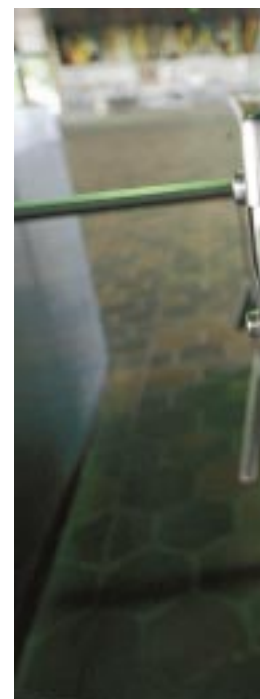


Inteligentne karty

*Dzięki komputerom elektroniczne portfele zawładną wkrótce
wszystkimi dziedzinami naszego życia*

Carol H. Fancher



Rewolucja półprzewodnikowa doprowadziła do tego, że moc obliczeniowa, wytwarzana niegdyś w urządzeniach wielkości pokoju, mieści się teraz w kieszeni wśród drobnych monet, kluczy i papierków po cukierkach. „Inteligentne” karty kredytowe z mikroskopijnymi układami półprzewodnikowymi są od ponad 10 lat używane we Francji i w innych częściach Europy. Ze staw znormalizowanych styków na przedniej stronie każdej karty zastępuje lub uzu-



pełnia znany nam pasek magnetyczny na jej odwrocie. Stany Zjednoczone jak dotąd pozostają w tyle, jeśli chodzi o stosowanie kart tego typu, ale seria trwających obecnie programów pilotażowych może wkrótce zmienić tę sytuację. Złośliwcy twierdzą, że dla inteligentnych kart bez końca poszukuje się sensownych zastosowań, jednakże rozmaite doświadczenia różnych państw dowodzą, że sprawa jest znacznie bardziej skomplikowana.

Ciekawe, że największy wpływ na wdrażanie inteligentnych kart miała polityka telekomunikacyjna. W Stanach Zjednoczonych, gdzie rozmowy telefoniczne są tanie, a podłączenie czytnika pasków magnetycznych do linii telefonicznej – proste, nie widzi się konieczności ponoszenia dodatkowych kosztów, by ograniczyć piractwo telefoniczne. Zamiast tego sprzedawca może przed zrealizowaniem transakcji zadzwonić do centralnej bazy danych, aby upewnić się, czy karta jest ważna. W Europie, gdzie rozmowy są droższe, a podłączenie do linii telefonicznych urządzeń wyposażonych w modem trudniejsze, kwestie bezpieczeństwa skłaniały do wprowadzenia inteligentnych kart.

Francja na przykład przeszła na ten system w połowie lat osiemdziesiątych, ponieważ piractwo przyjęło ogromne rozmiary i wciąż rosło. W przypadku inteligentnych kart sprzedawcy nie muszą mieć dostępu on-line do centralnych baz danych. Mogą opierać się na osobistym numerze identyfikacyjnym (PIN – personal identification number), który klient musi wpisać, by komputer zweryfikował jego zgodność z zapisanym na karcie. Układy półprzewodnikowe są ponadto trudniejsze do podrobienia niż paski magnetyczne, które można odczytywać i zapisywać za pomocą łatwo dostępnych urządzeń. We Francji jest obecnie w obiegu około 20 mln inteligentnych kart.

Jednym z argumentów za wprowadzeniem inteligentnych kart w USA jest obecnie możliwość wykorzystania jednej karty do różnych celów. Teoretycznie ten sam wzbogacony układami półprzewodnikowymi kawałek plastiku posłuży do identyfikacji osób, jako karta kredytowa, karta do bankomatów, karta telefoniczna, bilet komunikacyjny, nośnik podstawowych informacji medycznych oraz ekwiwalent gotówki w niewielkich transakcjach zawieranych

W ATLANCIE (GEORGIA) dokonano największego jak dotąd testu inteligentnych kart w USA. W związku z Igrzyskami Olimpijskimi '96 sprzedano ich ponad milion. Posługiwano się nimi w obiektach olimpijskich oraz restauracjach i sklepach na terenie miasta, a także w metrze.



INTELGENTNA KARTA zawiera pod złotymi stykami kontaktowymi pamięć i procesor. Ułożenie styków jest znormalizowane, tak aby karty i czytniki pochodzące z różnych źródeł mogły ze sobą współpracować.

osobiście lub za pośrednictwem Internetu. Inne zastosowania zależą już tylko od wyobraźni projektantów i od akceptacji klientów. W miarę jak pojedyncza karta będzie mogła przechowywać więcej informacji dotyczących naszego życia, staniemy przed problemami bezpieczeństwa i poufności; w przyszłości karty będą prawdopodobnie wysoce zindywidualizowane.

Międzynarodowe standardy

Atrakcyjność inteligentnych kart wzrasta wraz ze spadkiem cen mocy obliczeniowej mikrokomputerów i pamięci. Pod dwoma względami górują one nad kartami z paskiem magnetycznym. Po pierwsze, przechowują 10, a nawet 100 razy więcej informacji – i to bezpieczniej. Po drugie, w połączeniu z terminalem mogą wykonywać złożone zadania. Inteligentna karta na przykład porozumiewa się z czytnikiem, odpowiadając na szereg pytań, a także je zadając.

Pozwala to sprawdzić ważność informacji na niej zapisanych oraz „tożsamość” terminala-czytnika kart. Karta działająca według takiego algorytmu może bez ujawniania aktualnego salda czy numeru konta „przekonać” terminal, że jej posiadacz ma wystarczającą ilość pieniędzy na pokrycie kosztów transakcji. W zależności od wagi informacji stosowane są różne sposoby zabezpieczenia danych: od osobistego numeru identyfikacyjnego, takiego jak w bankomatach, poprzez system szyfrowania średniej klasy, taki jak Data Encryption Standard (DES), do bardzo skutecznej metody opartej na kluczu publicznym.

Inteligentne karty nie są pomysłem nowym. Prace nad nimi rozpoczęły się

pod koniec lat siedemdziesiątych. Znalazły one zastosowania w Europie, gdzie dotąd wyprodukowano ich ponad ćwierć miliarda sztuk. Większość układów umieszczono w opłacanych z góry kartach telefonicznych służących tylko raz, do chwili wyczerpania określonej liczby jednostek, mimo to uzyskane doświadczenie pozwoliło zmniejszyć koszty produkcji i podnieść niezawodność inteligentnych kart oraz udowodniło ich przydatność.

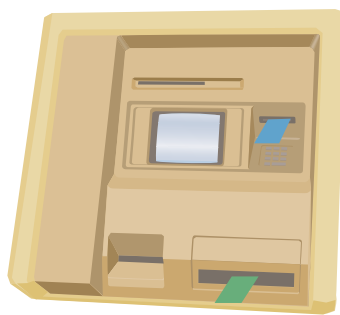
Prace nad międzynarodowymi i krajowymi standardami, które mają zapewnić bezusterkową i bezpieczną współpracę kart, czytników i oprogramowania są zaawansowane. Na przykład standardy ustanowione przez Międzynarodową Organizację ds. Standardów (ISO – International Organization for Standardization) narzucają umiejscowienie styków na przedniej stronie karty i zapewniają jej połączenie z każdym czytnikiem.

Opracowywane są standardy branżowe kart w tak różnorodnych zastosowaniach, jak cyfrowe telefony komórkowe, telewizja satelitarna i kablowa oraz oczywiście operacje finansowe. Niedawno Visa, MasterCard i Europay porozumiały się w sprawie wspólnej specyfikacji inteligentnych kart, określającej podstawowe protokoły komunikacji między kartami i czytnikami (analogicznie do standardów RS-232, ustalających metody komunikacji między komputerami osobistymi a modemami). Specyfikacja jest wystarczająco ogólna, aby niemal każdy rodzaj informacji mógł być wymieniany przez zgodny z nią sprzęt i oprogramowanie. Dzięki temu użytkownicy będą mogli korzystać z tej samej karty przy zakupach, pobieraniu pieniędzy z bankomatów, gromadzeniu punktów w programach linii lotniczych dla stałych pasażerów, a nawet łączeniu się z Internetem.

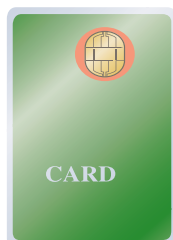
Pod maską

Standardy określają kształt karty i układ połączeń elektrycznych, jednakże technologia wykonania znacznie się rozwinęła. Najprostsze karty „pamięciowe” zawierają tylko trwałą pamięć i ograniczoną liczbę obwodów logicznych do sterowania i zabezpieczania. Służą one zwykle jako opłacone z góry karty telefoniczne – terminal wewnątrz automatu telefonicznego zmniejsza w trakcie rozmowy saldo w pamięci karty; gdy jednostki na karcie się wyczerpią, staje się ona bezużyteczna.

Inteligentne karty są bardziej złożone – zawierają układ z procesorem i różnego rodzaju komórkami pamięci trwałej



AUTOMAT SPRZEDAJĄCY
KARTY GOTÓWKOWE



INTELIGENTNA KARTA

MICHAEL GOODMAN

i ulotnej. Niektóre wersje mogą być również wyposażone w specjalny układ do operacji kryptograficznych, przyspieszający kodowanie i dekodowanie komunikatów lub generowanie podpisów cyfrowych służących do potwierdzenia przekazywanych informacji: [patrz: Thomas Beth, „Poufność w Internecie”; *Świat Nauki*, luty 1996, oraz David Chaum, „Osiągnąć elektroniczną dyskrecję”; *Świat Nauki*, październik 1992]. Standardy nie ograniczają mocy procesora na karcie, dany układ musi jedynie zmieścić się w przeznaczonym dla siebie miejscu pod stykami kontaktowymi.

Ceny dzisiejszych inteligentnych kart, produkowanych przez firmy takie jak Giesecke & Devrient, Gemplus, Schlumberger i Solaic, wahają się od poniżej dolara do około 20 dolarów. (Układy elektroniczne wewnątrz kart wytwarzają firmy takie jak Motorola, Siemens i SGS-Thompson.) Dla porównania: karta z paskiem magnetycznym może kosztować od 10 do 50 centów w zależności od tego, czy jest na niej zdjęcie lub hologram, czy też nie, oraz od wielkości jednorazowej emisji.

Ponieważ karty są zasilane z zewnątrz poprzez złącze czytnika, informacja przechowywana w zwykłej pamięci RAM ulegałaby zatarciu przy każdorazowym wyjmowaniu karty z czytnika. Mikroprocesory inteligentnych kart wykorzystują zaledwie kilkadziesiąt bajtów pamięci RAM jako notatnik do pracy nad przebiegiem transakcji. Oprogramowanie kontrolujące pracę karty musi przetrwać do następnego użycia karty, tak więc zajmuje ono 3–20 KB trwałej pamięci tylko do



odczytu (ROM). Zawartość pamięci ROM jest zapisywana w układzie w trakcie jego produkcji. Dane osobiste, finansowe lub medyczne, dzięki którym karta staje się cenna dla jej właściciela, znajdują się w pamięci trwałej, której zawartość można zmieniać (EEPROM – electrically erasable programmable read-only memory – elektronicznie kasowalna, programowalna pamięć tylko do odczytu) o pojemności od jednego do 16 KB.

Potrzeba zapewnienia bezpieczeństwa danych wpływa na konstrukcję i sposób posługiwania się kartą, wbudowane układy logiczne oraz oprogramowanie. Mikroprocesory w inteligentnych kartach opracowuje się specjalnie z myślą o ograniczeniu dostępu do zapisanej w nich informacji oraz uniemożliwieniu korzystania z karty przez osoby nie upoważnione. Zwykle karta działa tylko w odpowiednich środowiskach operacyjnych.

Osuźni mogą na przykład próbować użyć karty poza pewnym zakresem napięcia lub częstotliwości zegara w nadziei odkrycia i wykorzystania jej słabych stron; w takich warunkach odpowiednio skonstruowane urządzenie przestanie reagować automatycznie. W pewnych przypadkach można tak zaprojektować połączenia układów, aby po zaprogramowaniu karty już nie działały, uniemożliwiając w ten sposób modyfikację podstawowych danych. Producenci stosują również specjalne rozwiązania techniczne, które nie pozwalają złodziejowi na bezpośrednie dotarcie do mikroskopijnych układów.

CO DZIEJE SIĘ W CZYTNIKU KART

1 WKŁADAMY KARTĘ

2 ZASILANIE DOCIERA DO KARTY

3 KARTA I CZYTNIK DOKONUJĄ WZAJEMNEJ IDENTYFIKACJI

4 KLIENT POTWIERDZA ŻĄDANĄ KWOTĘ

5 ODPOWIEDNIA KWOTA PRZEKAZYWANA JEST Z KARTY DO CZYTNIKA

6 CZYTNIK NAKAZUJE KARCIE ZAPISAĆ NOWE SALDO: WARTOŚĆ KARTY ZMNIJEJSA SIĘ O KWOTĘ ZAKUPU

7 KARTA ZOSTAJE ODŁĄCZONA; CZYTNIK ZWRACA KARTĘ

CZYTNIK PRZEKAZUJE INFORMACJĘ DO BANKU; BANK PRZESYŁA PIENIĄDZE NA KONTO SPRZEDAWCY



CZYTNIK INTELIGENTNYCH KART



Większość inteligentnych kart wymaga bezpośredniego połączenia ze stykami czytnika, coraz częściej jednak stosowane są tzw. karty bezkontaktowe. Krótkozakresowe karty działają dzięki elektrycznemu sprzężeniu indukcyjnemu lub pojemnościowemu z czytnikiem, od którego karta jest oddalona o mniej więcej milimetr. Karty o dłuższym zasięgu komunikują się z czytnikiem drogą radiową. (Energia fal radiowych emitowana przez czujnik jest również źródłem zasilania kart, tak więc muszą one gospodarować nią wyjątkowo oszczędnie.) Inteligentne karty bezkontaktowe często stosuje się w sytuacjach, gdy operacje muszą być prze-

prowadzane bardzo szybko, na przykład w bramkach wejściowych (kołowodach), przez które przechodzi bardzo dużo osób. Operatorzy takich systemów w Hongkongu, Waszyngtonie, Manchesterze i kilkunastu innych miastach testują karty bezkontaktowe; Hongkong wyda do 1997 roku 3 mln takich kart.

Twórcy i użytkownicy wspólnie opracowują niezawodne standardy kart bezkontaktowych dalekiego zasięgu. Prowadzone są również prace nad znormalizowaniem kart hybrydowych, które mogłyby komunikować się albo bezpośrednio, albo przez łącza radiowe. Luftansa, niemiecka linia lotnicza, zaczęła już wydawać stałym klientom karty hybrydowe; część bezkontaktowa działa jako karta identyfikacyjna w elektronicznym systemie biletowym firmy, natomiast kontakty są zgodne z europejskim standardem inteligentnej karty kredytowej. Do końca roku do obiegu trafi około 350 tys. takich kart.

Inteligentne karty to osiągnięcie techniczne samo w sobie; są one jednak tylko najbardziej widoczną częścią du-

SWINDON W ANGLII to miejsce trwającego nieprzerwanie testu Mondexu, systemu „elektronicznej portmonetki”, w którym inteligentne karty przechowują gotówkę w postaci cyfrowej. Mondex pozwala na przekazywanie elektronicznych pieniędzy z ręki do ręki, bez pośrednictwa banku. Co czwarty mieszkaniec Swindon korzysta już z takiej karty w sklepach, restauracjach, pralniach i kioskach. Inny test rozpoczyna się jesienią w Guelph w prowincji Ontario w Kanadzie, gdzie karty będą przyjmowane nawet przez parkometry.

KARTY GOTÓWKOWE są elektronicznym ekwiwalentem czeku podróżnego. Można nimi płać na przykład za przekąski lub parkowanie. Klienci kupują w automacie karty naładowane pewną wartością nominalną i korzystają z nich w niewielkich transakcjach. Czytniki kart okresowo przekazują informacje do banku, który przelewa odpowiednie kwoty na konto sprzedawcy bezpośrednio lub poprzez izbę rozrachunkową. Bardziej złożone karty gotówkowe mogą być powtórnie ładowane; zwykle są bezużyteczne po wykorzystaniu znajdującej się na nich gotówki.

żego systemu handlowego, w który są wmontowane. Właściwości tej infrastruktury mogą w znacznie większym stopniu wpływać na upowszechnienie kart niż cechy samej karty. Aby więc zrozumieć, co decyduje o przydatności karty, trzeba wiedzieć, jak będzie ona działać w systemie.

Rozważmy na przykład kartę gotówkową, najpowszechniejszą z obecnych kart procesorowych. Jej atrakcyjność polega na tym, że nie pociąga za sobą kosztów dodatkowych, które towarzyszą innym formom płatności, takim jak karty kredytowe czy gotówka. Nawet w Stanach Zjednoczonych koszty weryfikacji są zbyt wysokie, aby kilkudolarowe transakcje za pomocą dotychczas używanych kart były opłacalne.

Zamiast banknotów

Karta gotówkowa minimalizuje koszty, ponieważ nie działa wyłącznie jako „wskaźnik” do konta, ale bezpośrednio przechowuje wartość pieniężną. Przekazuje ona cyfrowy odpowiednik banknotów lub monet do cyfrowej „kasy” sprzedawcy, po czym pieniądze trafiają do banku. Kart takich mogą używać dzieci, turyści i inne osoby nie mające konta w miejscowym banku. Można je nawet nabywać w automatach.

Karty gotówkowe są szczególnie przydatne w automatach telefonicznych, parkometrach, kserokopiarkach i automatach sprzedających. Dzięki likwidacji pojemnika na monety urządzenia te przestają wabić złodziei i wandalów. Cyfrowe kasy trzeba oczywiście zabezpieczyć zarówno przed opróżnieniem przez niepowołane osoby, jak i wypełnieniem fałszywymi pieniędzmi elektronicznymi, ale łatwiej to w nich uzyskać niż w rozwiązaniach tradycyjnych.

Odejście od posługiwania się pieniędzmi w formie banknotów lub monet może przynieść znaczne oszczędności. Ekonomści szacują, że liczenie, przesyłanie, przechowywanie i ochrona gotówki kosztuje około 4% wartości wszystkich transakcji. Korzyści banków płyną również



MONDEX

Niektóre zastosowania inteligentnych kart

RODZAJ I MIEJSCE	LICZBA	ZASIĘG
Karta gotówkowa <i>MasterCard Cash</i> , Canberra	Wydano 10 tys.	Wprowadzone w marcu 1996 roku. Z kart można korzystać w 250 sklepach
Karta gotówkowa <i>VisaCash</i> , Atlanta	Ponad milion	Karty używane w obiektach olimpijskich, miejskiej komunikacji oraz w kilku tysiącach sklepów
Karta gotówkowa <i>Proton</i> , Belgia, Holandia, Brazylia, Australia	Wydano 90 tys.	Wprowadzane są na wielką skalę
Karta opieki socjalnej; <i>Social Security ID card</i> , Hiszpania	Wydano 500 tys.; do końca 1997 roku – 7 mln; do 2001–40 mln	Wprowadzane są na wielką skalę. Zapewniają usługi medyczne, a tożsamość posiadacza jest weryfikowana na podstawie odcisków palców
Karta identyfikacyjna, <i>Citizen ID card</i> , Korea Płd.	Wydano 1500	Projekt pilotażowy. Karta zastępuje dowód tożsamości, prawo jazdy oraz książeczkę ubezpieczeniową
Karta ubezpieczenia medycznego, <i>Health insurance card</i> , Niemcy	Wydano 80 mln	Wprowadzono w 1994 roku wyłącznie w celach identyfikacji
Karta zdrowia, <i>Health insurance card</i> , Unia Europejska	Od 1996 roku emisja 200 tys. kart	Projekty pilotażowe kart zawierających wyłącznie najważniejsze informacje o stanie zdrowia
Bezkontaktowe karty przejazdowe, <i>Contactless transit farecard</i> , Hongkong	Wydano 20 tys.; 3 mln do 1997 roku	Projekt pilotażowy rozpoczęty w listopadzie 1995. Trwa wprowadzanie w całym systemie komunikacyjnym
Karta identyfikacyjno-gotówkowa, <i>ID and stored-value card</i> , Washington University, St. Louis	Wydano 12,5 tys.	W obiegu. Z kart można korzystać w automatach, pralniach i innych punktach, gdzie zawiera się transakcje o niskiej wartości. Służą one również jako identyfikatory przy wchodzeniu do budynków kampusu.

LISA BURNETT

ŹRÓDŁO: *CardTech/SecurTech '96 Conference Proceedings, Atlanta*

z mniejszej wypłaty odsetek klientom przechowującym pieniądze w gotówce zamiast na koncie. Royal Bank of Canada, uczestniczący w próbach z cyfrowymi pieniędzmi w Ontario, dysponuje stale około miliardem dolarów.

Koszty transakcji zawieranej za pomocą karty gotówkowej są niższe niż w przypadku kart kredytowych i gotówki, jednakże początkowe inwestycje – wyższe. Same karty są droższe, a ci, którzy pierwszy je zastosują, muszą ponieść koszty zainstalowania sieci czytników. Ponadto oprogramowanie do przeprowadzenia transakcji za pomocą kart kredytowych i debetowych musi być dostosowane do nowej formy płatności, która przypomina raczej cyfrowy czek podróżny. Zwykły czytnik inteligentnych kart kosztuje około 100 dolarów, co jest porównywalne z ceną skrzynki, która odczytuje karty z paskiem magnetycznym i dzwoni do firmy obsługującej karty kredytowe w celu potwierdzenia transakcji. W USA jest przeszło 13 tys. czytników inteligentnych kart, natomiast urządzeń obsługujących zwykłe karty kredytowe – więcej niż 5 mln.

Ponad 20 firm pracuje nad czytnikami inteligentnych kart; dzięki ich masowej produkcji ceny niewątpliwie spadną. Trzeba jednak zainstalować pokątną liczbę tych urządzeń. Poza Stanami Zjednoczonymi liczba kart gotówkowych stale wzrasta. Programy na dużą

skalę są wdrażane lub planowane w Australii, Chile, Danii, Hiszpanii, Kanadzie, Kolumbii, Portugalii, Singapurze, na Tajwanie, w Wielkiej Brytanii, we Włoszech i w innych krajach. Stopień akceptacji przez klientów jest różny; karty zapewniają potencjalne oszczędności bankom i sprzedawcom, ale przekształcenie tych korzyści na zachęty dla użytkowników może być trudne. Banki centralne obawiają się również czegoś, co jest w końcu nową metodą drukowania pieniędzy przy braku ustalonych reguł mówiących o tym, która instytucja gwarantuje ich wartość.

Większość kart gotówkowych znajdujących się obecnie w obiegu służy tylko raz, do chwili wyczerpania określonej kwoty. Urządzenia z możliwością ponownego załadowania będą działały w ten sam sposób, jeśli idzie o dokonywanie zakupów, ale zostaną wyposażone w dodatkowe oprogramowanie, pozwalające klientowi na przeniesienie pieniędzy na pustą już kartę. (Szyfrowanie lub inne techniki zabezpieczające zapewnią ładowanie karty tylko w wyniku dozwolonej transakcji.) Citibank, Chase Manhattan, Visa i MasterCard opracowują program pilotażowy kart gotówkowych dla Nowego Jorku. Firmy wydadzą ładowalne inteligentne karty około 50 tys. klientów; karty te będą też miały paski magnetyczne do zwykłych transakcji. W około 500

sklepach, restauracjach i innych punktach handlowych zostaną zainstalowane czytniki akceptujące transakcje cyfrowymi pieniędzmi. Ponad milion kart gotówkowych wyemitowano na Igrzyska Olimpijskie '96 w Atlancie; można z nich było korzystać w obiektach olimpijskich i w kilku tysiącach okolicznych sklepów.

Wiele grup przygotowuje konkurencyjne projekty inteligentnych kart gotówkowych. Wszystkie wymagają w zasadzie takiego samego sprzętu, ale różnią się oprogramowaniem. Producenci czytników kart opracowują więc urządzenia, które mogą obsługiwać wiele różnych protokołów. Nie wiadomo jeszcze, który system popraczą klienci; każdy z nich ma swoje wady i zalety. Protokoły kart gotówkowych stosowane w pilotażowych programach w Nowym Jorku i w Atlancie są stosunkowo proste, ale mają słabe punkty – nie przewidziano na przykład możliwości unieważnienia lub wymiany karty zgubionej czy ukradzionej. System DigiCash, oparty na złożonych protokołach kryptograficznych, jest bezpieczny i nie można go podrobić, ale wymaga większej mocy obliczeniowej, a więc karty są droższe. Natomiast British Mondex jest pomyślany jako bezpieczny ekwiwalent gotówki w pełnym zakresie: elektroniczne pieniądze mogą bez końca przechodzić od jednego użytkownika do drugiego bez przekazywania ich po drodze do banku. Testy odbywają się w Swindon w południowo-zachodniej Anglii, a inne rozpoczynają się w Guelph w prowincji Ontario (Kanada), gdzie nawet parkometry będą przyjmowały cyfrową walutę.

Ochrona zdrowia

O wszechstronności tej technologii świadczy to, że inteligentne karty mogą również przenosić ważne dane dotyczące ochrony zdrowia, na przykład szczegółowe informacje na temat ubezpieczenia medycznego użytkownika. Można także umieścić na kartach podstawowe fakty o stanie jego zdrowia, spis leków, na które jest uczulony, obecnie leczone dolegliwości, nazwisko i numer telefonu lekarza pacjenta oraz inne zapisy pomocne w razie wypadku. Inteligentna karta, która przechowuje tylko wiadomości najbardziej istotne dla obecnego leczenia, znacznie upraszcza formalności związane z opieką medyczną. Możliwe byłoby dalsze ułatwienia, np. gdyby urzędnicy służby zdrowia spróbowali umieścić w systemie informacyjnym pełną historię chorób i leczenia pacjenta. Wówczas jednak pojawiłyby się skomplikowane kwestie poufności i własności.

Tak naprawdę nawet zautomatyzowanie wprowadzania nazwiska i numeru konta pacjenta do formularzy medycznych może znacznie przyspieszyć procedury związane z ubezpieczeniem medycznym. Niemcy rozpoczęli niedawno wydawanie wszystkim obywatelom kart procesorowych zawierających podstawowe informacje o ich ubezpieczeniach medycznych, a Francja rozpatruje podobny program. Oba kraje zdecydowały się nie przechowywać na kartach bardziej osobistych danych, dopóki nie zostaną rozwiązane problemy prawne, etyczne i dotyczące bezpieczeństwa.

We Francji i w Japonii ludzie chorzy na nerki mogą nosić przy sobie karty zawierające dane o dializach i prowadzonym leczeniu. Pacjenci nierzadko muszą być poddawani dializie dwu- lub trzykrotnie w ciągu tygodnia. Za każdym razem trzeba właściwie ustawić parametry maszyny do dializy i podać odpowiedni zestaw leków. Przed wprowadzeniem inteligentnych kart pacjenci mogli korzystać tylko z miejscowego centrum dializy, gdzie przechowywane były dotyczące ich informacje, natomiast obecnie mogą poruszać się równie swobodnie jak większość z nas. Zabezpieczenia karty chronią informacje o leczeniu przed ich odczytaniem lub zmianą przez nie upoważnione osoby.

Koszty telekomunikacyjne wynikające z potrzeby weryfikacji transakcji zawieranych za pośrednictwem kart kredytowych przyczyniły się zasadniczo do rozwoju inteligentnych kart. Nie dziwi więc, że karty te wykorzystano w nowej generacji komunikacji przenośnej. Global System of Mobile Communications (GSM – Globalny System Komunikacji Przenośnej) to specyfikacja techniczna cyfrowych telefonów komórkowych; około 10 mln osób dysponuje telefonami GSM, a usługa ta jest dostępna lub wprowadzana w ponad 85 krajach. Wszystkie aparaty GSM akceptują inteligentne karty, zawierające oprócz numeru telefonu właściciela spis usług, z których może on korzystać. Podróżujący szwajcarski menedżer może po prostu wyjąć inteligentną kartę ze swojego domowego telefonu i włożyć ją do wypożyczonego aparatu w Belgii. Gdy

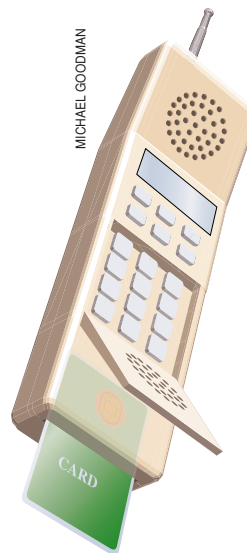
dzwoniący wybierają jego numer, system komórkowy automatycznie odnajduje aparat z jego inteligentną kartą w dowolnym miejscu na świecie i łączy z nim rozmowę. Poza tym inteligentna karta umożliwia szyfrowanie rozmowy, zapobiegając jej podsłuchiowaniu.

Podobnie jak w innych zastosowaniach inteligentnych kart Stany Zjednoczone plasują się pod względem usług GSM w tyle za wieloma innymi krajami. Wdrożenie na szeroką skalę kilku projektów pilotażowych nie nastąpi z pewnością przed 1997 rokiem. Systemy GSM budowane w USA działają na częstotliwości 1.9 GHz zamiast stosowanej powszechnie częstotliwości 1.8 GHz i wykorzystują dwie konkurencyjne, niezgodne ze sobą technologie. W efekcie aparaty mogą być bezużyteczne poza swoim rodzimym obszarem. Natomiast inteligentne karty powinny działać wszędzie.

Czy inteligentne karty, mogące nadać „tożsamość” urządzeniu elektronicznemu, posłużą kiedyś jako niezawodne listy uwierzytelniające dla ludzi? Inteligentne karty mogą przechować o wiele więcej informacji niż kawałki papieru lub plastiku, na których znajdują się nasze prawa jazdy, legitymacje ubezpieczeniowe czy inne dokumenty tożsamości. Prawdopodobnie te informacje będą przechowywane bezpiecznie.

Karty, które cię znają

Karty identyfikacyjne zawierają często zdjęcie i podpis posiadacza stanowiące dla odpowiednich urzędów potwierdzenie, że okaziciel jest jej rzeczywistym właścicielem. Aby zwiększyć stopień bezpieczeństwa, inteligentne karty mogą zawierać PIN oraz wiele identyfikatorów biometrycznych: próbki głosu, odciski palców, zdjęcia siatkówki lub tęczęwki oka, a także sposób składania podpisu. Porównując cechy okaziciela z danymi zapisanymi na karcie, komputery mogą określić dokładnie, czy jest on jej właścicielem. Urzędy celne w Holandii przetestowały już system przyspieszający kontrolę paszportową na lotnisku dla stałych klientów: osoba kładzie palec na szkla-



TELEFONY KOMÓRKOWE oparte na standardzie GSM są bezużyteczne bez inteligentnej karty, która przechowuje numer telefonu abonenta oraz inne dotyczące go informacje. Może ona również szyfrować rozmowy w celu uniemożliwienia podsłuchu, na który narażeni są użytkownicy zwykłych telefonów komórkowych.

ną płytkę, a kamera odczytuje odcisk palca; następnie komputer porównuje obraz wideo z wzorem zapisanym na inteligentnej karcie. Dzięki takiemu rozwiązaniu nie ma potrzeby łączyć się z centralną bazą danych w celu potwierdzenia tożsamości.

Techniki porównywania nie są jeszcze w pełni niezawodne – inteligentne karty działają dobrze, ale algorytmy do pobierania i porównywania wzorców biometrycznych są wciąż niedoskonałe. Poza tym projektanci muszą zdecydować, czy są bardziej zainteresowani wychwytywaniem oszustów, czy zapewnieniem prawowitym właścicielom kart, by byli zawsze rozpoznani. Karta, która naraża posiadacza na kłopoty z nieprawidłową identyfikacją nawet raz w roku, raczej nie zyska powszechnej akceptacji.

Wszystko to oznacza, że inteligentne karty osiągnęły pierwszy poziom dojrzałości technologicznej: ich pojemność nie jest już czynnikiem ograniczającym. Natomiast przyszłość zależy od oprogramowania, ekonomii, odpowiedzialności finansowej i poufności, akceptacji klientów oraz wielu innych kwestii natury politycznej i osobistej.

Tłumaczył
Krzysztof Przyłucki

* Przykładowo, po włożeniu karty do telefonu GSM jest on rozpoznawalny przez system jako aparat o numerze zapisanym na karcie, a rozmowy z niego obciążają właściciela karty. Telefon bez karty jest bezużyteczny – przyp. tłum.

Informacje o autorce

CAROL H. FANCHER przez ostatnie 4 lata pracowała w firmie Motorola nad zdefiniowaniem i rozwojem amerykańskiego rynku inteligentnych kart. Wcześniej piastowała stanowiska inżyniera w firmach Tracor i Ford Microelectronics oraz w Instytucie Układów Scalonych im. Fraunhofera w Erlangen w Niemczech. W roku 1979 Fancher ukończyła inżynierię układów elektrycznych w University of Texas w Austin.

Literatura uzupełniająca

GET SET! SMARTCARDS ARE COMING TO AMERICA. Patrick Gauthier, *Portable Design*, vol. 1, nr 6, ss. 31-34, V/1996.
A CHIP OFF THE OLD SECURITY BLOCK. Andrea McKenna Findlay, *Card Technology* (Faulkner & Gray), vol. 1, nr 2, ss. 52-60, V-VI/1996.
CRYPTOGRAPHIC SMART CARDS. David Naccache i David M'Raihi, *IEEE Micro*, vol. 16, nr 3, ss. 14-24, VI/1996.
PUBLIC-KEY SECURITY SYSTEMS. Mahdi Abdelguerfi, Burton S. Kaliski, Jr., i Wayne Patterson, *IEEE Micro*, vol. 16, nr 3, ss. 10-13, VI/1996.