https://www.zive.sk/clanok/128489/uz-sa-daju-vybavit-nove-elektronicke-podpisy/

31.10.2017 10:20 | Štát a IT

TOP Už sa dajú vybaviť nové elektronické podpisy

Ilustračná snímka Zdroj: iStock


Lukáš Kosno

Pracovisko musia ľudia zrejme navštíviť osobne.

Oddelenia dokladov už zahájili nahrávanie nových bezpečnejších certifikátov na občianske preukazy s čipom. Stručne sme o tom **informovali už včera**.

Certifikáty slúžia na vytváranie kvalifikovaných elektronických podpisov (KEP), ktoré sa dajú využiť pri úradných úkonoch. Cez internet sa podľa dostupných informácií zaobstarať ešte nedajú.

K nahradeniu prichádza po objavení zraniteľnosti v knižnici pre generovanie šifrovacích kľúčov od firmy Infineon. Problém spočíva v skutočnosti, že z verejného kľúča sa dá vypočítať súkromný zásadne

rýchlejšie, ako sa pôvodne predpokladalo. Kriminálnici potom dokážu falšovať elektronické podpisy. V digitálnej podobe sú na nerozoznanie od originálneho.

Vraj slabá informovanosť

Zmena certifikátov spočíva v prechode na dlhší šifrovací kľúč – z 2048 na 3072-bitový. Ešte pred dvomi týždňami štátna tajomníčka ministerstva vnútra Denisa Saková hovorila, že sa tak stane v horizonte štyroch až piatich týždňov.

Čítajte aj Ako útočiť na slovenské e-občianske: Návod je vonku, podpisy idú rušiť už...

Podľa diskusie na platforme Slovensko.Digital už minulý týždeň prebehol neverejný test a včera a verejný. Napriek tomu ale Finančná správa SR dala poobede na web oznam, že nahrávanie prebieha už od pondelka.

Aktuálne používatelia na internete konštatujú, že infolinka bratislavského klientskeho centra ešte dnes o ničom nevedela. Informovanosť je slabá. (...) Bol som dnes druhý za týmto účelom a zneplatnenie pôvodných a nahratie nových certifikátov trvali 15-18 minút," dodáva jeden.

Zatiaľ len dlhší kľúč

Pôjde pritom len o dočasné riešenie. „RSA kľúč s 3 072 bitmi nie je možné pomocou nami aktuálne známej metódy faktorizovať a získať tak privátny kľúč (v čase považovateľnom za prakticky uskutočniteľný útok). Zároveň je jeho bezpečnosť menšia, než by mal úplne náhodne vygenerovaný ‚správny' 3 072-bitový kľúč," uviedol pre Živé.sk Petr Švenda z výskumného tímu, ktorý na slabinu prišiel.

Aj preto sa limitovala certifikácia čipových kariet, pri ktorých sa využívali 2 048-bitové kľúče. „Zostala síce v platnosti, ale s obmedzeniami, ktoré vydal Federálny úrad pre bezpečnosť informačnej techniky v Nemecku. Tieto obmedzujú certifikáciu na kľúčové dĺžky RSA 3 072 a 3 584 bitov," uviedol Národný bezpečnostný úrad (NBÚ).

Švenda pripúšťa, že v budúcnosti môže dôjsť k zlepšeniu navrhnutého útoku a dnešný predpoklad o dostatočnej dĺžke kľúča a nemožnosti vykonať reálny útok sa zmení. „Toto je veľmi obtiažne predvídať," komentoval.

Ráta ale so situáciou, že vo všetkých prípadoch sa používa rovnaký algoritmus. NBÚ ale redakcii písal, že chystaný 3 072-bitový kľúč má využívať inú knižnicu.

Porovnajte si odhadované časy potrebné na prelomenie šifrovacích kľúčov rôznych dĺžok. Väčšia dĺžka neznamená automaticky kratší čas:

Dĺžka kľúča	2x Intel E5-2666 v3 @ 2,90 GHz	Náklady na prenájom cloudu

512 bitov	0,63 hodín	0,063 $
1 024 bitov	31,71 dní	76 $
2 048 bitov	45,98 rokov	40 305 $
3 072 bitov	9,28 * 10^ 24 rokov	8,13 *10^ 27 $
4 096 bitov	4,18 * 10^ 8 rokov	3,66 * 10^ 11 $

Zdroj: The Return of Coppersmith's Attack: Practical Factorization of Widely Used RSA Moduli

Teraz len osobne

Predpokladáme, že výmena sa zatiaľ nedá uskutočniť na diaľku cez internet. Aj samotná príprava pracovísk štátu údajne prebiehala osobnou inštaláciou potrebného softvéru, píše diskutér na webe. Ak informácie platia, tak občania musia navštíviť pracovisko vydávania dokladov osobne.

Štát ale chystá zmenu a už avizoval prechod na celkom iný algoritmus vytvárania kľúčov. Stať by sa tak malo už na začiatku budúceho roka.

Až nový algoritmus umožní správu certifikátov na diaľku a okrem toho aj zrýchli celý proces generovania kľúčového páru, uviedol pre Živé.sk NBÚ.