VĚSTNÍK

MINISTERSTVA VNITRA

Ročník 2008 **V Praze dne 3. března 2008** **Částka 24**

O B S A H

i. Seznam atestačních středisek

Ministerstvo vnitra zveřejňuje seznam atestačních středisek, kterým bylo v souladu se zákonem č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, vydáno pověření k výkonu atestací a toto pověření je dosud platné. Zároveň musí mít atestační středisko k provádění atestací, v souladu s § 6b zákona č. 365/2000 Sb., schválené **„postupy atestačního střediska při provádění atestací"** (schválené postupy). Bez schválených postupů nemůže atestační středisko provádět atestace, na jejichž provedení uzavře smlouvu po 1. 1. 2007.

V této tabulce uvádíme atestační střediska, která mají v současnosti platné pověření k výkonu atestací a zároveň také schválené postupy. Řazení je uvedeno podle přidělených registračních čísel.

Registrační číslo	Atestační středisko	IČ	Platnost pověření do	Schválené postupy od
6	**RELSIE spol. s r.o.**	62417339	**01. 01. 2009**	**9. 2. 2007**
7	**Equica, a.s.**	26490951	**01. 01. 2009**	**21. 2. 2007**
12	**secunet s.r.o.**	26478650	**01. 01. 2009**	**16. 5. 2007**
14	**Elektrotechnický zkušební ústav, s.p.**	00001481	**01. 01. 2009**	**6. 4. 2007**
15	**BDO IT a.s.**	25056646	**01. 01. 2009**	**7. 5. 2007**
16	**ADA, s. r. o.**	46992430	**01. 01. 2009**	**17. 5. 2007**

ii. Přehled udělených atestů informačním systémům veřejné správy

Ministerstvo vnitra zveřejňuje ve smyslu § 4 odst. 2, písm. h) zákona č. 365/2000 Sb. přehled udělených atestů.

Předmětem atestace podle novely zákona č. 365/2000 Sb., o informačních systémech veřejné správy je:

- dlouhodobé řízení informačních systémů veřejné správy, tj. informační koncepce a provozní dokumentace – souhrnně atestace dlouhodobého řízení,
- způsobilost k realizaci vazeb informačního systému veřejné správy s jinými informačními systémy prostřednictvím referenčního rozhraní.

Udělené atesty dlouhodobého řízení

- Statutární město Kladno
- Ministerstvo životního prostředí
- Moravskoslezský kraj – Krajský úřad

Udělené atesty způsobilosti k realizaci vazeb prostřednictvím referenčního rozhraní

Nebyl udělen žádný atest.

Název a sídlo atestačního střediska, IČ	Equica, a.s. IČ: 26490951 Rubeška 215/1 190 00 Praha 9
Název a sídlo žadatele o atestaci, IČ	Statutární město Kladno IČ: 234516 nám. Starosty Pavla 44 272 52 Kladno
Předmět atestace	**Dlouhodobé řízení ISVS**
Datum vydání atestu	14.11.2007
Výsledek zkoušky	SPLŇUJE
Datum provedení další zkoušky	1.11.2012

Název a sídlo atestačního střediska, IČ	Equica, a.s. IČ: 26490951 Rubeška 215/1 190 00 Praha 9
Název a sídlo žadatele o atestaci, IČ	Moravskoslezský kraj – Krajský úřad IČ: 70890692 28. října 117 702 18 Ostrava
Předmět atestace	**Dlouhodobé řízení ISVS**
Datum vydání atestu	26.11.2007
Výsledek zkoušky	SPLŇUJE
Datum provedení další zkoušky	1.11.2012

Název a sídlo atestačního střediska, IČ	Equica, a.s. IČ: 26490951 Rubeška 215/1 190 00 Praha 9
Název a sídlo žadatele o atestaci, IČ	Ministerstvo životního prostředí IČ: 00164801 Vršovická 1442/65 100 10 Praha 10
Předmět atestace	**Dlouhodobé řízení ISVS**
Datum vydání atestu	28.11.2007
Výsledek zkoušky	SPLŇUJE
Datum provedení další zkoušky	1.11.2012

iii. Účet zřízený za účelem placení správních poplatků v souvislosti s řízením podle zákona č. 365/2000 Sb.

Za účelem placení správních poplatků stanovených zákonem č. 634/2004, o správních poplatcích, ve znění pozdějších předpisů, v souvislosti s řízeními podle zákona č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, zřídilo Ministerstvo vnitra České republiky účet u České národní banky.

- **Podání žádosti o udělení pověření k provádění akreditace**
- **Podání žádosti o udělení pověření k provádění atestací**
- **Podání žádosti o udělení souhlasu se změnou atestačních podmínek**

část I položka 22 písm. i) sazebníku správních poplatků

účet číslo **3711-8920071/0710**, VS: **IČ**, KS: **0308**, SS: **neuvádět**

správní poplatek **Kč 10 000**

iv. Výsledky ověření kvalifikovaných systémových certifikátů, které používá kvalifikovaný poskytovatel certifikačních služeb

Ministerstvo vnitra zveřejňuje v souladu s § 9 odst. 2, písm. e) a § 6 odst. 2 zákona č. 227/2000 Sb.

Ministerstvo vnitra ověřilo ve smyslu písm. d) odst. 2 § 9 zákona č. 227/2000 Sb., kvalifikované certifikáty, resp. kvalifikované systémové certifikáty poskytovatelů certifikačních služeb[1)] a zveřejňuje údaje platných kvalifikovaných, resp. kvalifikovaných systémových certifikátů následujících subjektů:

Poř. číslo	**Ověření kvalifikovaného certifikátu poskytovatele**			
	Subjekt		Adresa	
1.	**První certifikační autorita, a. s., identifikační č. 26 43 93 95**		**Podvinný mlýn 2178/6, PSČ 190 00 Praha 9**	
Výsledky ověření:				
A.	Jméno	**RootCERT_Qica.pem**		Délka: **2265 byte**
	Formát certifikátu		**Otisk**	
	PEM	SHA-1	**4BFB ED36 68FC 2B0A B729 8EC0 53B5 3649 6E15 0AAE**	
		MD5	**297C 49A7 B63C B15A F3B7 0F45 2D3B 5132**	
B.	Jméno	**RootCERT_Qica.pem**		Délka: **1630 byte**
	Formát certifikátu		**Otisk**	
	DER	SHA-1	**6E32 893F 22A5 E1CD 9CD6 32E4 10E2 76FF 14B7 66BE**	
		MD5	**C3F3 5AB5 24C7 9276 634B 4DB4 E86A FE57**	
C.	Jméno	**RootCERT_Qica.txt**		Délka: **6256 byte**
	Formát certifikátu		**Otisk**	
	TXT	SHA-1	**AC46 FB40 E929 F12D 758A 0B8E 0192 516B 1B65 6C8A**	
		MD5	**5EAC 0082 F5F5 9E3D EAB4 0FE6 27BE 5ED2**	

[1)] Pojem „kvalifikovaný systémový certifikát" byl zaveden novelou zákona o elektronickém podpisu účinnou od 26. července 2004.

Poř. číslo	Ověření kvalifikovaného systémového certifikátu poskytovatele			
	Subjekt		Adresa	
2.	**První certifikační autorita, a.s., identifikační č. 26 43 93 95**		**Podvinný mlýn 2178/6, PSČ 190 00 Praha 9**	
Vzhledem k tomu, že došlo k novelizaci zákona o elektronickém podpisu č. 227/2000 Sb., vznikla poskytovateli povinnost vydat kořenový kvalifikovaný systémový certifikát, na jehož základě označuje vydané kvalifikované certifikáty a seznamy certifikátů, které byly zneplatněny. Certifikát má **platnost od 1.6.2005** a **První certifikační autorita, a.s. jej začala používat dnem 1. 7. 2005.**				
Výsledky ověření:				
A.	Jméno	**RootCERT_Qican.pem**		Délka: **1550 byte**
	Formát certifikátu:		**Otisk:**	
	PEM	SHA-1	0E3B C53F F3B7 F040 AC91 4733 4FD5 7D11 6E82 5628	
		MD5	9128 E8BB F5F7 A72E 7D2D 7702 6C92 4395	
B.	Jméno	**RootCERT Qican.der**		Délka: **1084 byte**
	Formát certifikátu		**Otisk**	
	DER	SHA-1	9866 58B9 4448 A2A0 85F9 7B06 0F85 10AC D4AA D4B5	
		MD5	5FF2 D99B 7E64 EBF4 A1A5 5EF2 D45D A293	
C.	Jméno	**RootCERT Qican.txt**		Délka: **4931 byte**
	Formát certifikátu		**Otisk**	
	TXT	SHA-1	E797 543F 6ECE 924C 9FAA 3D80 C7DB B896 5F4F CFD5	
		MD5	AB83 9563 DA4A 1BA7 B941 22CE 671E A9D1	

Poř. číslo	Ověření kvalifikovaného systémového certifikátu poskytovatele			
	Subjekt		Adresa	
3.	**Česká pošta, s.p. identifikační číslo 47 11 49 83**		**Olšanská 38/9, PSČ 225 99 Praha 3**	
Výsledky ověření				
A.	Jméno	**postsignum_qca_root.pem**		Délka: **2199 byte**
	Formát certifikátu		**Otisk**	
	PEM	SHA-1	**3BCB 0BEA EB9E 95BB DFD3 AC96 9102 066B F49D 4C37**	
		MD5	**4D3A 8498 3AE6 B114 3643 90EA 66E4 3377**	
B.	Jméno	**postsignum_qca_root.der**		Délka: **1582 byte**
	Formát certifikátu		**Otisk**	
	DER	SHA-1	**AF3B 84BA 3437 63BB BE03 6C76 5A44 119E 48B5 2D34**	
		MD5	**385F 2FBD BC06 F7B0 28ED F21C 86AC 2E05**	

C.	Jméno	**postsignum_qca_root.txt**		Délka: **4057 byte**
	Formát certifikátu		**Otisk**	
	TXT	SHA-1	**A50D C93D 29D1 47E3 F804 555B 52C8 C9B6 21AA 8877**	
		MD5	**4F99 D35F 3134 F1D2 64FA 4FB0 AA39 B0E7**	

Poř. číslo	**Ověření kvalifikovaného systémového certifikátu poskytovatele**			
	Subjekt		Adresa	
4.	**Česká pošta, s.p. identifikační číslo 47 11 49 83**		**Olšanská 38/9, PSČ 225 99 Praha 3**	
Výsledky ověření				
A.	Jméno	**postsignum_qca_sub.pem**		Délka: **2204 byte**
	Formát certifikátu		**Otisk**	
	PEM	SHA-1	**F003 37C6 474C 06BD 099C F863 5D5C 8DA7 FABD 76EB**	
		MD5	**3F1B C084 80B0 7B70 8B74 B94E 0F51 D9F4**	
B.	Jméno	**postsignum_qca_sub.der**		Délka: **1586 byte**
	Formát certifikátu		**Otisk**	
	DER	SHA-1	**1BDB 87C4 8102 977C A277 65E9 CCA4 1424 6C6D 88A2**	
		MD5	**5ACB F806 A17D B75D 93AD BB9A 4E54 EFB8**	
C.	Jméno	**postsignum_qca_sub.txt**		Délka: **4063 byte**
	Formát certifikátu		**Otisk**	
	TXT	SHA-1	**7E2D F680 722F E209 2B08 A744 4166 87B6 C4C4 B0C0**	
		MD5	**CCAD 9144 6635 5071 5C44 19BA 56AC D7F9**	

Poř. číslo	**Ověření kvalifikovaného systémového certifikátu poskytovatele**			
	Subjekt		Adresa	
7.	**eIdentity a.s. identifikační číslo 27 11 24 89**		**Vinohradská 184/2396 PSČ 130 00 Praha 3**	
Výsledky ověření				
A.	Jméno	**rca.pem**		Délka: **2382 byte**
	Formát certifikátu		**Otisk**	
	PEM	SHA-1	**6D8D 2C6F A10D FF7C 799D A42C 52AD DFD0 8620 D8CD**	
		MD5	**D5C7 340D 88CF 688F 1480 E7B6 4795 F42C**	
B.	Jméno	**rca.der**		Délka: **1701 byte**

	Formát certifikátu		**Otisk**
	DER	SHA-1	**62A6 9CFB 4E93 1829 7E83 F94B FFEB DD1A E5F3 1E3A**
		MD5	**1C14 914D 9C8E 9F27 477D 7927 4829 5D7E**
C.	Jméno	**rca.cp1250.txt**	Délka: **6556 byte**
	Formát certifikátu		**Otisk**
	TXT	SHA-1	**2F37 0C8F 4159 94E0 216C 24F8 6B31 C7B6 039B 199B**
		MD5	**A0F7 F938 3C16 C98D 288F 4E8E 9CB2 9FEA**

Poř. číslo	**Ověření kvalifikovaného systémového certifikátu poskytovatele**	
	Subjekt	Adresa
8.	**eIdentity a.s.** **identifikační číslo 27 11 24 89**	**Vinohradská 184/2396** **PSČ 130 00 Praha 3**

Výsledky ověření			
A.	Jméno	**aca.pem**	Délka: **2752 byte**
	Formát certifikátu		**Otisk**
	PEM	SHA-1	**455A 2841 7727 8AF2 54C3 9BE0 D5D7 FBDD 896F BB9B**
		MD5	**162B 7C39 2F69 3061 E6FD 90C0 2380 5D4B**
B.	Jméno	**aca.der**	Délka: **1970 byte**
	Formát certifikátu		**Otisk**
	DER	SHA-1	**CBC5 8D41 87F2 4206 955E 6A8B 28AA 2E80 D4D8 E3FD**
		MD5	**730C EA1A D77C 87D8 9F0C FE76 F868 0A15**
C.	Jméno	**aca.cp1250.txt**	Délka: **7094 byte**
	Formát certifikátu		**Otisk**
	TXT	SHA-1	**EE6C C356 B6AF 1125 3BCD 7D2E FDE9 AAFC CC46 8027**
		MD5	**68B6 19D7 3ABB B13D DEE8 0AC6 D8C8 21C5**

Poř. číslo	**Ověření kvalifikovaného systémového certifikátu poskytovatele**	
	Subjekt	Adresa
9.	**První certifikační autorita, a.s.** **identifikační číslo 26 43 93 95**	Podvinný mlýn 2178/6, PSČ 190 00 Praha 9
Kvalifikovaný systémový certifikát, na jehož základě jsou označována kvalifikovaná časová razítka, v souladu se zákonem č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu), ve znění pozdějších předpisů.		

Certifikát má **platnost od 1.2.2006**.			
Výsledky ověření			
A.	Jméno	**qtsa.pem**	Délka: **1840 byte**
	Formát certifikátu		**Otisk**
	PEM	SHA-1	**FF22 28C6 7481 517F 414D 0C74 B494 AE08 804C 20F1**
		MD5	**5EA1 F4A7 121D 8E26 AA52 EDA8 3199 7A3B**
B.	Jméno	**qtsa.der**	Délka: **1296 byte**
	Formát certifikátu		**Otisk**
	DER	SHA-1	**9EFD B496 DF7A 9F02 0370 119F 9E1C 8398 7DE9 F46C**
		MD5	**12B7 132C A653 6313 E656 EEC4 D315 743D**
C.	Jméno	**qtsa.txt**	Délka: **5644 byte**
	Formát certifikátu		**Otisk**
	TXT	SHA-1	**A2E5 592D 9051 D008 1D5D D3AF 8461 DF3F A939 E4B2**
		MD5	**1C20 2939 E5F7 3035 EE25 665D 6541 AAED**

Poř. číslo	**Ověření kvalifikovaného systémového certifikátu poskytovatele**	
	Subjekt	Adresa
10.	**První certifikační autorita, a.s.** **identifikační číslo 26 43 93 95**	Podvinný mlýn 2178/6, PSČ 190 00 Praha 9
Kvalifikovaný systémový certifikát, na jehož základě jsou označována kvalifikovaná časová razítka, v souladu se zákonem č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu), ve znění pozdějších předpisů. Certifikát má **platnost od 4.10.2007**.		
Výsledky ověření		

A.	Jméno	**qtsa1.pem**	Délka: **1813 byte**
	Formát certifikátu		**Otisk**
	PEM	SHA-1	**131D AD4E FBA8 7727 4B53 3586 8857 54B0 5FC5 8E9C**
		MD5	**CB36 700C BAF4 7CEB B22B AFA5 0A8D 0A85**
B.	Jméno	**qtsa1.der**	Délka: **1294 byte**
	Formát certifikátu		**Otisk**
	DER	SHA-1	**0BF6 BC28 7E42 1328 0C79 DB29 C3DC 849D 9FC8 FCCE**
		MD5	**0758 724A 31B8 F873 3F23 101D 2D25 927F**

C.	Jméno	**qtsa1.txt**	Délka: **3812 byte**
	Formát certifikátu		**Otisk**
	TXT	SHA-1	**BAA3 F6E3 D69E 239E 33C4 EC28 3A5D 6E52 81DD 6112**
		MD5	**A156 7116 4CE9 3F20 1A64 AE25 8FA2 2C1A**

Poznámka:

1. Uvedené otisky byly počítány z obsahu celého souboru, a to podle následujících standardů:
   - **SHA-1** (National Institute of Standards and Technology, *Secure Hash Standar*d, Federal Information Processing Standards Publication 180-1, April 17, 1995)
     a
   - **MD5** (Request for Comments: 1321, The MD5 Message-Digest Algorithm, R. Rivest, MIT Laboratory for Computer Science and RSA Data Security, Inc., April 1992).
2. Tyto zveřejněné otisky slouží k tomu, aby před instalací kvalifikovaného systémového certifikátu, případně kvalifikovaného certifikátu akreditovaného poskytovatele certifikačních služeb byla možnost porovnáním otisků zjistit, zda:
   - kvalifikovaný systémový certifikát, případně kvalifikovaný certifikát byl skutečně ověřen Ministerstvem vnitra,
   - zda kvalifikovaný systémový certifikát, případně kvalifikovaný certifikát byl vydán příslušným akreditovaným poskytovatelem certifikačních služeb,
   - se jedná o kvalifikovaný systémový certifikát, případně kvalifikovaný certifikát, kdy k němu odpovídající data pro vytváření elektronických značek, resp. elektronických podpisů daného akreditovaného poskytovatele certifikačních služeb, jsou určena pro označování, resp. podepisování kvalifikovaných certifikátů, kvalifikovaných systémových certifikátů, seznamu kvalifikovaných certifikátů, které byly zneplatněny a seznamu kvalifikovaných systémových certifikátů, které byly zneplatněny.

Aktuální výsledky ověření otisků (hash SHA-1 a MD5) různých formátů kvalifikovaných certifikátů, resp. kvalifikovaných systémových certifikátů (PEM, DER, TXT) jsou také zveřejňovány na webových stránkách ministerstva.

Program DataHash

Na webových stránkách ministerstva je umístěn volně ke stažení program „DataHash" pro výpočet otisků certifikátů akreditovaného poskytovatele certifikačních služeb. Program je určen k výpočtu otisků souborů pomocí hashovacích algoritmů MD5 a SHA-1.

Ministerstvo vnitra tento program zpřístupňuje všem uživatelům, kteří se spoléhají na certifikát akreditovaného poskytovatele certifikačních služeb. Pomocí programu se lze ujistit, že certifikát nebyl zaměněn. Uživatel má možnost si pomocí tohoto programu (či jiného obdobného programu dle vlastního výběru) vypočítat otisk certifikátu, který získal jako certifikát akreditovaného poskytovatele certifikačních služeb a vypočtený otisk porovnat s otiskem zveřejněným ministerstvem ve Věstníku a na webových stránkách ministerstva. Pokud se otisky shodují, je zaručeno, že certifikát nebyl zaměněn.

v. Seznam účtů zřízených za účelem placení správních poplatků v souvislosti s řízením podle zákona č. 227/2000 Sb.

Za účelem placení správních poplatků stanovených zákonem č. 634/2004 Sb., o správních poplatcích, ve znění pozdějších předpisů, v souvislosti s řízeními podle zákona o elektronickém podpisu, zřídilo Ministerstvo vnitra následující účty u České národní banky:

- **Přijetí žádosti o udělení akreditace k působení jako akreditovaný poskytovatel certifikačních služeb**

  /část I položka 22 písm. f) sazebníku správních poplatků/

účet číslo **3711-8920071/0710**, VS: **IČ**, KS: **0308**, SS: **neuvádět**

správní poplatek **Kč 100 000**

- **Přijetí žádosti o vyhodnocení shody nástrojů elektronického podpisu**

/část I položka 22 písm. g) sazebníku správních poplatků/

účet číslo **3711-8920071/0710**, VS: **IČ**, KS: **0308**, SS: **neuvádět**

správní poplatek **Kč 10 000**

- **Oznámení o rozšíření služeb akreditovaného poskytovatele certifikačních služeb**

/část I položka 22 písm. h) sazebníku správních poplatků/

účet číslo **3711-8920071/0710**, VS: **IČ**, KS: **0308**, SS: **neuvádět**

správní poplatek **Kč 25 000**