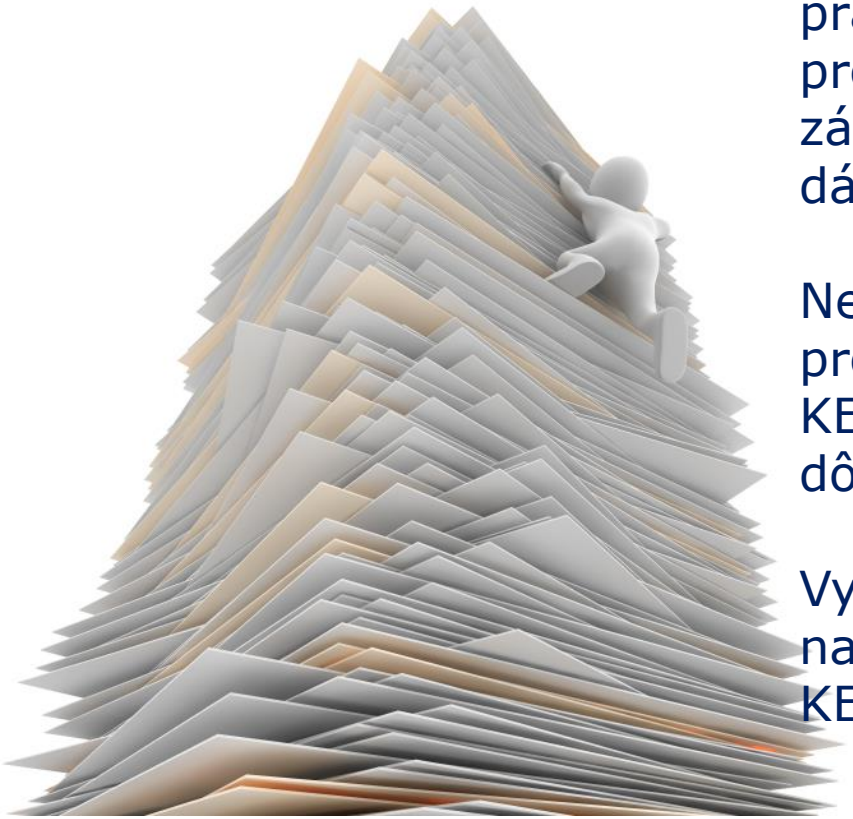
ITAPA 2018

Certifikácia SW produktov pre kvalifikovaný elektronický podpis a pečať - Aby dôveryhodné služby boli dôveryhodné

Jozef Chebeň

CHRÁNIME VAŠE HODNOTY

Prečo ?



... Možnosť zachytenia obsahu právneho úkonu elektronickými prostriedkami je v občianskom zákonníku zakotvená už dávnejšie.

Neoddeliteľnou súčasťou tejto problematiky sú prostriedky pre KEP, ich bezpečnosť a dôveryhodnosť.

Vykonali sme audity najpoužívanejších produktov pre KEP

VYHOTOVENIE PODPISU V SCA

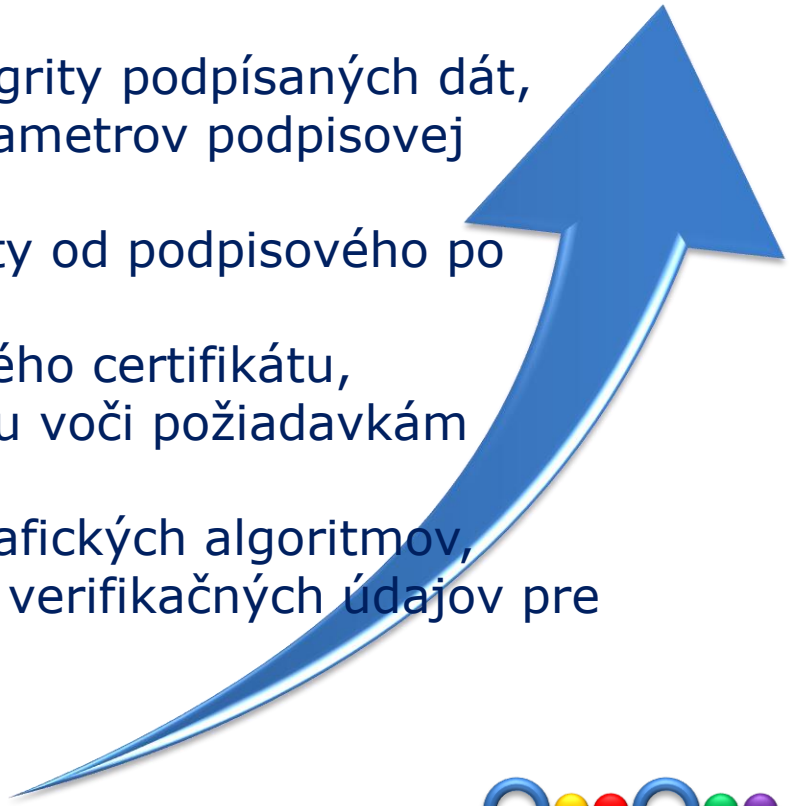
- validácia dátových objektov,
- doplnenie atribútov a zostavenie dátovej štruktúry pre podpis,
- korektné zobrazenie podpisovaných dát používateľovi,
- výpočet hash odtlačku podpisovaných dát, kontrola atribútov podpisového certifikátu,
- odoslanie hash odtlačku do SCD (Signature creation device),
- kryptografická validácia vytvoreného podpisu,
- zostavenie finálnej štruktúry podpisu overenie totožnosti oprávnenej osoby

CHRÁNIME VAŠE HODNOTY

OVERENIE PODPISU V SVCA

- validácia dátových objektov,
- validácia podpísaných dátových objektov,
- overenie, či štruktúra podpisu obsahuje povinné atribúty,
- kryptografická kontrola integrity podpísaných dát,
- identifikácia a načítanie parametrov podpisovej politiky,
- zostavenie certifikačnej cesty od podpisového po koreňový certifikát,
- overenie platnosti podpisového certifikátu,
- kontrola parametrov podpisu voči požiadavkám podpisovej politiky,
- kontrola použitých kryptografických algoritmov,
- prípadné doplnenie úplných verifikačných údajov pre

A formu podpisu



CHRÁNIME VAŠE HODNOTY

METODIKA AUDITU

- protokolárna kompilácia zdrojových kódov,
- realizácia testovacích scenárov
- analýza rizík,
- posúdenie aplikačnej architektúry – optimálnosť návrhu logických modulov aplikácie a vzájomných väzieb medzi nimi,
- hodnotenie dokumentácie – kontrola predpísaného rozsahu a obsahu predloženej dokumentácie,
- vypracovanie auditnej správy

NASADENIE A PREVÁDZKA

- certifikovaný produkt, by mal byť nasadený a prevádzkovaný za podmienok, ktoré definuje výrobca v dokumentácii

- bolo by potrebné auditovať aj spôsob implementácie, prevádzkové prostredie aplikácie a súvisiace procesy

  poznámka: u dôveryhodných služieb, ktoré majú kvalifikovaný štatút (napr. služba validácia kvalifikovaných elektronických podpisov a pečatí) sa tento postup uplatňuje v rámci posúdenia zhody.

- pri aplikáciách pre vyhotovenie KEP, keďže sa nejedná o službu ktorá má kvalifikovaný štatút, je spôsob nasadenia a prevádzkovania aplikácie v podstate mimo akejkoľvek kontroly

CHRÁNIME VAŠE HODNOTY

PRÁVNY RÁMEC

- eIDAS je platný od 1. júla 2016
- v SR bol vydaný Zákon č. 272/2016 Z. z. o dôveryhodných službách - zrušil pôvodný zákon o elektronickom podpise a všetky dovtedy platné vyhlášky (vrátane metodiky auditu)
- vyhotovovanie elektronického podpisu je podľa eIDAS jednou z dôveryhodných služieb
- eIDAS - ak má byť služba a teda aj aplikácia dôveryhodná, mal by existovať dôkaz, že sú splnené funkčné a bezpečnostné požiadavky
- eIDAS navrhlo z certifikácie vylúčiť aplikácie pre vyhotovenie KEP (bod 56)

CHRÁNIME VAŠE HODNOTY

PRÁVNY RÁMEC

- dobrá správa - národná legislatíva požiadavku auditu zachovala (Zákon 272/2016 o dôveryhodných službách § 10 Certifikácia, odsek 2)

- metodické usmernenie NBÚ SR: „Pre potreby certifikácie je potrebné predložiť auditnú správu vyhotovenú nezávislým odborným audítorom, s výrokom o splnení bezpečnostných požiadaviek kladených na aplikáciu.“

PRÁVNY RÁMEC

- zlá správa - V technickej norme, Príloha A2, ISO 14533 [8] aj usmerneniach NBÚ SR o audite, nie sú špecifikované žiadne bezpečnostne požiadavky, ani hrozby, ktoré je potrebné adresovať v rámci analýzy rizík.

- dokument CWA 14170 (2004) referencovaný v metodike pre certifikáciu aplikácii pre KEP je neplatný

- v podstate je možné podpísať akýkoľvek formát údajov (nielen tie, ktoré boli dohodnuté v rámci výnosu o štandardoch),

- nerieši sa vizualizácia podpisovaného obsahu, ani bezpečnostné požiadavky spojené s jeho vizualizáciou

CHRÁNIME VAŠE HODNOTY

ZÁVER

V oblasti certifikácie aplikácii pre KEP existuje stav, ktorý by sa dal označiť ako „metodické vákuum“. Na stránke NBÚ SR je síce definovaný formálny postup, ktorý je potrebné pri certifikácii dodržať, ale neexistuje metodický rámec a ani jednoznačné pravidlá, podľa ktorých by sa malo pri audite postupovať.

OTÁZKY ?