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.

🔯 Postfach-Einstell	ungen bearbe	eiten			×
Visitenkarte Gru	undeinstellu	Ingen			
Postfachname	BakESV - bel	BPo-Test			
Postfachschlüss	el				
		Inhaber	Staatsbetrieb Sächsische Informatik Dienste		
		Aussteller	Staatsbetrieb Sächsische Informatik Dienste		
		Gültig bis	14.09.2025, 13:32:53 MESZ		
	▼ Details	;			
	Gültig ab		14.09.2022, 13:29:53 MESZ		^
<u> </u>	Gültig bis		14.09.2025, 13:32:53 MESZ		
Erstellen	Seriennur	mmer	1663155193520		
			01 83 3b c6 46 b0		
Auswählen	Öffentlich	ner Schlüssel			
	Algorithm	nus	RSA/PKCS#1 v1.5		
	Schlüssell	länge	4096 Bit		
	Modulus		00 b4 0b a3 cf 44 0f 24 89 e4 bd 8f 59 9d 81 f4 d8 de cc 5c 1d 1c 1b	ee 3b f7 1a	a 1
	Exponent		01 00 01		
	Signatur	des Aussteller	· · · · · · · · · · · · · · · · · · ·		~
Schlüssel-	PIN für das P	ostfach speich	ern und nicht erneut fragen.		
				_	
			OK Abbrechen	н	lilfe

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
```

Cos 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, 0=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: Signaturalgorithmusname: SHA256withRSA Public Key-Algorithmus von Subject: 4096-Bit-RSA-Schlüssel Version: 3	51:0	8	^
Erweiterungen:			
<pre>#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 36v.U6 0010: 01 4A EA 0B 98 57 3C 53 F0 C0 E4 38 78 70 25 08 .JW<s8xp%. 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 060E.! 0040: ED 52 A2 61 A3 A5 D9 95 CA 08 CE F2 68 32 31 69 .R.ah211 0050: 68 7D 6A 98 08 9C 3A D6 E2 C0 EC 87 02 20 24 E5 k.j\$. 0060: 85 05 B1 C1 A7 6A 17 CF 11 B6 BC 96 55 2C C9 A7jU\$. 0070: 51 48 8F 6C 4F 12 6C DA 82 24 F9 B1 52 14 00 76 QH.10.1.\$.R.v 00880: 00 DA 86 BF 6B 3F B5 B6 22 9F 9B C2 B8 5C 6B E8k?."\k. 00800: 70 91 71 6C B8 51 84 85 34 BD A4 3D 30 48 D7 FB p.ql.Q4.=0H 004A2 AB 00 00 18 8 AF D6 C0 75 00 00 44 03 00 47 30</s8xp%. </pre>			

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.

Termina	й	t _t	De 📧)	4)) 13:24 🔅
	See 💿 malk@malk-VirtualBox: ~			
0	maik@maik-VirtualBox:-\$ sudo openssl x509 -noout -text -in "/etc/sslzertifikat/beispiel.crt" [sudo] Passwort für maik:			
	Certificate:			
	Data:			
Section 2.	Version: 1 (0x0)			
	Serial Number: 94401506441152/5336 (0X830220Tea88aa/e48)			
	Signature Algorithm: SnazsowithKSAEncryption			
	Validitu			
	Not Reform: Feb 22 11:58:54 2016 CMT			
	Not After : Feb 21 11:58:54 2017 GMT			
	Subject: C=DE. ST=Niedersachsen, L=Hannover, O=Chip, CN=testserver.de			
	Subject Public Key Info:			
1	Public Key Algorithm: rsaEncryption			
	Public-Key: (2048 bit)			
	Modulus:			
1	00:e1:e4:fa:ee:c6:51:99:26:ef:e7:b1:1f:40:e8:			
	9c:2a:f1:ff:bd:9c:b7:8a:85:06:10:53:49:c8:06:			
and then	26:9e:Bf:B3:36:D8:2f:14:4e:46:d7:2e:f9:d7:37:			
A	T4:a0:/1:02:3a:32:04:a/:44:/a:06:00:D0:D5:08:			
	70:94:D0:a2:e0:91:76:90:90:40:05:e0:75:56:81:			
e 61	u4.cu.20.ou.03.10.102.70.41.04.104.00.36.08.72.40.			
21	78 • 66 • 53 • 69 • 68 • 64 • 61 • 64 • 33 • 64 • 67 • 68 • 68 •			
	b3;be;bb;00:5c;c3:10:3e:1c;5e:25;dc;f0:b4:00;			
	01:a2:c6:82:ed:20:40:55:01:58:7d:fc:ee:d2:ba:			
	35:6e:76:8e:27:27:f0:9e:85:46:a1:3e:96:4f:ec:			
100	4d:2d:6a:b9:d7:d4:0b:27:9f:3c:d4:db:a3:51:6f:			J.
	e3:db:5e:37:e9:4b:69:70:c6:72:f8:35:4f:49:05:			
· P_ ·	67:c4:74:80:d9:90:c2:18:3f:c7:31:a4:92:50:e1:			
	da:4c:c5:12:57:d1:9a:a8:de:c9:18:3a:72:73:cd:			
	5e:55:6d:9a:4a:4d:00:87:d3:78:fc:7f:77:c8:44:			
• (A)	87:55:db:95:56:59:97:52:t4:2d:eb:16:t5:t0:b1:			
	Exponent: 0553/ (WXI0001)			
	Signature Algoritim: SnazowitikSAEncryption			
Served a	3 - 3 - 5 - 6 - 1 - 1 - 5			
	Papierkorb			
and the second s				