

Smart Card Middleware

Smart Card Middleware (MW) umožňuje počítačovým aplikáciám komunikovať s čipovými kartami použitím štandardizovaných aplikačných programovacích rozhraní (API).



Architektúra MW a jeho funkcionality je založená na príslušných medzinárodných štandardoch a technických smerniciach, obzvlášť na

- ISO/IEC 24727 Identification cards - ICC programming interfaces
- CEN 15480-3 European Citizen Card – ECC Interoperability using an application interface
- BSI TR-03112 eCard-API-Framework

Nízkoúrovňové implementačné vlastnosti a špecifiká jednotlivých čipových kariet sú klientskej aplikácii skryté vďaka jednotnému aplikačnému programovaciemu rozhraniu (API).

Middleware zásobník je definovaný abstraktnými vrstvami zaisťujúcimi interoperabilitu. ISO/IEC 24727 MW abstraktné vrstvy sú:

- Service Access Layer (SAL) má na starosti interpretáciu žiadostí adresovaných klientskou aplikáciou karte cez vysokoúrovňové API (SAL-API) špecifikované v ISO/IEC 24727-3.
- Generic Card Access Layer (GCAL) má na starosti preklad APDU príkazov pre čipovú kartu zo SAL vrstvy. GCAL vrstva je špecifikovaná v ISO/IEC 24727-2.
- ISO/IEC 24727 architektúra Smart Card MW umožňuje webovým aplikáciám bežiacim na serveri poskytovateľa služieb komunikovať so vzdialenou čipovou kartou prostredníctvom zabezpečeného komunikačného kanála.

Kľúčové vlastnosti

- API čipových kariet:
 - > Cryptoki (PKCS#11)
 - > SAL (ISO/IEC 24727-3)
 - > Microsoft CryptoAPI
- Architektúra umožňuje bezpečnú komunikáciu so vzdialenou čipovou kartou
- Podporované OS platformy:
 - > Windows
 - > Linux
 - > Mac OS X

Hlavné výhody

- Štandardné rozhrania umožňujú počítačovým aplikáciám komunikáciu s rôznymi čipovými kartami jednotným spôsobom
- Webové aplikácie môžu komunikovať so vzdialenou čipovou kartou bezpečným kanálom, vďaka ktorému môžu napríklad vypočítať identitu občana alebo obnoviť kvalifikované certifikáty na karte
- Dostupné väčšine užívateľom (multiplatformová podpora)
- Jednoduchá integrácia nových typov čipových kariet