Národný bezpečnostný úrad
Sekcia informačnej bezpečnosti a elektronického podpisu
Budatínska 30, 850 07 Bratislava 57

Príloha č.1 k č.: 3679/2006/IBEP-001 V Bratislave 4. októbra 2006

USMERNENIE K POSÚDENIU CERTIFIKOVANÝCH SW APLIKÁCIÍ PRE ZARUČENÝ ELEKTRONICKÝ PODPIS, POUŽÍVAJUCE PODPISOVÉ POLITIKY PLATNÉ DO 31. 12. 2006

Úvod

Pri overovaní podpisu je zaručený elektronický podpis (ZEP), okrem iného, platný, ak bola na jeho vyhotovenie použitá Národným bezpečnostným úradom (NBÚ) schválená podpisová politika.

1. Analýza schválených podpisových politík v certifikovaných aplikáciách pre ZEP

Niektoré certifikované aplikácie pre ZEP využívajú nasledovné schválené podpisové politiky:

- **ES** Podpisová politika pre zaručený elektronický podpis (policyEs.der),
- **ES-T** Podpisová politika pre zaručený elektronický podpis s časovou pečiatkou (policyEsT.der),
- **ES-C** Podpisová politika pre zaručený elektronický podpis s úplnou informáciou na overenie (policyEsC.der),
- **ES-A** Podpisová politika pre zaručený elektronický podpis archívny (policyEsA.der),
- **ES-T-UTF8** Podpisová politika pre zaručený elektronický podpis s časovou pečiatkou textových údajov v ASCII a UTF8 kódovaní (policyEsTUtf8.der),

ktorých **platnosť končí 31. 12. 2006.** Po ukončení platnosti horeuvedených podpisových politík bude zaručený elektronický podpis vyhotovený na základe horeuvedených podpisových politík vyhodnotený ako neplatný z dôvodu použitia neplatnej podpisovej politiky. Aplikácia pre ZEP certifikovaná NBÚ, ktorá vie pracovať **len** s horeuvedenými podpisovými politikami bude od 1.1.2007 nespôsobilá pre podpisovanie a overovanie ZEP, nakoľko platnosť týchto politík skončila 31.12.2006. NBÚ na základe tejto skutočnosti si vyhradzuje právo zrušiť platnosť certifikátu, lebo po jeho vydaní nastali okolnosti, pre ktoré certifikovaný produkt nesplňuje podmienky použitia (napríklad v prílohe certifikátu je uvedené, že “aplikácia pre ZEP smie byť použitá len s danou podpisovou politikou s uvedeným OID danej politiky“).

2. Podpisová politika „QES Zaručený elektronický podpis v súlade s legislatívou Slovenskej republiky“

NBÚ vydal novú podpisovú politiku „**QES Zaručený elektronický podpis v súlade s legislatívou Slovenskej republiky (policyQES.der)“** s dobou platnosti od 20.3.2006 do 1.1.2008. Táto podpisová politika nahradzuje všetky horeuvedené podpisové politiky a rieši ďalšie požiadavky medzinárodných štandardov a slovenskej legislatívy.

Pri budúcich certifikáciách aplikácií pre ZEP audítor overí, ktoré položky a aké hodnoty položiek podpisovej politiky je aplikácia schopná spracovať. Tieto položky budú uvedené v auditnej správe a certifikát aplikácie nebude obmedzovaný na konkrétnu podpisovú politiku, ale pri importe podpisovej politiky aplikácia prekontroluje, či vie rozpoznať všetky položky podpisovej politiky a ak sa nachádzajú neznáme položky, aplikácia prehlási, že s podpisovou politikou nevie pracovať a preto podľa tejto podpisovej politiky nemôže určiť správny výsledok overenia.

Životný cyklus podpisovej politiky sa bude riadiť dokumentom **„Správa podpisových politík“** v platnej a NBÚ schválenej verzii.

3. Postup na odstránenie vzniknutého stavu

Dňa 25.7.2006 sa uskutočnilo v priestoroch NBÚ stretnutie „Pracovnej skupiny k problematike certifikácie SW aplikácií pre ZEP“, ktorá sa zaoberala problematikou ukončenia platnosti horeuvedených podpisových politík. Na stretnutí sa zúčastnili aj zástupcovia výrobcov aplikácií, ktoré používajú len podpisové politiky uvedené v bode 1.

Na stretnutí bol prijatý záver:

Dotknuté firmy sa dohodnú s NBÚ na spoločnom postupe na odstránenie vzniknutého problému. Na jednotlivých stretnutiach bude potrebné analyzovať, či:

- je aplikácia schopná pracovať s novou univerzálnou schválenou podpisovou politikou **QES**,
- zmena podpisovej politiky znamená zásah do kódu aplikácie,
- je potrebné vykonať nový audit.

Po analýze výrobcovia, ktorých aplikácia nedokáže pracovať so schválenými NBÚ podpisovými politikami platnými po 1.1.2007, musia podať žiadosť o novú certifikáciu aplikácie pre ZEP. Pri procese certifikácie NBÚ zohľadní už známe skutočnosti a proces certifikácie vykoná v čo najkratšom čase.

Záver

Zavedením novej univerzálnej podpisovej politiky „QES Zaručený elektronický podpis v súlade s legislatívou Slovenskej republiky“ a jej spravovaním podľa dokumentu „Správa podpisových politík“ v platnej a NBÚ schválenej verzii bude vyriešený problém používania podpisovej politiky v aplikáciách pre vyhotovovanie a overovanie ZEP.

Spracovali: Mgr. Ivan Chrenko
Ing. Anton Lachký