Smart karty

Dnes, keď informačné technológie nekompromisne a s veľkým tempom prenikajú do všetkých sfér bežného života, sa čoraz viac v rôznych situáciách stretávame s používaním inteligentných čipových kariet. Mnohé z nich zapĺňajú naše peňaženky, iné sa povaľujú doma. Často nevieme na čo slúžia, resp. akým spôsobom sa stávajú prínosom do nášho života. Okrem platobných kariet, ktoré sú dnes najčastejšie vybavené elektronickým čipom, pribúda čoraz viac elektronických dokladov, ako sú pasy, identifikačné doklady a osvedčenia o vozidle. Iné, bežnému obyvateľstvu bohužiaľ málo známe, sa používajú pre realizáciu zaručeného elektronického podpisu, autentifikáciu pri prístupe k elektronickým službám poskytovateľov služieb alebo šifrovanie.

Prínosy čipových kariet

Hlavným prínosom čipových kariet je bezpečnosť údajov v nich uložených. Bezpečnosť sa poníma z pohľadu samotného čipu – fyzická bezpečnosť, ako aj z pohľadu operačného systému – softvérová bezpečnosť. Svojou technológiou umožňujú čipové karty bezpečné uloženie dát rôzneho charakteru a účelu, dokážu ich nielen chrániť, ale zabezpečiť aj ich autenticitu. V závislosti od senzitivity údajov je možné pri prístupe k údajom čipovej karty požadovať rôzne stupne ochrany. Pri jednoduchších je to zadanie PIN, pri zložitejších moderné autentifikačné protokoly, ktoré nielen autentifikujú používateľa, ale poskytujú ďalšie možnosti pre vzájomné overenie autenticity terminálu a čipu – často nazývané ako „mutual authentication“.

Napríklad údaje uložené v platobnej karte, ako je meno a priezvisko držiteľa, číslo karty, termín platnosti, atď., sú pred vyčítaním chránené pomocou PIN, tzn. držiteľ zadaním PIN súhlasí s vyčítaním údajov z čipu, čím požadovanú transakciu autorizuje. Údaje v takomto čipe sú pred modifikáciou chránené elektronickým podpisom banky, ktorá platobnú kartu vydala. Niektoré karty sú vybavené aj prostriedkami pre ochranu pred kopírovaním ich obsahu – tzv. ochrana pred klonovaním.

Bezpečnosť

Nové čipové karty boli postupom technológie rozšírené o moderné kryptografické algoritmy, ktoré rozširujú nielen možnosti ochrany dát vo forme autentifikačných protokolov, ale umožňujú aktívne použitie čipových kariet pri elektronickej komunikácii občana so systémami verejnej správy –eGovernment. Na Slovensku sú takýmito napríklad pripravované elektronické identifikačné karty – eID. Doklad bude obsahovať údaje, ktoré môže čítať len oprávnený terminál. Terminál sa voči čipu autentifikuje protokolom tzv. terminálovej autentifikácie, ktorá umožní čipu vyhodnotiť oprávnenia terminálu pre prístup k uloženým údajom. Autenticita čipu a údajov v ňom uložených bude zabezpečená prostredníctvom čipovej autentifikácie, pri ktorej medzi čipom a terminálom vznikne zabezpečený šifrovaný kanál. Údaje je možné prečítať len so súhlasom držiteľa a to zadaním PIN. Terminál so špeciálnym oprávnením, nazývaný aj ako inšpekčný terminál, pristupuje k údajom dokladu bez súhlasu držiteľa. Jedná sa napr. o kontrolu osôb príslušníkmi polície.

Kombinácia spomenutých autentifikačných protokolov navyše umožňuje vytvoriť zabezpečený kanál medzi čipom dokladu eID a vzdialeným systémom, napr. serverom poskytovateľa elektronických služieb, čo serveru umožní autentifikovať a overiť identitu občana a tým ho autorizovať pre prístup k službám eGovernmentu.

Plánovaný spôsob riadenia prístupu v dokladoch eID umožní ich neskoršie rozšírenie o ďalšie služby, ktorými sú napr. zaručený elektronický podpis a šifrovanie.

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