



NÁZEV MATERIÁLU	Připomínky Svazu průmyslu a dopravy České republiky k návrhu vyhlášky o provádění certifikace při zabezpečování kryptografické ochrany utajovaných informací
Č. J.	100/2024
DATUM ZPRACOVÁNÍ	21. 10. 2024
KONTAKTNÍ OSOBA	Kateřina Kalužová
E-MAIL	kkaluzova@spcr.cz

ZÁSADNÍ KONKRÉTNÍ PŘIPOMÍNKY

1. Způsob a provádění certifikace kryptografického prostředku (připomínky k § 6 odst. 1 písm. f) a g)):

Ustanovení § 6 odst. 1 návrhu vyhlášky o provádění certifikace při zabezpečování kryptografické ochrany utajovaných informací (dále jen „vyhláška o certifikaci“) upravuje způsob a postup, jakým Národní úřad pro kybernetickou a informační bezpečnost (dále jen „NÚKIB“) provádí certifikaci kryptografického prostředku. Mezi kritéria, které NÚKIB v rámci procesu certifikace prověřuje, patří dle § 6 odst. 1 písm. f) a g) vyhlášky o certifikaci také následující:

„f) naplnění požadavků na výrobu, provozování a ochranu kryptografického prostředku a materiálu k zajištění jeho funkce,

g) naplnění požadavků na začlenění kryptografického prostředku do komunikačního nebo informačního systému (...).“

Ze znění těchto kritérií vyplývá, že se jedná o požadavky, které kryptografický prostředek musí naplnit k tomu, aby mohl být certifikován. Podle § 8 odst. 2 návrhu vyhlášky o zajištění kryptografické ochrany utajovaných informací (dále jen „vyhláška o kryptografické ochraně“) tyto požadavky „*stanoví provozní dokumentace kryptografického prostředku a bezpečnostní standard Národního úřadu pro kybernetickou a informační bezpečnost*“.

Bezpečnostní standard, na nějž předmětné ustanovení odkazuje, však nebyl dle našich informací ze strany NÚKIB dosud publikován. Domníváme se, že k tomu, aby se mohla odborná veřejnost k procesu certifikace kryptografického prostředku vyjádřit, je zásadní, aby byla seznámena rovněž s výše uvedenými požadavky na certifikaci kryptografického prostředku, jež mají být mimo jiné upraveny v rámci předmětného bezpečnostního standardu. **V souvislosti s výše uvedeným tak žádáme NÚKIB, aby uveřejnil k připomínkování ze strany odborné veřejnosti rovněž bezpečnostní standard, na nějž odkazuje § 8 odst. 2 návrhu vyhlášky o kryptografické ochraně, pokud je tento dokument již k dispozici.**