



# IT-Sicherheit

## 05 Open SSL



**Gerrit Kalkbrenner**  
**Gerrit.Kalkbrenner@hwr-berlin.de**



## Bibliotheken für Krypto-Software

- Proprietäre Implementierungen
- Bestandteil des Betriebssystems
- Hardware (TPM)

Weiterhin → OpenSSL

## Was ist es?

- robust
  - commercial-grade,
  - full-featured
  - general-purpose
  - Für Kryptographie und sichere Kommunikation.
- 
- command line application
  - kryptographische Funktionen
  - Generierung von Schlüsseln and Zertifikate



## Wo kommt es her?

- OpenSSL is komplett open source.
- Versionen ab 3.6 stehen unter der Apache v2 license.
- <https://www.openssl.org/source>
- Vorkompiliert für Windows:  
<https://www.heise.de/download/product/win32-openssl-47316/download>



# Arbeiten mit der Konsole

```
Win64 OpenSSL Command Prompt

OpenSSL 3.6.0 1 Oct 2025 (Library: OpenSSL 3.6.0 1 Oct 2025)
built on: Wed Oct  8 20:29:58 2025 UTC
platform: VC-WIN64A
options: bn(64,64)
compiler: cl /Z7 /Fdssl_static.pdb /Gs0 /GF /Gy /MD /W3 /wd4090 /nologo /O2 -DL_ENDIAN -DOPENSSL_PIC -D"OPEN
SSL_BUILDING_OPENSSL" -D"OPENSSL_SYS_WIN32" -D"WIN32_LEAN_AND_MEAN" -D"UNICODE" -D"_UNICODE" -D"CRT_SECURE_NO
_DEPRECATED" -D"_WINSOCK_DEPRECATED_NO_WARNINGS" -D"NDEBUG" -D_WINSOCK_DEPRECATED_NO_WARNINGS -D_WIN32_WINNT=0x
0502
OPENSSLDIR: "C:\Program Files\Common Files\SSL"
ENGINESDIR: "C:\Program Files\OpenSSL\lib\engines-3"
MODULESDIR: "C:\Program Files\OpenSSL\lib\openssl-modules"
Seeding source: os-specific
CPUINFO: OPENSSL_ia32cap=0x029ae3ffffebffff:0x0000000000000000:0x000000009c000000:0x0000000000000000:0x00000000
00000000

C:\Users\kalkbrenner>
```



## sha256

```
D:\ssl>openssl dgst -sha256 name.txt
```

```
SHA2-256(name.txt)=  
99671587e0856ec3a860511aa979e863d90dc8ee  
02b89ab2cce3077f242e106f
```



# AES

```
openssl enc -e -aes256 -in name.txt -out name.aes
```

```
openssl enc -d -aes256 -out name2.txt -in name.aes
```



## openssl enc -ciphers

-aes-128-cbc	-aes-128-cfb	-aes-128-cfb1
-aes-128-cfb8	-aes-128-ctr	-aes-128-ecb
-aes-128-ofb	-aes-192-cbc	-aes-192-cfb
-aes-192-cfb1	-aes-192-cfb8	-aes-192-ctr
-aes-192-ecb	-aes-192-ofb	-aes-256-cbc
-aes-256-cfb	-aes-256-cfb1	-aes-256-cfb8
-aes-256-ctr	-aes-256-ecb	-aes-256-ofb

...