Bezpečnostné mechanizmy

Basic Access Control, Pasívna a Aktívna Autentifikácia

Tromi bezpečnostnými mechanizmami definovanými normou ICAO sú: Basic Access Control (BAC), Pasívna Autentizácia (PA) a Aktívna autentizácia (AA). Mechanizmus Basic Access Control slúži na ochranu pred neautorizovaným prístupom k údajom uloženým v čipe. Umožňuje vybudovanie kryptografického kanála, ktorý chráni komunikáciu čipu s inšpekčným systémom pred neželaným odpočúvaním. Zároveň zabezpečuje, že inšpekčný systém môže údaje z čipu vyčítať len za predpokladu, že disponuje vybranými údajmi zaznamenanými v opticky čitateľnej zóne údajovej strany pasu. Týmto spôsobom BAC zabraňuje čítaniu obsahu bezkontaktných čipov z pasov náhodne okoloidúcich osôb.

Pasívna autentizácia (PA) chráni autenticitu a integritu údajov v čipe. Mechanizmus využíva elektronický podpis generovaný vo fáze personalizácie (zápisu údajov) čipu. Hoci je PA účinným prostriedkom pre zabezpečenie autenticity údajov v čipe, neumožňuje inšpekčnému systému overiť, či komunikuje s pôvodným čipom, alebo s kópiou, do ktorej mohol falšovateľ zapísať nezmenené údaje spolu s digitálnym podpisom vyčítaným z pravého pasu (tzv. klonovanie čipu).

Ochranu pred klonovaním čipu poskytuje tretí mechanizmus, ktorým je Aktívna autentizácia (AA). Využíva challenge-response protokol založený na asymetrickej kryptografii. Počas kontroly čip svojim (nevyčítateľným) privátnym kľúčom podpíše náhodný reťazec vygenerovaný inšpekčným systémom. Inšpekčný systém overí podpis pomocou verejného kľúča vyčítaného z čipu. Autenticitu verejného kľúča chráni vyššie zmienený mechanizmus pasívnej autentizácie.

Čipová a terminálová autentifikácia

Odporúčanie TR-03110 definuje ďalšie dva bezpečnostné mechanizmy, Čipovú a Terminálovú autentizáciu, súbežné uplatnenie ktorých je označované ako Extended Access Control (EAC). Čipová autentizácia (CHA) predstavuje alternatívu k (nepovinnému) mechanizmu Aktívnej autentizácie definovanému štandardom ICAO. Je založená na princípoch Diffie-Hellmanovského odvodenia zdieľaného tajomstva. Zabraňuje treťostrannému sledovaniu držiteľa pasu, pre ktoré je možné zneužiť AA a zároveň poskytuje silný kľúč pre zabezpečenie šifrovanej komunikácie medzi čipom a inšpekčným systémom.

Terminálová autentizácia (TA) umožňuje zamedziť neoprávnenému prístupu k citlivým údajom zapísaným v čipe. Pre autentizáciu terminálu inšpekčného systému je využitý challenge-response protokol. Slabým článkom TA je kontrola expirácie certifikátu inšpekčného systému. Čip totiž nemá stále napájanie a teda ani nepretržite idúce hodiny, pomocou ktorých by mohol určiť aktuálny dátum. EAC pre stanovenie dátumu využíva aproximačný mechanizmus založený na odvodení času z najčerstvejšieho platného certifikátu z reťaze certifikátov poskytovaných inšpekčným systémom.

EAC poskytuje vyššiu úroveň ochrany súkromia držiteľa pasu ako mechanizmy ICAO, na druhej strane však kladie väčšie nároky na technickú infraštruktúru a v súčasnosti nejde o celosvetovo akceptovaný štandard. Pasy vydávané členskými krajinami EU implementujú mechanizmy EAC kvôli ochrane prístupu k citlivým údajom, ako napríklad digitálna reprezentácia odtlačkov prstov držiteľa pasu.

Cestovné doklady

Cestovné doklady je možné využiť pri styku s verejnosťou (napr. v bankách, na poštách, úradoch atď.) ako prostriedok na jednoznačnú identifikáciu ich držiteľa. V rámci našich riešení ponúkame možnosť zakomponovať túto kontrolu a identifikáciu do informačných systémov a procesov front-office.

V uplynulom desaťročí mnohé krajiny sveta pristúpili k vydávaniu pasov vybavených elektronickými čipmi. Medzinárodne uznávaným štandardom v uvedenej oblasti je ICAO (International Civil Aviation Organization) Doc 9303 (elektronické pasy špecifikuje časť 1, zväzok 2).

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