

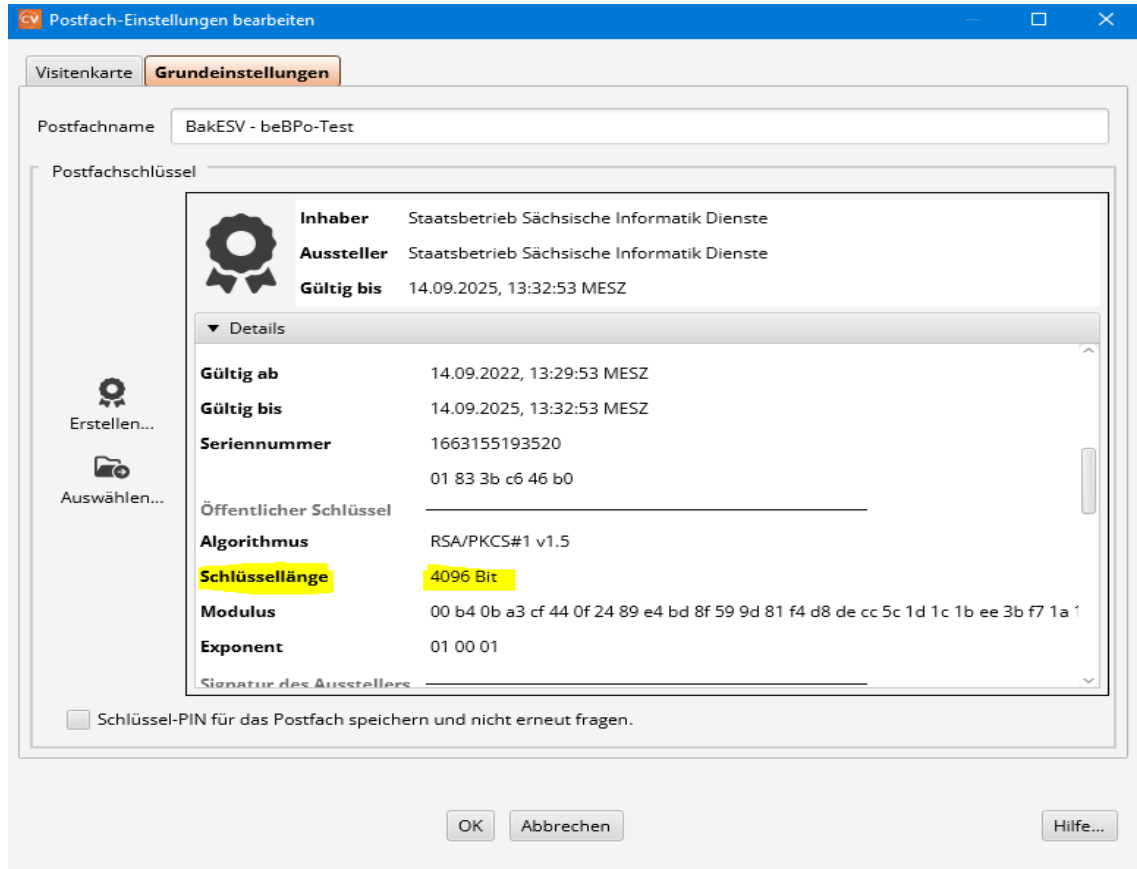
# Anzeigen des Zertifikat-Inhalts zur Ermittlung der RSA-Schlüssellänge

## Inhalt

- Anzeigen des Zertifikat-Inhalts zur Ermittlung der RSA-Schlüssellänge.....1
  - Variante 1: mittels OSCI-Client COM Vibilia.....1
  - Variante 2: mittels keytool.exe (Bestandteil von Java).....2
  - Variante 3: mittels Windows Zertifikatsanzeige .....3
  - Variante 4: mittels OpenSSL unter Linux.....4

## Variante 1: mittels OSCI-Client COM Vibilia

Menü: [Postfach->Bearbeiten](#) dann auf [Register Grundeinstellungen](#). In dem rechten Fenster suchen sie den Eintrag **Schlüssellänge**. Hier können sie auch über [Erstellen](#) ein neues Zertifikat generieren und in das Postfach einbinden.



## Variante 2: mittels keytool.exe (Bestandteil von Java)

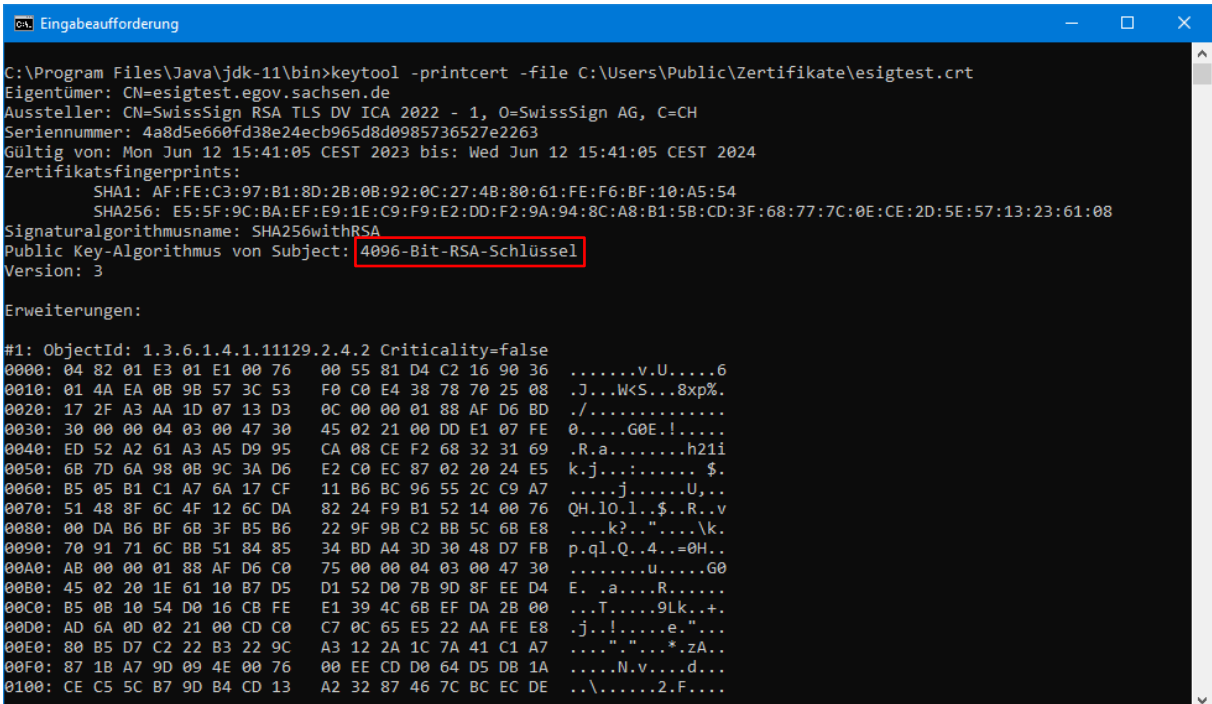
Wenn Java auf dem PC installiert ist, kann mit Hilfe des Kommandozeilen-Tools **keytool.exe** der Inhalt einer Zertifikatsdatei angezeigt werden. In diese Informationen ist auch die Länge des verwendeten RSA-Schlüssels (Key-Algorithmus) enthalten.

Syntax:

```
[LW]:\[Pfad_zum_Java-Ordner]\keytool.exe -printcert -file  
[LW]:\[Pfad]\[Zertifikatsdatei]
```

Beispiel:

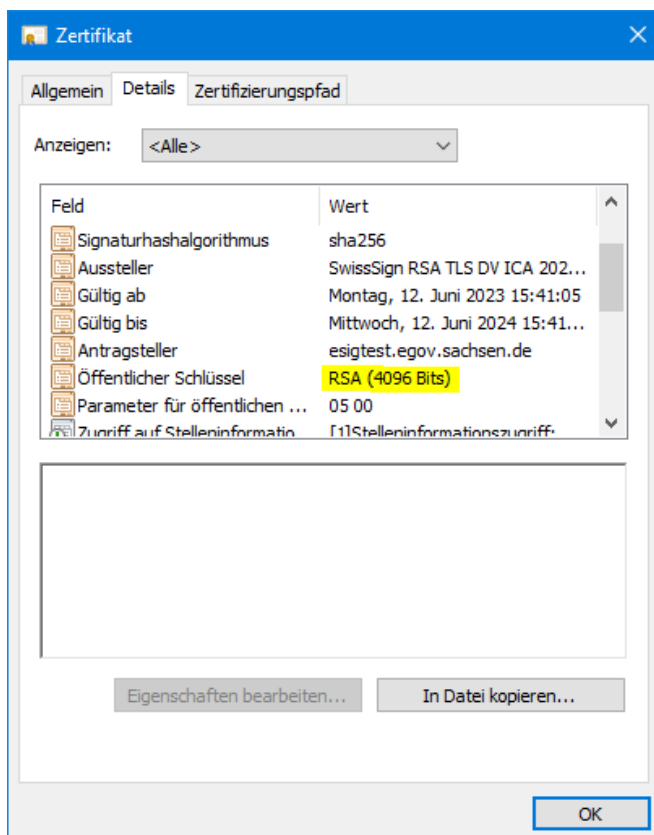
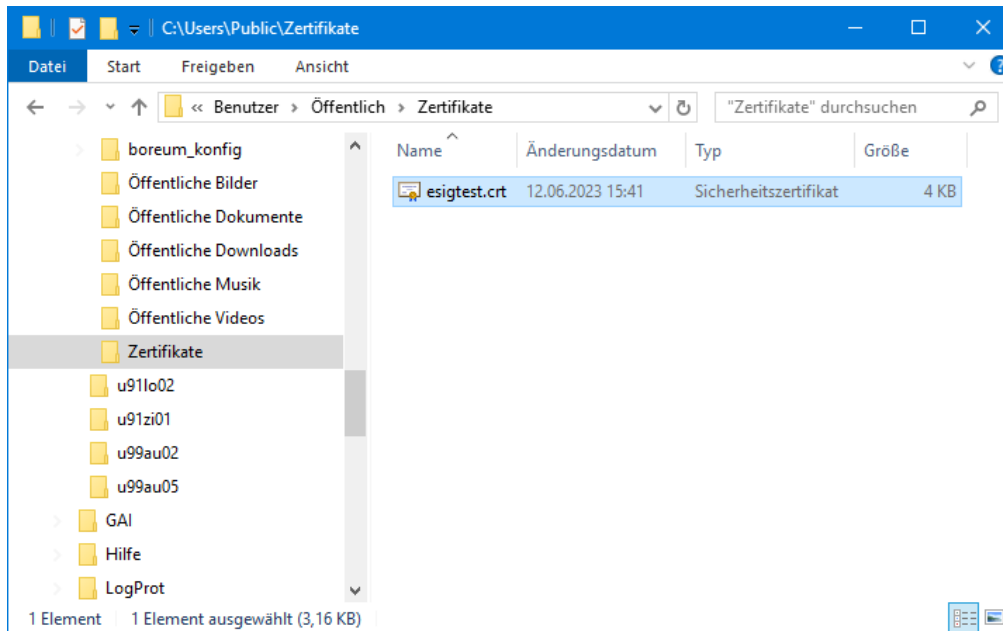
```
C:\Program Files\Java\jdk-11\bin\keytool.exe -printcert -file  
C:\Users\Public\Zertifikate\esigtest.crt
```



```
Eingabeaufforderung  
C:\Program Files\Java\jdk-11\bin>keytool -printcert -file C:\Users\Public\Zertifikate\esigtest.crt  
Eigentümer: CN=esigtest.egov.sachsen.de  
Aussteller: CN=SwissSign RSA TLS DV ICA 2022 - 1, O=SwissSign AG, C=CH  
Seriennummer: 4a8d5e660fd38e24ecb965d8d0985736527e2263  
Gültig von: Mon Jun 12 15:41:05 CEST 2023 bis: Wed Jun 12 15:41:05 CEST 2024  
Zertifikatsfingerprints:  
SHA1: AF:FE:C3:97:B1:8D:2B:0B:92:0C:27:4B:80:61:FE:F6:BF:10:A5:54  
SHA256: E5:5F:9C:BA:EF:E9:1E:C9:F9:E2:DD:F2:9A:94:8C:A8:B1:5B:CD:3F:68:77:7C:0E:CE:2D:5E:57:13:23:61:08  
Signaturalgorithmusname: SHA256withRSA  
Public Key-Algorithmus von Subject: 4096-Bit-RSA-Schlüssel  
Version: 3  
  
Erweiterungen:  
#1: ObjectId: 1.3.6.1.4.1.11129.2.4.2 Criticality=false  
0000: 04 82 01 E3 01 E1 00 76 00 55 81 D4 C2 16 90 36 .....v.U.....6  
0010: 01 4A EA 0B 9B 57 3C 53 F0 C0 E4 38 78 70 25 08 .J..WKS...8xp%.  
0020: 17 2F A3 AA 1D 07 13 D3 0C 00 00 01 88 AF D6 BD ./.....  
0030: 30 00 00 04 03 00 47 30 45 02 21 00 DD E1 07 FE 0.....G0E.!....  
0040: ED 52 A2 61 A3 A5 D9 95 CA 08 CE F2 68 32 31 69 .R.a.....h21i  
0050: 68 7D 6A 98 08 9C 3A D6 E2 C0 EC 87 02 20 24 E5 k.j.....$.  
0060: B5 05 B1 C1 A7 6A 17 CF 11 B6 BC 96 55 2C C9 A7 .....j.....U,..  
0070: 51 48 8F 6C 4F 12 6C DA 82 24 F9 B1 52 14 00 76 QH.10.l.$.R.v  
0080: 00 DA B6 BF 6B 3F B5 B6 22 9F 9B C2 BB 5C 6B E8 ....k?..."..k.  
0090: 70 91 71 6C BB 51 84 85 34 BD A4 3D 30 48 D7 FB p.q1.Q..4..=0H..  
00A0: AB 00 00 01 88 AF D6 C0 75 00 00 04 03 00 47 30 .....u.....G0  
00B0: 45 02 20 1E 61 10 B7 D5 D1 52 D0 7B 9D 8F EE D4 E. .a....R.....  
00C0: B5 0B 10 54 D0 16 CB FE E1 39 4C 6B EF DA 2B 00 ...T....9Lk..+.  
00D0: AD 6A 0D 02 21 00 CD C0 C7 0C 65 E5 22 AA FE E8 .j.!.....e."...  
00E0: 80 B5 D7 C2 22 B3 22 9C A3 12 2A 1C 7A 41 C1 A7 .....".*zA..  
00F0: 87 1B A7 9D 09 4E 00 76 00 EE CD D0 64 D5 DB 1A .....N.v....d...  
0100: CE C5 5C B7 9D B4 CD 13 A2 32 87 46 7C BC EC DE ..\.....2.F....
```

### Variante 3: mittels Windows Zertifikatsanzeige

Der Inhalt eines Zertifikats kann mit Hilfe der Windows-Zertifikatsanzeige angezeigt werden. Das erfolgt durch Doppelklick mit der linken Maustaste auf die jeweilige Zertifikatsdatei. In der Registerkarte „Details“ kann im Feld „Öffentlicher Schlüssel“ die RSA-Schlüssellänge abgelesen werden. Der Ablageort der Zertifikatsdatei muss bekannt sein.



## Variante 4: mittels OpenSSL unter Linux

1. Klicken Sie mit der rechten Maustaste auf den Desktop und wählen Sie "Terminal öffnen".
2. Geben Sie den Befehl `sudo openssl x509 -noout -text -in "/etc/sslzertifikat/beispiel.crt"` ein. Ersetzen Sie `/etc/sslzertifikat/beispiel.crt` durch den Speicherort Ihres Zertifikates.
3. Sie bekommen nun Ihr Zertifikat mit allen wichtigen Parametern wie etwa den Daten des Ausstellers, Gültigkeit, Schlüssellänge... etc. angezeigt.

Terminal