OpenSSL

- show contents of a PEM encoded certificate: `openssl x509 -in <cert>.pem -text`
- extract public key from certificate: `openssl x509 -pubkey -noout -in cert.pem > pubkey.pem`

ECDSA

- list EC curves: `openssl ecparam -list_curves`
- generate ECDSA key: `openssl ecparam -name brainpoolP256r1 -genkey -noout -out <keyfile-priv.pem>`
- write public key: `openssl ec -in <keyfile-priv.pem> -pubout -out <keyfile-pub.pem>`
- show ECDSA key: `openssl ec -in <keyfile-priv.pem> -text -noout`
- show digest: `openssl dgst -sha256 -sign <keyfile-priv.pem> -hex ectest.txt`
- sign file: `openssl dgst -sha256 -sign <keyfile-priv.pem> ectest.txt > ecdsa256sig.bin`
- verify file: `openssl dgst -sha256 -verify <keyfile-pub.pem> -signature ecdsa256sig.bin ectest.txt`
- SHA-256 Digest: `sha256sum ectest.txt > sha256.hex; xxd -r -p sha256.hex > sha256.bin`

From:
https://wiki.rho62.de/ - **rho62 Wiki**

Permanent link:
https://wiki.rho62.de/doku.php?id=linux:utilities:openssl

Last update: **2023/11/13 11:06**