Elektronická evidence tržeb

Miroslav Hejna
náměstek ministra financí pro informační a komunikační technologie

Konference EET: Zkušenosti a očekávání

Praha, 16. června 2015

EET – shodné principy českého a chorvatského modelu 1/6

Jsou zachovány základní principy chorvatského modelu:

- **Online model fiskalizace** s bezprostředním předáváním informací do centrálního EET
- **Podpora off-line zpracování** s dodatečným zasláním informací pro vymezené či mimořádné případy – zejména případy výpadků či trvalé nedostupnosti on-line připojení
- **Otevřenost pro trh koncových zařízení** a jejich řešení s tím, že nejsou kladeny žádné požadavky na specifické certifikace koncových zařízení
- **Využití standardních komunikačních a bezpečnostních modelů** a protokolů (XML, SSL, PKI včetně certifikátů a elektronického podpisu)
- **Důraz na nízké náklady** na straně poplatníka
- Využití portálových WWW aplikací pro uživatele (ověřování, loterie, apod.)
- **Otevřenost** pro mobilní řešení

EET – shodné principy českého a chorvatského modelu 2/6

Český model EET přizpůsobuje a doplňuje chorvatský model a jeho implementaci českému prostředí a potřebám. Tyto odlišnosti jsou v následujících oblastech:

- Legislativní rámec zavedení a provozování EET
- Potřebná kapacita a výkon celého řešení EET
- Prvotní přidělení a správa autentizačních údajů poplatníka
- Rozšířený přístup poplatníka k vlastním údajům
- Modifikace či posílení vybraných mechanizmů zabezpečení

EET – shodné principy českého a chorvatského modelu 3/6

Potřebná kapacita a výkon celého řešení EET:

- V ČR je nutno počítat s **více než 3-násobným kapacitou a výkonem systému**

- S ohledem na počet poplatníků a počet obyvatel je nutno počítat s násobným objemem transakcí rozprostřených v čase i ve špičkách

- Kapacita a výkon systému EET je navrhován s následujícími parametry pro špičkový výkon:

  - **až 600 tisíc poplatníků**
  - **až 30 miliónů transakcí/den**
  - **až 4000 transakcí/sekundu**

EET – shodné principy českého a chorvatského modelu 4/6

Prvotní přidělení a správa autentizačních údajů poplatníka:

- **Prvotní přidělení autentizačních údajů prostřednictvím:**
  - Datové schránky
  - FÚ
  - Využití principu distribuce bezpečných předtištěných obálek

- **Využití portálového řešení EET:**
  - Bezpečná inicializace účtu poplatníka na portálu EET
  - Bezpečné přihlašování k účtu poplatníka na portálu EET
  - Zajištění privilegovaných operací poplatníka na portálu EET
  - Správa účtu a informací (např. provozovny) poplatníka
  - Správa certifikátů poplatníka.

EET – shodné principy českého a chorvatského modelu 5/6

Rozšířený přístup poplatníka k vlastním údajům:

- Přístup k základním informacím o poplatníkovi na portálu EET
- Přístup k informacím o spravovaných autentizačních údajích a certifikátech na portálu EET
- Přístup k agregovaným údajům zasílaných poplatníkem do EET na portálu EET
- Přístup k detailním údajům zasílaných poplatníkem do EET na portálu EET

EET – shodné principy českého a chorvatského modelu 6/6

Modifikace či posílení vybraných mechanizmů zabezpečení:

- **Otevřený prostor pro způsob řešení systémů a procesů na straně poplatníka**
  - Poplatníkovi jsou poskytnuty prostředky a nástroje pro řádné předávání požadovaných informací (zejména autentizační údaje, certifikát/ty, komunikační rozhraní EET, portál EET).
  - Způsob jejich implementace na straně poplatníka je odpovědností a kompetencí poplatníka. Poplatník není např. omezován zda s EET komunikují jednotlivé pokladny, centrálně celé provozovny či jeden centrální systém nebo jakým způsobem jsou technicky distribuovány, spravovány a využívány jeho certifikáty. Není např. vynucován výlučný model komunikace koncových pokladen s EET.
  - Poplatník odpovídá za jím předávaná data včetně důsledků nevhodné či chybné implementace řešení na své straně.
- **Nastavení kryptografických mechanizmů v souladu s českou legislativou (použití RSA klíčů v délce 2048 bitů a SHA-256 pro elektronický podpis)**
- **Posílení ochranných prvků fyzické „papírové“ účtenky při off-line módu (doplnění o kód PKP)**
- **Náhrada MD5 při výpočtu kódů – minimálně použití SHA1**
- **Změna prezentace vybraných informací (kódů) s důrazem na přijatelný rozsah (počet tištěných znaků), potřebný rozsah informací (zejména velkého PKP) a jejich „čitelnost“ – využití modifikované BASE64 reprezentace.**

Děkuji za pozornost

Miroslav.Hejna@mfcr.cz