Standard č. 3

Manažera kybernetické bezpečnosti MD

Věc: Schválené kryptografické prostředky

Informační systém	Všechny aplikace Ministerstva dopravy ČR, zařazené do Systému řízení kybernetické bezpečnosti (SŘKB)
Zodpovědná osoba	Správci a provozovatelé jednotlivých aplikací

Odůvodnění standardu
V příloze Bezpečnostní politiky informací Část V kapitola 2 (Symetrické algoritmy asymetrické algoritmy a hashovací funkce) přílohy č. 4 – Pravidla pro provozovatele IS je k ochraně informací vyžadováno používání Manažerem KB schválených kryptografických prostředků. Konkrétní typy protokolů a kryptografické (šifrovací) algoritmy nejsou součástí Bezpečnostní politiky informací MD, protože relativně rychle zastarávají. Proto je určuje tento standard.

Schválené kryptografické prostředky

V oblasti asymetrické kryptografie schvaluje MD všechny certifikáty těchto certifikačních autorit:

- PostSignum,
- První certifikační autorita,
- Eidentity,
- Thawte,
- GeoTrust.
- Sectigo.

V oblasti komunikačních protokolů je minimálním standardem TLS 1.2.

V oblasti blokových a proudových šifer schvaluje MD tyto šifrovací algoritmy:

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256

Pravidelná kontrola dodržování šifrovacího standardu je prováděna:
- namátkově výpisem ssllabs.com jednotlivých aplikačních serverů,
- naskenováním šifrovacích klíčů vybraných komunikací v rámci INFRA O2ITS i MD.

V Praze dne dle elektronického podpisu

Ing. Josef Svozilík
Digitálně podepsal Ing. Josef Svozilík
Datum: 2021.09.02 20:56:42 +02'00'

……
Ing. Josef Svozilík
Manažer kybernetické bezpečnosti