INSTRUKCE OI č. 7/2007

POUŽÍVÁNÍ CERTIFIKÁTŮ

1. Tato instrukce stanoví obecný postup pro práci s certifikáty (získávání, uchovávání, používání, zneplatňování).
2. Práce s certifikáty je podřízena certifikační politice příslušné certifikační autority (dále jen CA). Ustanovení této instrukce nesmí být v rozporu s certifikační politikou CA.
3. Přednostně jsou používány kvalifikované certifikáty, které vystavují v ČR certifikační autority, mající příslušnou akreditaci, jejichž seznam zveřejňuje Ministerstvo informatiky v souladu s § 9 odst. 2 písm. e) zákona č. 227/2000 Sb. Pouze ve speciálních případech certifikátů pro autentizaci ke komerčním službám (např. CzechPOINT, REP) a certifikátů pro technologické komponenty jsou používány komerční certifikáty, které jsou podle účelu získávány od certifikačních autorit v ČR i v zahraničí.
4. Certifikáty, na které se vztahuje tato instrukce, jsou rozlišovány následovně:
    a) Kvalifikované osobní zaměstnanecké certifikáty,
    b) Komerční osobní zaměstnanecké certifikáty,
    c) Kvalifikované systémové certifikáty,
    d) Komerční certifikáty pro technologické komponenty,
    e) Komerční šifrovací certifikáty pro skupiny osob,
    f) Kořenové certifikáty certifikačních autorit.
5. Za dodržení certifikační politiky odpovídá zaměstnanec, který certifikát osobně přebírá a tuto skutečnost osobně potvrzuje CA.
6. Za ochranu soukromých klíčů odpovídá zaměstnanec, pro kterého byly klíče s žádostí generovány.
7. Evidenci certifikátů a oprávněných osob vede odbor informatiky.
8. Evidenci hesel pro zneplatnění certifikátů vede odbor informatiky.
9. Generování klíčů a žádosti o certifikát provádí žadatel nebo pracovník odboru informatiky za přítomnosti žadatele, tak, aby hesla a klíče zůstaly pod výhradní kontrolou žadatele.
10. Generování následného certifikátu provádí žadatel nebo pracovník odboru informatiky za přítomnosti žadatele, tak, aby hesla a klíče zůstaly pod výhradní kontrolou žadatele.
11. Pokud jsou klíče s žádostí generovány na technických prostředcích, které nejsou pod výhradní kontrolou žadatele, musí být klíče generovány za přítomnosti žadatele jako exportovatelné a po úspěšném exportu musí být z technického prostředku odstraněny.
12. Je upřednostňováno uložení certifikátů s klíči na zabezpečeném úložišti (čipová karta, USB token).
13. V případě podezření na zneužití certifikátu nebo ztráty čipové karty (USB tokenu) s certifikátem je zaměstnanec nebo jeho nadřízený (vedoucí odboru) povinen neprodleně požádat o zneplatnění certifikátu prostřednictvím odboru informatiky.
14. V případě rozvázání pracovního poměru se zaměstnancem odpovídá vedoucí odboru (tajemník úřadu) za podání žádosti o zrušení uživatelského účtu a zneplatnění zaměstnaneckého certifikátu. Na základě žádosti zajistí odbor informatiky zneplatnění certifikátu a vyřazení zaměstnance ze seznamu oprávněných osob. Zneplatnění zaměstnaneckého certifikátu je podmínkou pro potvrzení výstupního listu.
15. Tato revize platí od 8. 12. 2009.