# Public key infrastructure

Dnešné riešenia využívajú moderné prostriedky na zabezpečenie prístupu a ochrany dát. Jednou z nich je kryptografia asymetrických kľúčov s vlastnou infraštruktúrou verejných kľúčov PKI. Základ celej PKI infraštruktúry tvorí integrovaná certifikačná autorita PrimeKey EJBCA, ktorá patrí medzi špičku súčasných Enterprise PKI riešení na svete. EJBCA je v súčasnosti nasadená vo viacerých krajinách vo verejnom sektore, príkladom sú ministerstvo obrany a ministerstvo financií vo Francúzsku, polícia a verejný sektor vo Švédsku, ministerstvo zdravotníctva v Španielsku, daňový úrad v Číne, a iné.

## Čipové karty

Prístup do informačných systémov zabezpečujú inteligentné čipové karty. Čipové karty sa využívajú jednak na autorizáciu a autentizáciu používateľov v systéme ako aj na utajenie obsahu a zabezpečenie integrity citlivých údajov finančných transakcií. Na tieto účely sa využívajú viaceré princípy a technológie asymetrickej kryptografie, ako sú elektronický podpis, šifrovanie dát a komunikácie medzi klientskou aplikáciou a serverom (SSL).

Naše riešenie bolo navrhnuté a vyvinuté pre čipové karty tak, aby umožňovalo držať na čipovej karte súčasne viaceré aplikácie pre elektronický podpis (EP) a zaručený elektronický podpis (ZEP). Aplikácia pre ZEP na použitej čipovej karte bola certifikovaná NBÚ ako bezpečný produkt pre zaručený elektronický podpis. Možnosť využitia zaručeného elektronického podpisu v našom riešení otvára do budúcna nové možnosti pre automatizáciu poštových operácií a integráciu nových služieb.

Aby bolo možné naplno využiť možnosti nového riešenia aplikácií na čipových kartách, vyvinuli sme vlastnú knižnicu prístupu k čipovým kartám, implementujúcu štandardy PKCS#11 a PKCS#15. Nová knižnica spĺňa všetky požiadavky predpísané zákonom pre elektronický podpis a prináša taktiež možnosť použitia zariadení na bezpečné zadávanie PINu pre ZEP.

Plaut Slovensko, s.r.o
Karloveská 34, 841 04 Bratislava
Slovenská Republika
Tel.: + 421 2 3215 1411
Fax: + 421 2 3215 1412
E-mail: info@plaut.sk
Web: www.plaut.sk