PRILOG 2.

IZRAČUN I PRIMJENA KONTROLNOG BROJA

(označena polja ispod grupe podataka III. na stranici A Obrasca R-Sm)

Kontrolni broj ili HASH je zapis duljine četrdeset (40) znakova koji se programski generira iz određenog seta podataka. U ovom slučaju to je zapis generiran iz svih dostavljenih podataka na magnetnom nositelju (kompletan sadržaj formata »MN OBRAZAC R-Sm« koji je opisan u prilogu 4 ovog Pravilnika).

Kontrolni broj generira se prema algoritmu SHA-1. Navedeni algoritam je javno dostupan i objavljen u publikaciji FIPS 180-1 (Federal Information Processing Standards). SHA algoritam služi za generiranje sažete reprezentacije bilo kojeg niza podataka, a primjenjen na nizu bajtova bilo koje duljine uvijek daje rezultat (HASH) veličine 20 bajtova. Svrha algoritma je mogućnost kontrole integriteta podataka za koje se generira HASH. Algoritam garantira da će svaka promjena orginalnog niza podataka uzrokovati generiranje drugog HASH broja. Nije moguće napraviti dva seta podataka koji daju isti HASH, a tim svojstvom algoritam osigurava integritet podataka. Ako se kasnije želi provjeriti da li se predani set podataka, za koji je prethodno izračunat HASH, u međuvremenu promijenio, ponovno se izračuna HASH i usporedi ga se s prije zapisanim HASH-om. Ako su HASH brojevi isti, niz podataka sigurno nije mijenjan.

Nad podacima iz svih slogova datoteke »MN OBRAZAC R-Sm« (nad cijelom datotekom) primjenjuje se SHA algoritam koji daje 20 bajtova prezentiranih u ASCII obliku heksadecimalnog broja. Rezultat je 40 znakova koji se, pri tisku stranice A Obrasca R-Sm, upisuju u predviđenu rubriku. Ukoliko datoteka sadrži podatke za više obrazaca R-Sm (više skupina slogova 3, 5 i 7), tada se isti rezultat SHA algoritma upisuje u predviđenu rubriku na svim stranicama A svih obrazaca R-Sm. Time dobivamo pisani zapis kontrolnog broja svih predanih podataka u jednoj datoteci na magnetnom nositelju. U slučaju spora između primatelja i podnositelja podataka, HASH se uvijek može ponovno izračunati i usporediti s originalnim zapisom na stranici A Obrasca R-Sm.
Radi lakšeg čitanja i kontrole podataka koji se predaju na papiru, u predviđenoj rubrici za HASH na stranici A Obrasca R-Sm, stavlja se znak crtica (–) nakon svakih 10 upisanih znakova.

Na šalteru REGOS-a, kod primitka stranice (ili stranica) A Obrasca R-Sm i magnetnog nositelja s podacima, izvršit će se, od strane šalterskog službenika, kontrola HASH broja izračunatog primjenom SHA algoritma pri učitavanju podataka, te njegova usporedba s HASH brojem koji je zapisan na stranici (ili stranicama) A Obrasca R-Sm. Ako je HASH broj identičan, podaci se službeno prihvaćaju i prosljeđuju na obradu, a podnositelj podataka je siguran da u slučaju reklamacije može dokazati koje podatke je predao. U tu svrhu preporuča se podnositelju da u svojoj arhivi čuva svaku predanu datoteku kao i stranicu A svakoga predanog Obrasca R-Sm.