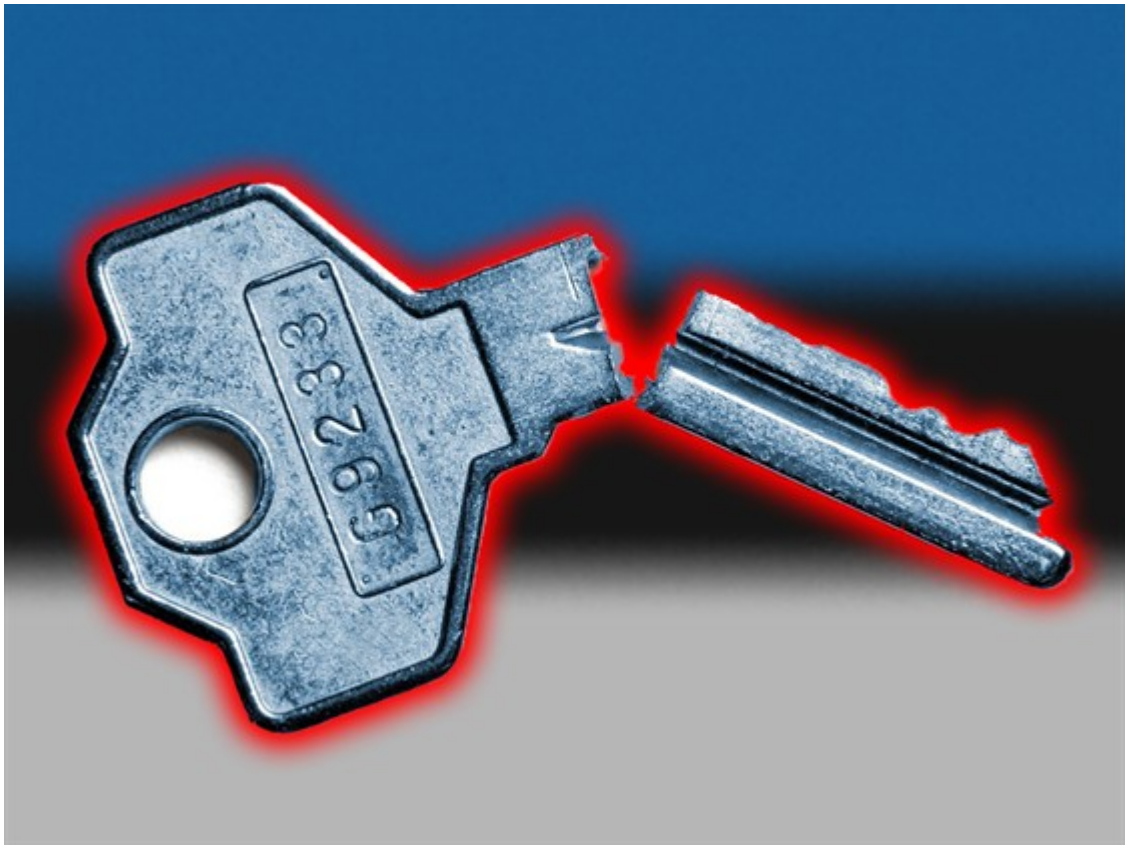
Estonsko blokuje revoluční „internetové občanky“, hrozí krádež identity

8. listopadu 2017 13:48, aktualizováno 14:26
https://technet.idnes.cz/chyba-v-elektronickych-obcankach-d4d-/sw_internet.aspx?c=A171108_134815_tec-kratke-zpravy_pka

Estonské elektronické občanské průkazy byly dočasně pozastaveny. Důvodem je chyba, kterou výzkumníci objevili v kryptografickém zabezpečení certifikátů.



Zvětšit fotografii

Problém se šifrováním zasáhl miliony estonských certifikátů. | foto: montáž: Pavel Kasík, Technet.cz, Profimedia.cz

Už koncem léta varovala skupina bezpečnostních expertů, že estonské elektronické občanky obsahují závažnou chybu v ověřování certifikátů. Od té doby se ukázalo, že chyba je ve skutečnosti ještě závažnější a ohroženy by mohly být miliony vydaných ID karet, píše ArsTechnica. Chyba se týká všech karet vydaných od roku 2008. Estonsko zároveň dočasně zastavilo vydávání elektronického občanství.

Podle Kasparo Krojuse, který má program e-Residency na starosti, zatím nejsou známy žádné případy, kdy by došlo ke krádeži identity. Estonské elektronické občanky umožňují

komunikovat po internetu s úřady, podepisovat dokumenty nebo dokonce hlasovat po internetu v estonských volbách.

Staré certifikáty byly zablokovány

Chyba spočívá v tom, že z veřejného klíče lze „uhodnout“ (dopočítat) klíč soukromý. Právě pomocí soukromého klíče lze kryptograficky podepsat zprávy, dokumenty nebo například hlasovat v elektronických volbách. Proto by tato chyba mohla vést k podepsání zprávy cizím klíčem, a tedy dokonalému napodobení - zcizení - identity jen na základě klíče veřejného.

Uživatelé mohou zažádat o vydání nového certifikátu, který touto chybou netrpí. Na update mají občané Estonska (a tzv. e-rezidenti) čas do března 2018. Staré certifikáty byly estonskou policií suspendovány.

„Pokud zatím víme, nedošlo ke zneužití této chyby,“ uvedl premiér Estonska Jüri Ratas. „Ale policie a hraniční stráž riziko analyzovaly a dospěly k tomu, že jde o reálné ohrožení bezpečnosti. Tím, že jsme tyto postižené karty zablokovali, jsme zajistili bezpečnost systému ID karet.“

Slovensko má stejný problém

Na konci října začaly Slovenské úřady vydávat nové zaručené elektronické podpisy do čipů občanských průkazů, které slouží k podpisování dokumentů v elektronické podobě. Podle státní tajemnice ministerstva vnitra Denisy Sakové úřady zároveň plošně deaktivují stávající rizikové elektronické podpisy. Opatřením, které se na pětimilionovém Slovensku dotkne asi 300 000 lidí, Bratislava reaguje na odhalení bezpečnostního rizika spojeného s čipy německého výrobce Infineon Technologies. Na problém upozornili vědci z brněnské Masarykovy univerzity v polovině října.

V první vlně budou moci požádat o bezplatné nahrání nových podpisových certifikátů hlavně osoby, které zaručený elektronický podpis dosud použily v praxi. Podle Sakové jde o 100 000 lidí, z toho aktivně jej využívá asi 30 000 osob, které elektronicky komunikují například se státními institucemi.

Držitelům zaručeného elektronického podpisu, kteří jej nepoužívají, plánují úřady nahrát jeho bezpečnější verzi na dálku v příštích týdnech.

Slovenské ministerstvo vnitra předminulý týden oznámilo, že pozastavilo vydávání občanských průkazů umožňující vytvářet zaručený elektronický podpis. Dříve tvrdilo, že riziko vzniku bezpečnostního problému na Slovensku v souvislosti s prolomením zaručeného podpisu je pouze teoretické.

Ministr vnitra Robert Kaliňák dokonce veřejně vybídl k prolomení svého zaručeného elektronického podpisu. Experti tehdy tvrdili, že ministerstvo riziko zlehčuje. Minulý týden ale příslušná slovenská certifikační autorita rozhodla o zrušení vydaných rizikových elektronických certifikátů na vytváření zaručeného elektronického podpisu.

Aktualizováno: Článek jsme aktualizovali o informace ze Slovenska.

Zdroj: https://technet.idnes.cz/chyba-v-elektronickych-obcankach-d4d-/sw_internet.aspx?c=A171108_134815_tec-kratke-zpravy_pka