ČESKÝ ÚŘAD ZEMĚMĚŘICKÝ A KATASTRÁLNÍ
ODBOR ŘÍZENÍ ÚZEMNÍCH ORGÁNŮ
182 11 Praha 8, Pod sídlištěm 9, pošt. přihrádka 21

Všem
katastrálním úřadům
a zeměměřickým a katastrálním
inspektorátům

VÁŠ DOPIS ZNAČKY / ZE DNE	NAŠE ZNAČKA	VYŘIZUJE / LINKA	MÍSTO ODESLÁNÍ / DATUM
/	ČÚZK-574/2014-22	Ing. Kmínek / 1234	Praha / 2014-01-09

Ověřování ZPMZ a neměřických záznamů v elektronické podobě a doplnění informací k potvrzování geometrických plánů v elektronické podobě

V důsledku nabytí účinnosti zákona č. 257/2013 Sb., kterým se mění některé zákony v souvislosti s přijetím zákona o katastru nemovitostí, došlo ke změně zákonné úpravy ověřování výsledků zeměměřických činností a od 1. ledna 2014 je nutné k elektronickému podpisu při ověřování připojovat kvalifikované časové razítko. V současné době probíhá příprava nové verze programu KDirSign, kterým lze ověřovat výsledky zeměměřických činností (s výjimkou geometrických plánů) způsobem podle § 18 odst. 5 a 6 vyhlášky č. 31/1995 Sb., kterou se provádí zákon č. 200/1994 Sb., o zeměměřictví a o změně a doplnění některých zákonů souvisejících s jeho zavedením, ve znění pozdějších předpisů (dále jen „vyhláška“). Současná verze KDirSign v. 2.1.0.0 neumožňuje připojení časového razítka, při ověřování výsledků zeměměřických činností je tak nutné dočasně časové razítko (ideálně ve formátu Time Stamp Response .TSR) připojovat k textovému souboru vyhotovenému podle § 18 odst. 6 vyhlášky jiným způsobem, například pomocí nástrojů certifikačních autorit (viz tabulka).

Certifikační autorita	Nástroj na připojení časového razítka
PostSignum	http://www.postsignum.cz/jakym_zpusobem_sluzbu_vyuzivat.html (sekce Aplikace TSA klient)
I.CA	http://www.ica.cz/Download-application (sekce QTSA Klient)
eIdentity	O časová razítka může žádat prostřednictvím klientské aplikace přímo ze svého účtu u eIdentity

Zároveň upozorňujeme, že v souvislosti s vystavením nové verze programu KDirSign bude na webových stránkách zveřejněn nový dokument stanovující ve smyslu § 18 odst. 6 vyhlášky formát textového souboru. V tomto dokumentu bude současný hashovací algoritmus pro vyhotovení otisků SHA-1 nahrazen algoritmem ze sady SHA-2 (konkrétně SHA-512), který poskytuje vyšší bezpečnost (algoritmus SHA-1 je v současné době již považován za „prolomený“). O tomto kroku budou katastrální úřady a zeměměřické a katastrální inspektoráty zvlášť informovány.

V návaznosti na metodický a organizační pokyn pro přebírání geometrického plánu v elektronické podobě, jeho potvrzení, uchovávání a poskytování ze dne 19. prosince 2013 čj. ČÚZK-25095/2013-22 a v souvislosti s výše uvedeným sdělujeme, že i v případě

geometrických plánů je nezbytné používat při podepisování PDF algoritmus ze sady SHA-2 (nejméně SHA-256). Tento algoritmus je podporován od verze PDF 1.6. Pokud je předložen k potvrzení geometrický plán ve verzi PDF starší, ve které nelze použít algoritmus SHA-2, není technicky možné k dokumentu připojit elektronický podpis katastrálního úřadu s časovým razítkem a program JSignPDF-PGP připojení podpisu neprovede. V případě předložení geometrického plánu s použitým nevyhovujícím hashovacím algoritmem je nutné, aby žadatel o potvrzení na základě výzvy k doplnění předložil geometrický plán odpovídající výše uvedenému požadavku (lze provést například tak, že se původní soubor „přepodepíše“ bez zachování předchozích podpisů). Požadavek na použitý algoritmus bude na webové stránce http://www.cuzk.cz/Je-dobre-vedet/Zivotni-situace/Overovani-vysledku-zememerickych-cinnosti-v-elektr.aspx uveden při úpravách souvisejících se zveřejněním nové verze KDirSign.

K příloze „*JSignPDF-PGP - příručka pro správce*“ uvedeného Metodického a organizačního pokynu dále doplňujeme:

U programu JSignPDF-PGP je třeba změnit všem uživatelům konfigurační soubor tak, aby program používal hashovací funkci SHA-256. Ve vystaveném programu na adrese \\a200001\instalace\katastr\JSignPDF-PGP je konfigurační soubor již upraven.

Ing. Bohumil Janeček
ředitel odboru řízení územních orgánů

Přílohy: ---
Na vědomí: ---