

NOVINKY VE SLUŽBÁCH AKREDITOVANÝCH POSKYTOVATELŮ CERTIFIKAČNÍCH SLUŽEB

Ing. Petr Budiš, Ph.D.

Klíčové body prezentace

- Start datových schránek a autorizované konverze dokumentů
- Přejechod na silnější kryptografii
- Časová razítka – zvýšená poptávka po kvalitních službách
- Problém ověření elektronického podpisu

Využití certifikátů v datových schránkách

- Autentizace
- Elektronický podpis dokumentů
- Autorizovaná konverze



Přechod na silnější kryptografii

- Diskuse s partnery
- Obtížně odhadnutelný dopad na klienty
- Technologické obtíže
- Nutnost výměny HW a SW komponentů
- Složitost harmonogramu nasazení a koordinace
- Náklady
- Obtížné vyčíslení přínosů

Časové razítko – TS

- *Kvalifikovaným časovým razítkem je datová zpráva, kterou vydal kvalifikovaný poskytovatel certifikačních služeb a která důvěryhodným způsobem spojuje data v elektronické podobě s časovým okamžikem, a zaručuje, že uvedená data v elektronické podobě existovala před daným časovým okamžikem*
- *Požadavek na kvalitní, dostupné a přístupné služby*
- *Počet vydaných časových razítek strmě roste*
- *Nové aplikace (el. fakturace, bankovníctví, elektronická komunikace, archivace elektronických dokumentů)*

Ověření elektronického podpisu

- Technicky a technologicky poměrně složitý problém
- Spoléhající se strana musí provést veškeré úkony, aby si ověřila, že zaručený elektronický podpis je platný a kvalifikovaný certifikát nebyl zneplatněn
- CRL, OCSP
- On-line služba ověření podpisu založená na SCVP

Budoucnost

- Elektronická komunikace a elektronické dokumenty se bez popisovaných technologií (EP, TS...) neobejdou
- Počet uživatelů roste v lokálním i celosvětovém měřítku
- Legislativa a technické normy se rychle vyvíjí
- Budou se objevovat nové prvky, založené na PKI

Petr Budiš
budis@ica.cz

DĚKUJI ZA POZORNOST