

Karty elektroniczne

Krzysztof Maćkowiak

Historia kart elektronicznych

Początek kart elektronicznych sięga lat siedemdziesiątych. W roku 1970 japoński wynalazca Kunitaka Arimura jako pierwszy opatentował „plastikową kartę zawierającą jeden lub więcej układów scalonych do generowania określonych sygnałów”. Przełomową datą okazał się jednak rok 1974, kiedy to Roland Moreno opatentował tzw. „niezależny obiekt elektroniczny z pamięcią”.

Pierwsza karta bez mikroprocesora opracowana została w roku 1976 przez Honeywell Bull we współpracy z Motorolą. Dwa lata później zbudowano kartę z mikroprocesorem. W roku 1986 stworzono pierwszy standard dla kart elektronicznych – ISO/IEC 7816-1.

Karty elektroniczne znalazły szerokie zastosowanie w usługach bankowych i telekomunikacyjnych już w latach 80-tych.

Budowa kart elektronicznych

Na kartach elektronicznych w plastikowym podłożu osadzony jest jeden lub wiele układów elektronicznych.

Elementy znajdujące się w karcie elektronicznej:

- pamięć modyfikowalna (EEPROM),
- pamięć niemodyfikowalna (EPROM),
- pamięć RAM
 - dynamiczna – DRAM,
 - statyczna – SRAM,
- pamięć ROM (z systemem operacyjnym niezbędnym do funkcjonowania mikroprocesora),
- mikroprocesor
 - 8-bitowy,
 - 16-bitowy,
- układy we/wy,
- układy pomocnicze.

Porównanie kart elektronicznych i magnetycznych

Karty elektroniczne w przeciwieństwie do kart magnetycznych, dzięki zastosowaniu pamięci modyfikowalnych, umożliwiają wielokrotny zapis danych na karcie. Cechuje je również większa ilość pamięci, co wiąże się z zaawansowanymi możliwościami. Karty elektroniczne są trwalsze od kart magnetycznych i dzięki wbudowanemu mikroprocesorowi umożliwiają dokonywanie operacji logicznych i matematycznych. Karty magnetyczne cechuje brak zabezpieczeń przed odczytem zapisanych danych. W przypadku kart elektronicznych mamy możliwość m.in. kontroli dostępu do pamięci oraz weryfikacji autentyczności karty. Dodatkowo korzystając z wbudowanego koprocatora arytmetycznego można implementować w karcie silne algorytmy kryptograficzne. Mikroprocesor zapewnia również kontrolę odczytu i zapisu danych umieszczonych w pamięci np. poprzez numer PIN. Wadą karty elektronicznej jest potrzeba dostarczenia zasilania.

Komunikacja karta-czytnik

Karty elektroniczne ze względu na sposób komunikacji z układami zewnętrznymi dzielimy na karty:

- stykowe – w celu korzystania z karty należy ją włożyć do czytnika,
- bezstykowe – wystarczy, że karta będzie w pełnej odległości od czytnika.

W przypadku kart bezstykowych dane przesyłane są drogą radiową. Zasilanie następuje z zewnętrznej baterii lub poprzez pobudzenie cewek polem elektromagnetycznym. Zasięg takich kart wynosi od kilku mm do ponad 2 metrów. Karty te uważane są za mniej bezpieczne od kart stykowych, ponieważ transmisja może zostać podsłuchana drogą radiową. W celu przeciwdziałania podsłuchowi korzysta się z algorytmów kryptograficznych.

Karty mogą zawierać zarówno interfejs stykowy jak i bezstykowy. Oprócz układów scalonych na karcie można również umieścić pasek magnetyczny.

Zabezpieczenie kart elektronicznych [2]

W celu zwiększenia bezpieczeństwa przechowywanych danych oraz podczas ich przesyłania wprowadza się algorytmy kryptograficzne:

- szyfrowanie symetryczne
 - DES,
 - IDEA,
- szyfrowanie asymetryczne
 - RSA,
 - ECC,
- podpis cyfrowy
 - RSA,
 - ECDSA,
- funkcje jednokierunkowe
 - SHA,
 - MD5.

W celu przyspieszenia obliczeń stosowane są koprocessory arytmetyczne.

Programowanie kart elektronicznych

Językiem programowania wykorzystywanym najczęściej w kartach elektronicznych jest język Java. Precyzyjnie mówiąc, jest to jego okrojona wersja przeznaczona specjalnie do programowania kart elektronicznych, nosząca nazwę Java Card. Ograniczenia zostały wprowadzone ze względu na ograniczoną pojemność pamięci.

Sterowniki Java Viryual Machine znajdują się w pamięci ROM. Natomiast Java Application Programming Interfaces (Java API) wraz z plikami i apletami umieszczone są w pamięci EEPROM.

Zastosowanie kart elektronicznych

Karty elektroniczne znajdują swoje zastosowanie w wielu dziedzinach życia:

- bankowość,
- telekomunikacja,
- handel,
- sieci GSM (karty SIM),
- szkolnictwo,
- płatne usługi TV (dekodery telewizji kablowej),
- służba zdrowia,
- systemy ubezpieczeń,
- systemy opieki społecznej,
- komunikacja i transport.

Dzięki usługom kryptograficznym używane są w celu uwierzytelnienia oraz autoryzacji w przedsiębiorstwach i instytucjach. Mogą być również stosowane do składania podpisów elektronicznych.

Literatura

1. Kubas Monika, Molski Marian, *Karta elektroniczna. Bezpieczny nośnik informacji*. MIKOM 2002.
2. Maćkowiak Krzysztof, *Bezpieczeństwo kart elektronicznych*. 2003.