpydrCE5R8KTt8P65Xie5+g8YCU0mql1vCzD0O48y5dK5SHD4
PhkpG2BAayGiNUR7bDSkVElb3uybwjb0BQI+q0hu4NqpeZjTY0pTnu5oZhQW49e4
M+gKJEoSUceI3CSZ6nSfHwIDAQABo1MwUTAdBgNVHQ4EFgQUTA74FlziE6v2OKUH
HM4n/i8u8uMwHwYDVR0jBBgwFoAUTA74FlziE6v2OKUHHM4n/i8u8uMwDwYDVR0T
AQH/BAUwAwEB/zANBgkqhkiG9w0BAQsFAAOCAQEAGaJ65BAAKb8B4gxSWF2tkkFZ
7ThEftd8pdp7wTdGOb6uR1fh5wnyHs/TZeM7vJHAmqaobekFpFX0LOnDXAQ9k4kI
O+qYYNJas0YcC9n1R/ZZWkPkJpOnbzArBZq5w6gafLLEiK+nc0GX0swyPbsCL+jh
kYMi38ea4xFpzlIvvharYhr+K9X2P2um6Js/YYuB9i4lzRss5JinVIQyc3OY7u62
zqkUDQ/3Ggu2j+GPF/Ij7+jwIuxXuOB3XpvC8zxSQ/unozRTNY3TR7kvcIxyMA9I
Mo0l1Bhktwu7txYDxCUWXmhqakzLIu9OAL+vpdek1QPp4rKST0NMwMK+kETNJQ==
-----END CERTIFICATE-----
```

This certificate can also be securely downloaded via HTTPS from this location, e.g. via curl:

eduID.at SAML Metadata Signing Key

```
curl -O https://eduid.at/keys/aconet-metadata-signing.crt
```

The public key from that certificate is this (`openssl x509 -pubkey -noout -in aconet-metadata-signing.crt`):

```
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAwSDLS25Y5spmrB8fykSq
zXbTaEssR/cD12foFIDoLwN5PUEwXWWPsl8zXyoFw2nWlrORK47Z8wjU1QlO4BcZ
Rt8ix52GJXs9Q5xgBs4zE/Xp6hgUBa0if2PxOWoA2UTqUgBj8L6joVkz5rBeiY7J
2CkfvRw+QSzkMm+YEsmAcwpyghavKfDvYSOxubuYBacqkwGa0J8AkDuiG3kfpydr
CE5R8KTt8P65Xie5+g8YCU0mql1vCzD0O48y5dK5SHD4PhkpG2BAayGiNUR7bDSk
VElb3uybwjb0BQI+q0hu4NqpeZjTY0pTnu5oZhQW49e4M+gKJEoSUceI3CSZ6nSf
HwIDAQAB
-----END PUBLIC KEY-----
```

The fingerprints of that certificate are:

```
SHA-1    6B:11:58:68:AC:6D:45:BC:7E:51:9B:5D:45:22:2A:8D:85:C1:02:2F
SHA-256  0A:8B:47:D5:B9:F3:8C:61:9A:7A:99:A6:62:ED:A5:A0:43:71:B6:45:17:2E:62:2D:DB:BF:0A:E5:49:17:8C:2D
```

You can always contact ACOnet to verify the fingerprint, e.g. via telephone. To calculate the fingerprint of the downloaded certificate use the following `openssl` command (on MS-Windows you could use these binaries):

```
openssl x509 -noout -fingerprint -sha256 -in aconet-metadata-signing.crt
```

Optional Web of Trust check

For added assurance about the authenticity of the key reproduced and referenced above you may download an OpenPGP signature from one of the eduID.at operators.

The commands below will download the Metadata Signing Key (`aconet-metadata-signing.crt`), a file containing an OpenPGP-signature of it (`aconet-metadata-signing.crt.asc`) and then verify that the Metadata Signing Key has in fact been signed by that OpenPGP-key:

```
$ curl -O "https://eduid.at/keys/aconet-metadata-signing.crt{,.asc}"
$ gpg --verify aconet-metadata-signing.crt.asc aconet-metadata-signing.crt
gpg: Signature made Wed 11 Apr 2018 03:35:10 PM CEST
gpg:                using RSA key 336A59F993C634AD50D6DBE2AFF60721F868B59A
gpg: Good signature from "Peter Schober <peter.schober@univie.ac.at>" [full]
gpg:                 aka "Peter Schober <peter@aco.net>" [full]
```

How much additional trust you derive from that procedure depends solely on the trust you put into the Web of trust signatures on the OpenPGP key used to sign that file, i.e. whether you believe the people who have signed the eduID.at operator's key to be legit thereby testifying to the authenticity of the identity represented in that OpenPGP key.