VĚSTNÍK

MINISTERSTVA VNITRA

Ročník 2008 V Praze dne 25. srpna 2008 Částka 71

O B S A H

i. Seznam atestačních středisek s pověřením k provádění atestací uděleným podle novely zákona č. 365/2000 Sb. (zákon č. 81/2006 Sb.)

Ministerstvo vnitra zveřejňuje ve smyslu § 4 odst. 2 písm. h) zákona č. 365/2000 Sb. seznam atestačních středisek.

Novela zákona č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, zavedla nový postup při akreditaci atestačních středisek.

Podle tohoto postupu musí mít od 1.1.2009 atestační střediska pověření k provádění atestací, které uděluje Ministerstvo vnitra pouze za předpokladu, že atestační středisko předloží osvědčení o akreditaci od kreditující osoby (ČIA).

Ministerstvo vnitra podle § 6b zákona č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění pozdějších předpisů, udělilo pověření k provádění atestací těmto atestačním střediskům:

registrační číslo 01

Vydáno na základě rozhodnutí č.j.: MV- 41547-7/OKK-2008 ze dne 28. května 2008

RELSIE spol. s r.o.

se sídlem Praha 5

Na Stárce 1201/12, PSČ 150 00

IČ: 62417339

Pověření bylo vydáno k provádění atestací pro stanovení shody:

- způsobilosti k realizaci vazeb informačního systému veřejné správy s jinými informačními systémy prostřednictvím referenčního rozhraní,
- dlouhodobého řízení informačních systémů veřejné správy s požadavky zákona č. 365/2000 Sb. a prováděcích právních předpisů k tomuto zákonu.

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

- Středočeský kraj
- Praha - Zbraslav
- Pardubický kraj
- Město Liberec
- Město Rakovník

Udělené atesty způsobilosti k realizaci vazeb prostřednictvím referenčního rozhraní

Nebyl udělen žádný atest.

Dříve vydané atesty byly zveřejněny v předchozích Věstnících Ministerstva vnitra.

Název a sídlo atestačního střediska, IČ	Atestační středisko pro ISVS Inspekční orgán A-TEST č. 4042 RELSIE spol. s r.o. Kontaktní adresa: Plzeňská 221, 150 00 Praha 5 Sídlo: Na Stárce 1201/12 IČ: 62417339
Název a sídlo žadatele o atestaci, IČ	Středočeský kraj Zborovská 11, 150 21 Praha 5 IČ: 70891095
Předmět atestace	**Dlouhodobé řízení ISVS**
Datum vydání atestu	30.6.2008
Výsledek zkoušky	SPLŇUJE
Datum provedení další zkoušky	29.6.2013

Název a sídlo atestačního střediska, IČ	Atestační středisko pro ISVS Inspekční orgán A-TEST č. 4042 RELSIE spol. s r.o. Kontaktní adresa: Plzeňská 221, 150 00 Praha 5 Sídlo: Na Stárce 1201/12 IČ: 62417339
Název a sídlo žadatele o atestaci, IČ	Úřad městské části Praha - Zbraslav Zbraslavské náměstí 464, 156 00 Praha - Zbraslav IČ: 241857
Předmět atestace	**Dlouhodobé řízení ISVS**
Datum vydání atestu	30.6.2008
Výsledek zkoušky	SPLŇUJE
Datum provedení další zkoušky	29.6.2013

Název a sídlo atestačního střediska, IČ	Atestační středisko pro ISVS RELSIE spol. s r.o. Kontaktní adresa: Plzeňská 221, 150 00 Praha 5 Sídlo: Na Stárce 1201/12 IČ: 62417339
Název a sídlo žadatele o atestaci, IČ	Pardubický kraj Komenského nám. 125, 532 11 Pardubice IČ: 70892822
Předmět atestace	**Dlouhodobé řízení ISVS**
Datum vydání atestu	22.4.2008
Výsledek zkoušky	SPLŇUJE
Datum provedení další zkoušky	21.4.2013

Název a sídlo atestačního střediska, IČ	Atestační středisko pro ISVS RELSIE spol. s r.o. Kontaktní adresa: Plzeňská 221, 150 00 Praha 5 Sídlo: Na Stárce 1201/12 IČ: 62417339
Název a sídlo žadatele o atestaci, IČ	Město Liberec nám. Dr. E. Beneše 1, 460 59 Liberec 1 IČ: 00262978
Předmět atestace	**Dlouhodobé řízení ISVS**
Datum vydání atestu	18.1.2008
Výsledek zkoušky	SPLŇUJE
Datum provedení další zkoušky	17.1.2013

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	Město Rakovník IČ: 00244309 Husovo nám. 27 269 18 Rakovník
Předmět atestace	**Dlouhodobé řízení ISVS**
Datum vydání atestu	12.12.2007
Výsledek zkoušky	SPLŇUJE
Datum provedení další zkoušky	1.12.2012

iii. 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.

Dříve ověřené kvalifikované certifikáty, resp. kvalifikované systémové certifikáty poskytovatelů certifikačních služeb byly zveřejněny v předchozích Věstnících Ministerstva vnitra.

<table>
<tr><td rowspan="2">Poř. číslo</td><td colspan="3">Ověření kvalifikovaného systémového certifikátu poskytovatele</td></tr>
<tr><td colspan="2">Subjekt</td><td>Adresa</td></tr>
<tr><td>11.</td><td colspan="2">První certifikační autorita, a.s.
identifikační číslo 26 43 93 95</td><td>Podvinný mlýn 2178/6,
PSČ 190 00 Praha 9</td></tr>
<tr><td colspan="4">Certifikát má platnost od 1.4.2008 a První certifikační autorita, a.s. jej začala používat dnem 3.8.2008.</td></tr>
<tr><td colspan="4">Výsledky ověření</td></tr>
<tr><td rowspan="4">A.</td><td>Jméno</td><td>qica_root_20080311.pem</td><td>Délka: 1529 byte</td></tr>
<tr><td colspan="2">Formát certifikátu</td><td>Otisk</td></tr>
<tr><td rowspan="2">PEM</td><td>SHA-1</td><td>76D0 C339 635D 4F2A 020B C4ED 970D 9165 7444 40BF</td></tr>
<tr><td>MD5</td><td>6A45 9538 029C CEF5 CC5D 8C7B E76A 84A1</td></tr>
<tr><td colspan="4"></td></tr>
<tr><td rowspan="4">B.</td><td>Jméno</td><td>qica_root_20080311.der</td><td>Délka: 1085 byte</td></tr>
<tr><td colspan="2">Formát certifikátu</td><td>Otisk</td></tr>
<tr><td rowspan="2">DER</td><td>SHA-1</td><td>6490 2AD7 277A F3E3 2CD8 CC1D C79D E1FD 7F80 69EA</td></tr>
<tr><td>MD5</td><td>48D1 1E62 7801 C26E 4369 A42C EE13 0AB5</td></tr>
<tr><td colspan="4"></td></tr>
<tr><td rowspan="4">C.</td><td>Jméno</td><td>qica_root_20080311.txt</td><td>Délka: 4846 byte</td></tr>
<tr><td colspan="2">Formát certifikátu</td><td>Otisk</td></tr>
<tr><td rowspan="2">TXT</td><td>SHA-1</td><td>E8E6 9BAC 4C9A 9C3A E7A8 E65C F478 FBEF 36D8 44DB</td></tr>
<tr><td>MD5</td><td>42AD E0B8 02ED 2A60 9884 4D89 A15E C707</td></tr>
</table>

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

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 Standard*, 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.