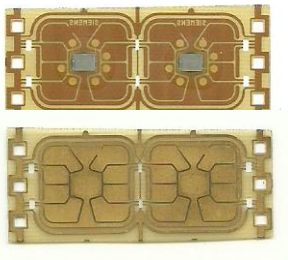
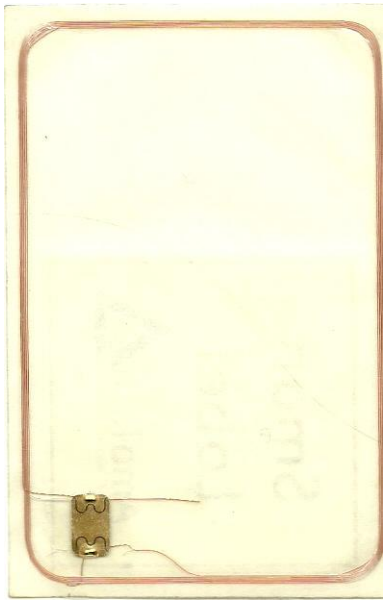
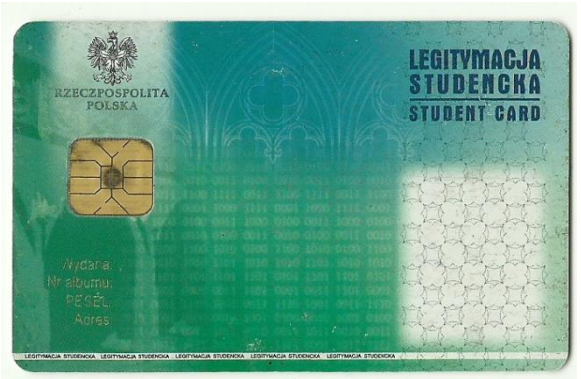


ELEKTRONICZNE KARTY IDENTYFIKACYJNE





Kontakt

mgr inż. Włodzimierz Chocianowicz

Zachodniopomorski Uniwersytet Technologiczny
Wydział Informatyki
Katedra Inżynierii Oprogramowania
Zakład Ochrony Informacji
ul. Żołnierska 52, Szczecin
pok.105 (WI2)

PRÓBA ZDEFINIOWANIA OBIEKTU ROZWAŻAŃ…

Elektroniczna karta identyfikacyjna **(Integrated Circuit(s) Card – ICC) to plastikowa karta o znormalizowanych wymiarach, zawierająca jeden (lub więcej) elektronicznych układów scalonych.**

W sensie funkcjonalnym jest to *nieulotna pamięć* uzupełniona o towarzyszące podukłady umożliwiające komunikację ze światem zewnętrznym (*interfejs wejścia/wyjścia*) oraz mniej lub bardziej złożone struktury sprzętowo-programowe służące do *kontroli dostępu* do tej pamięci oraz *zarządzania jej zasobami*.

KRÓTKI RYS HISTORYCZNY

Za początek dynamicznego rozprzestrzeniania się plastikowych kart identyfikacyjnych przyjmuje się wczesne lata pięćdziesiąte ubiegłego stulecia, kiedy to taką formę trwałego identyfikatora upoważniającego do korzystania z usług związanych z płatnościami zainicjowała korporacja *Diners Club*. Wkrótce podążyły w jej ślady *Visa* i *Mastercard*, zaś dążenie do zautomatyzowania czynności identyfikacji posiadacza karty doprowadziło do „osadzenia" na powierzchni karty paska magnetycznego. Niemniej jednak ostatecznym krokiem w procesie identyfikacji było złożenie podpisu na rachunku przez posługującego się kartą magnetyczną klienta.

DYGRESJA NA TEMAT JEDNOCZESNEGO DOJRZEWANIA ELEKTRONICZNYCH KART IDENTYFIKACYJNYCH I PODPISU CYFROWEGO/ELEKTRONICZNEGO

Digital Signature

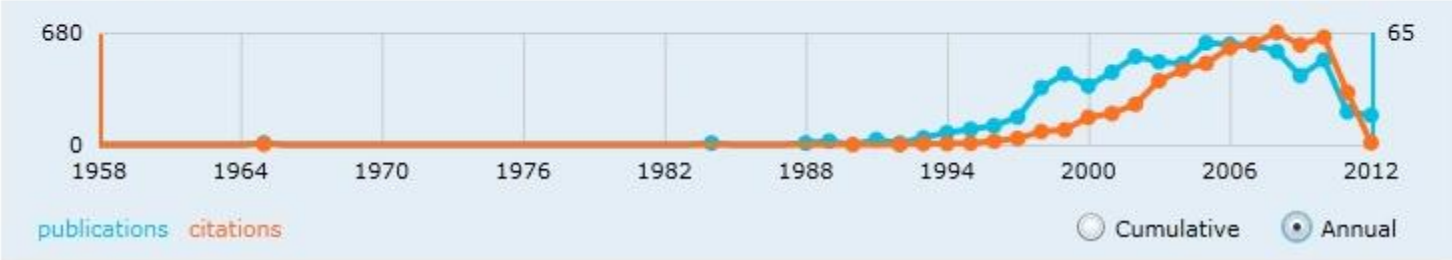
Publications: 3,553 | Citation Count: 40,398

Stemming Variations: Digital Signatures, digitized signature, Digitalized signatures, digitally signatures

smartcard

Publications: 816 | Citation Count: 7,012

Stemming Variations: smartcards



(źródło: Microsoft Academic Search Beta http://65.54.113.26)

NARODZINY, DZIECIŃSTWO I MŁODOŚĆ KARTY ELEKTRONICZNEJ

1968 – Niemcy - Zgłoszenie patentowe dotyczące „wbudowania” w plastikową kartę identyfikacyjną układu scalonego zwiększającego bezpieczeństwo danych identyfikacyjnych. Uznaje się tą datę za datę narodzin *elektronicznych kart identyfikacyjnych* (popularnie zwanych *„smart cards”/”chip cards”*).

Juergen Dethloff
1924 (Stettin) – 2002

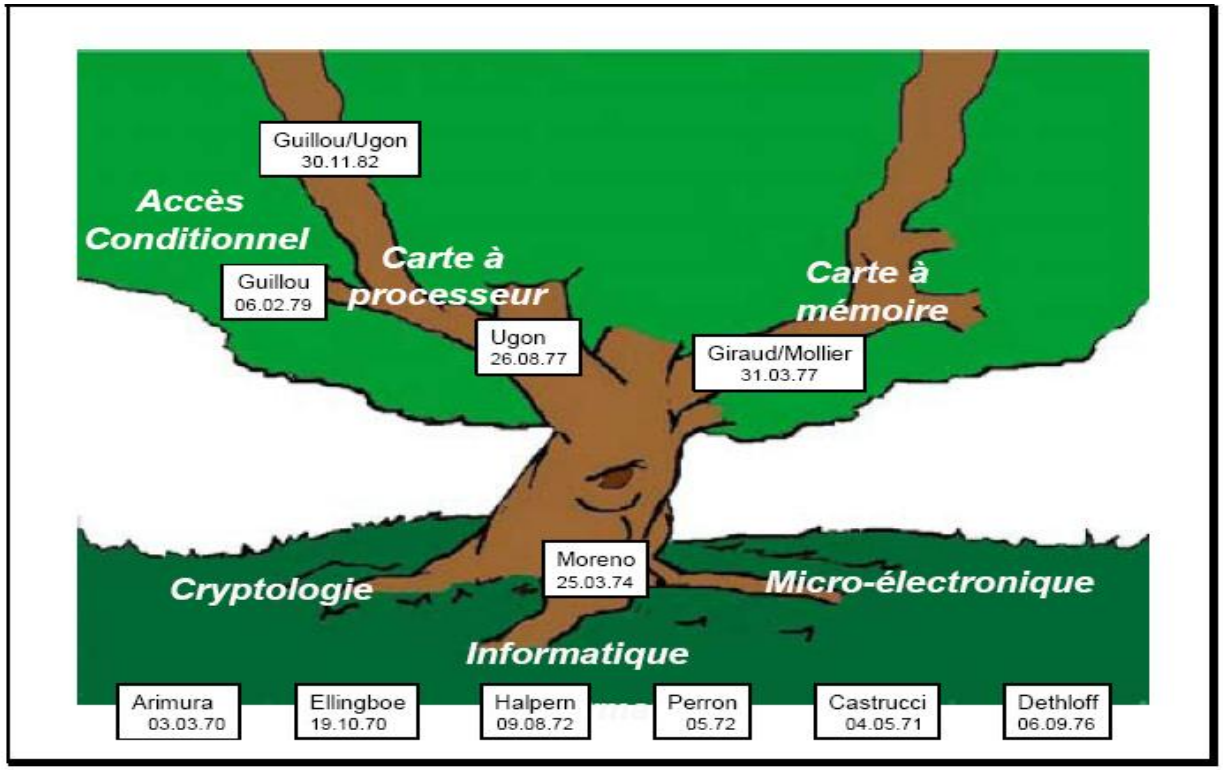
Helmut Groettrup
1916-1981

1970 - Podobny patent w Japonii - Kunitaka Arimura.

1974 – Francja – Patent Rolanda Moreno - Koncepcja *umieszczenia w układzie scalonym* nie tylko *pamięci nieulotnej*, ale także *podsystemu zarządzającego dostępem do tej pamięci*.

1976 – Zgłoszenie patentowe Juergena Dethloffa - Karta elektroniczna z procesorem i pamięcią nieulotną (Patent USP 4105156 w 1978).

1977 – Francja – Michel Ugon z Honeywell Bull „wynalazł” pierwszą kartę procesorową.



(źródło: Louis C. Guillou, Introduction of Cryptology in the Public Domain and Smart Card Saga, 2007)

1978 – Bull patentuje SPOM (self-programmable one-chip microcomputer) , określając min. architekturę niezbędną do programowania układu scalonego.

1981 – Motorola wykorzystuje patent SPOM w układzie scalonym CP8.

1983 - We Francji uruchomiono pilotażową aplikację z kartami elektronicznymi służącymi do realizacji płatności za rozmowy telefoniczne w telekomunikacji publicznej (technologia EPROM). W tym samym roku rozpoczęto podobne eksperymenty w Niemczech (technologia EEPROM).

1985 – Prezentacja pierwszej karty elektronicznej z procesorem.

1986 – Prace studialne w Japonii dotyczące „supersmart cards" z klawiaturą i wyświetlaczem.

1987 – 6 milionów procesorowych kart płatniczych i 25 milionów kart telefonicznych we Francji.

1991 – Giesecke & Devrient produkuje pierwsze karty SIM.

1994 - Europay, Mastercard i Visa publikują pierwszy „draft" specyfikacji standardu EMV dotyczącego kart płatniczych z układem scalonym.

1996 – 20 millionów telefonów komórkowych z kartami SIM.

1996 – Pierwsza wersja specyfikacji PC/SC (rozwiązania „kartowe" jako CSP).

1971 – Pierwsze posiedzenie ISO/TC 95/SC 17 „Office Machines. Credit Cards”.

1987 – Opublikowana pierwsza norma dotycząca kart elektronicznych ISO 7816-1 „Identification cards – Integrated circuit(s) cards with contacts – Part 1: Physical characteristics”.

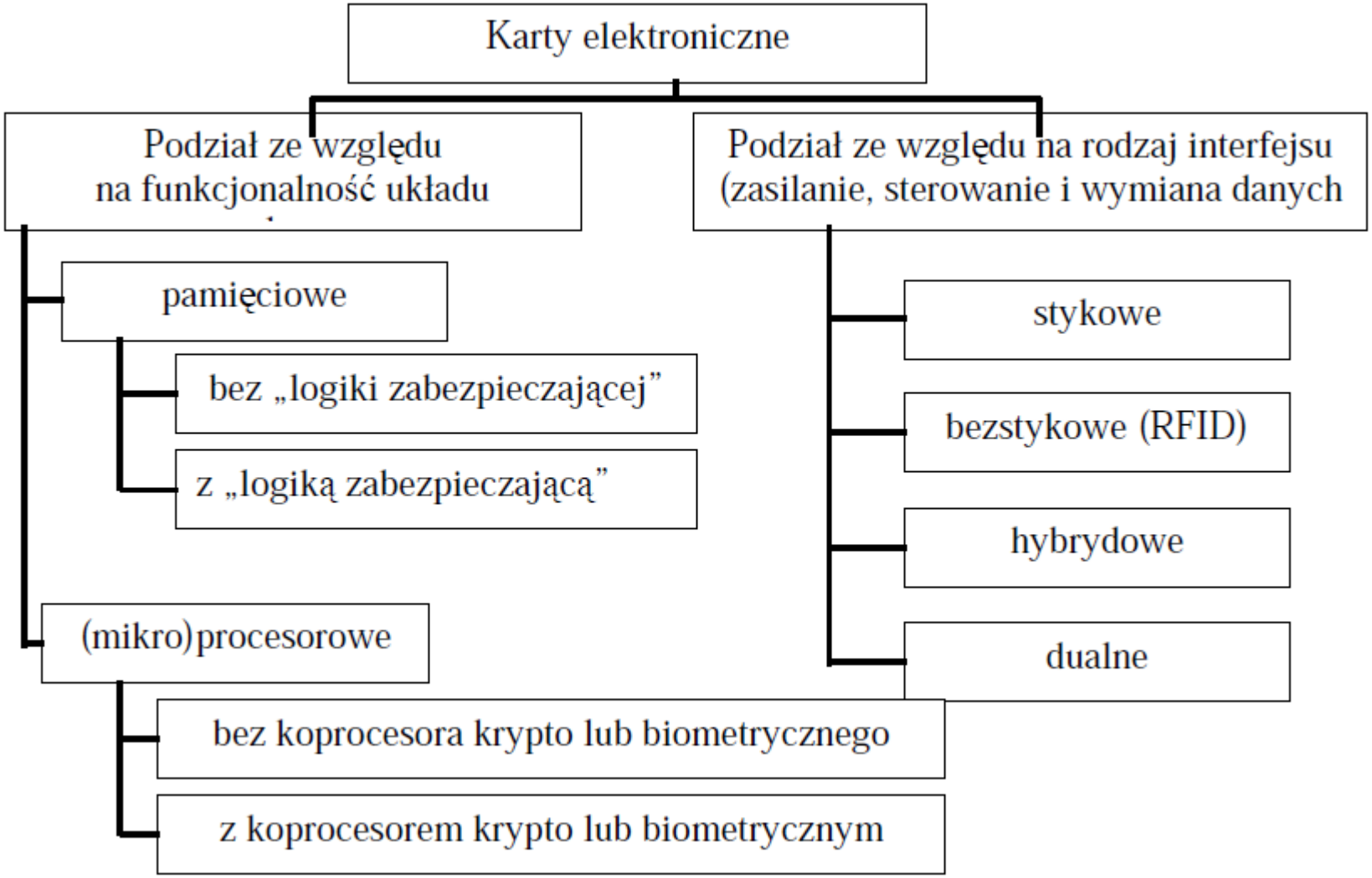
1988 – Podkomitet po różnych fazach reorganizacyjnych staje się częścią ISO/IEC JTC1 („Information technology”) jako SC 17 „Identification cards and related devices”.

1999 – Podkomitet ISO/IEC JTC1 SC17 zmienia nazwę na „Information technology. Identification cards and personal identification”.

1989 – Powołano CEN TC 224 „ Machine readable cards, related device interfaces and operations” w celu tworzenia norm dotyczących technologii i ogólnych własności kart, interfejsu użytkownika, „elektronicznej portmonetki”, kart elektronicznych i terminali stosowanych w telekomunikacji i transporcie lądowym.

Obecna nazwa komitetu: „Personal identification and related personal devices with secure element, systems, operations and privacy in a multi sectorial environment”

KLASYFIKACJA KART ELEKTRONICZNYCH



Karty stykowe

Interfejs galwaniczny

Karty bezstykowe

Wymiana danych oraz dostarczenie energii zasilającej za pośrednictwem odpowiedniej modulacji natężenia pola magnetycznego lub elektrostatycznego

Karty dualne („combi-cards") i hybrydowe

Połączenie w jednej karcie dwóch technologii; oba układy niezależne („*coexistent technologies*") lub możliwość współpracy z tą samą pamięcią nieulotną obu układów interfejsu (reguła: odrębne „profile" praw dostępu)

Karty pamięciowe

Bezpośredni dostęp do pamięci w trybie zapisu lub odczytu; dostęp przez wskazanie bezwzględnego adresu w obszarze pamięci.

Karty procesorowe

Pamięć nieulotna (EEPROM,Flash) jest zorganizowana w formie drzewiastej struktury katalogów i plików (dostęp przez wybór konkretnego pliku i wskazanie „offsetu" bajtu(-ów), numeru(-ów) rekordu(-ów) lub identyfikatora(-ów) obiektu(-ów)).

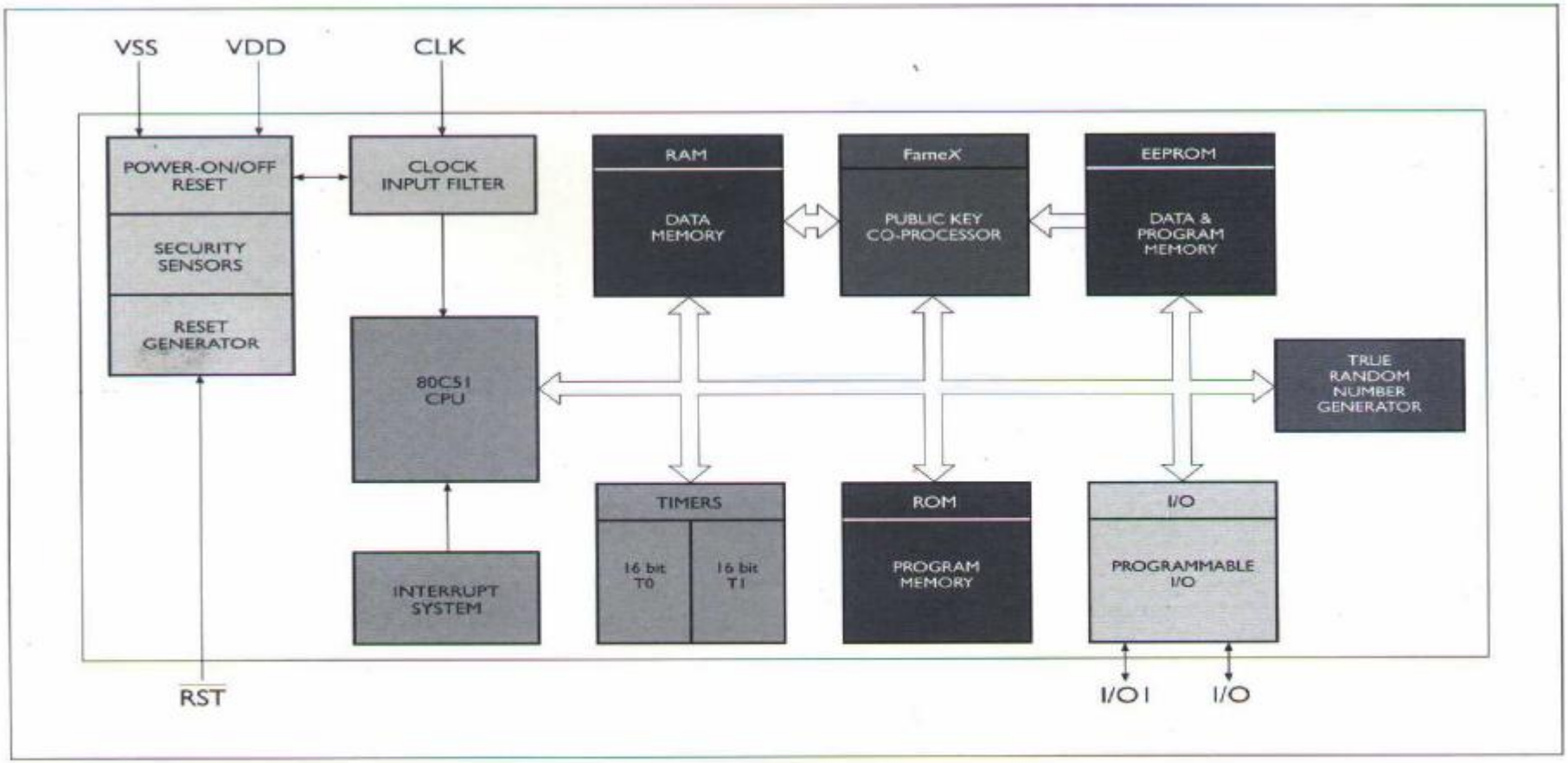
albo

niezależnych równoległych plików aplikacyjnych (np. cardlety JavaCard).

Klasyfikacja kart elektronicznych ze względu sposób fizycznej realizacji komunikacji ze światem zewnętrznym oraz sposób zasilania

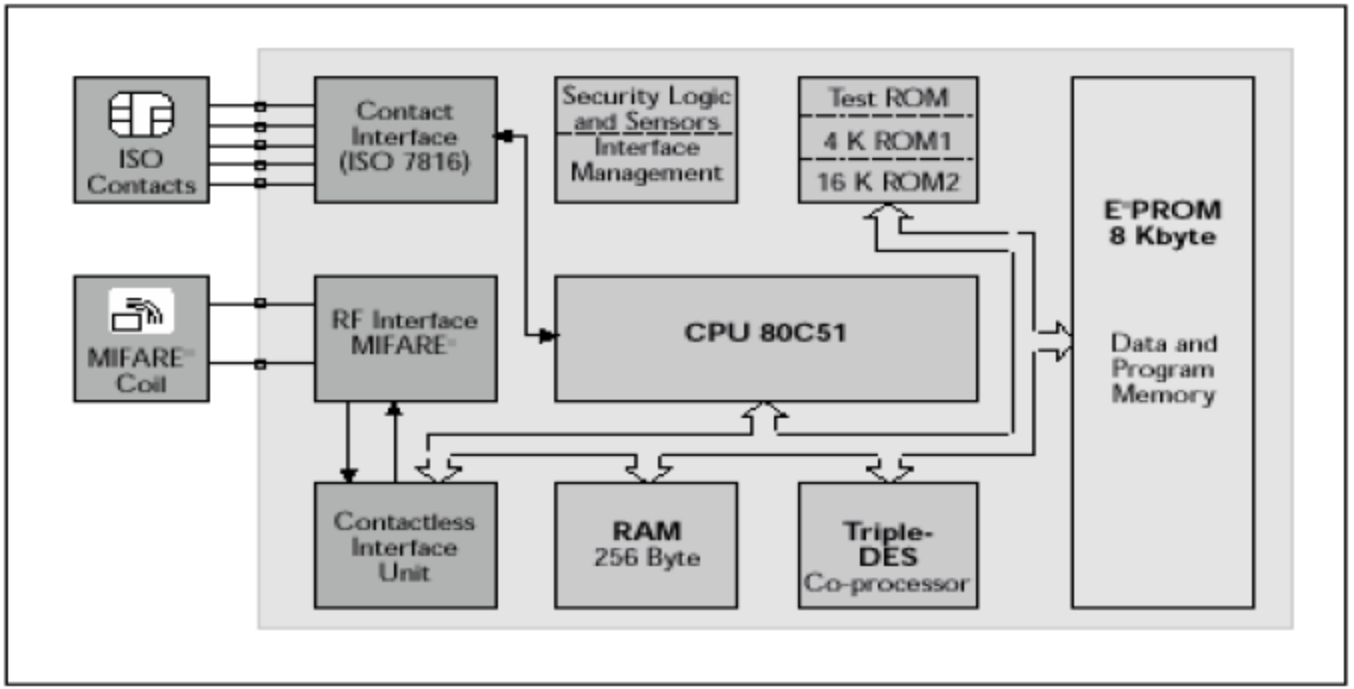
rodzaj kart		częstotliwość sygnału taktującego	rodzaj interfejsu	prędkość komunikacji	odległość od urządzenia interfejsowego (czytnika, IFD)
stykowe (contact)		3.57 MHz	galwaniczny	9.6 kb/s (~kilka Mb/s dla USB)	0
bezstykowe (contactless)	"klasyczne" (closed-coupled - CICC)	4.91 MHz	pojemnościowy i/lub indukcyjny	9.6 kb/s	~2 mm
	zbliżeniowe (proximity - PICC)	13.56 MHz	indukcyjne	106 kb/s	~10 cm
	dystansowe (vicinity – VICC)	13.56 MHz	indukcyjne	~10 kb/s	~70 cm
	mikrofalowe (microwave)	2.45 GHz (5.80 GHz ?)	fale radiowe	~Mb/s	kilka m

← NFC – Near Field Communication



PHILIPS

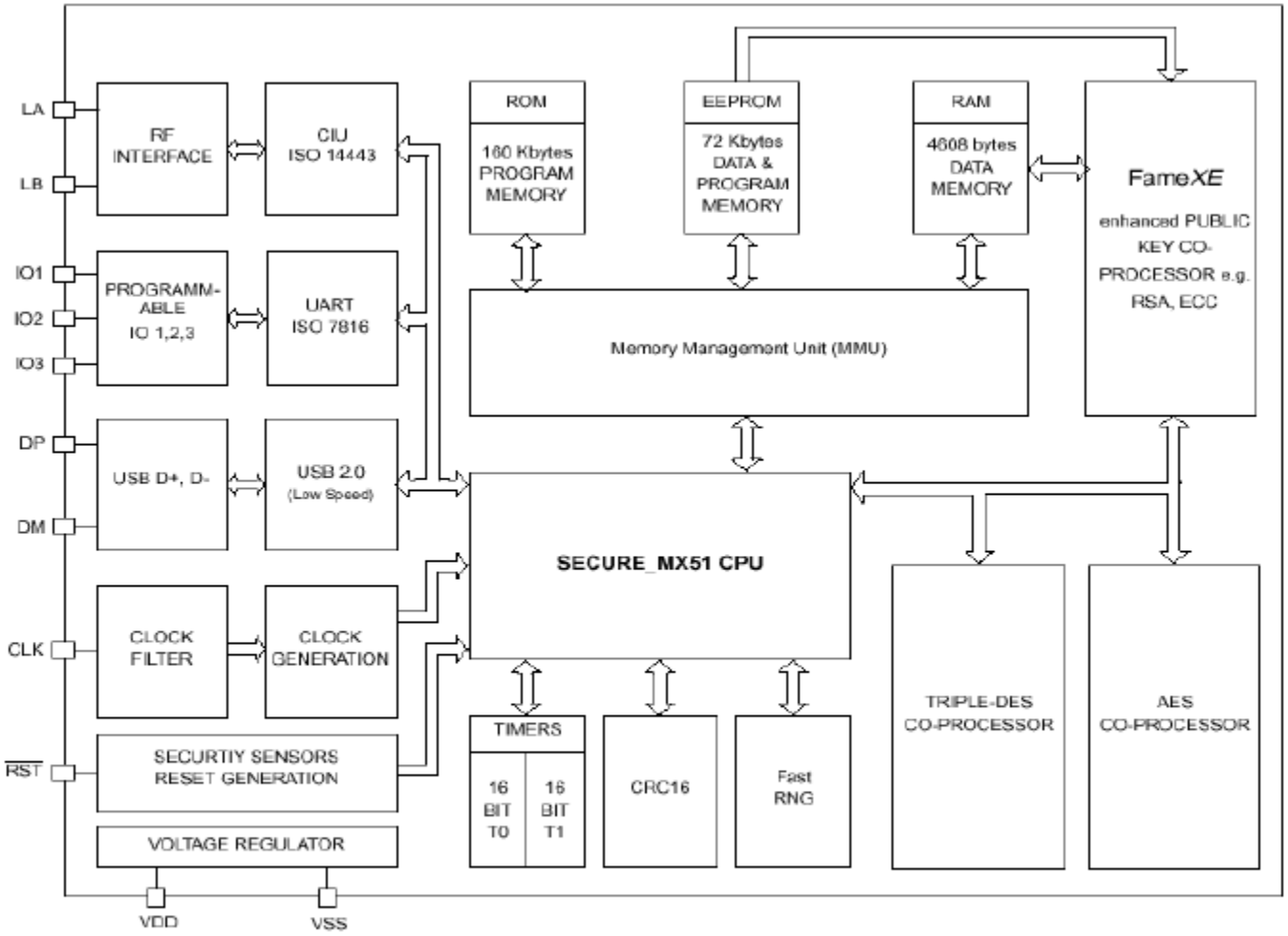
Przykład architektury sprzętowej stykowej karty procesorowej (P83W85xx - PHILIPS)



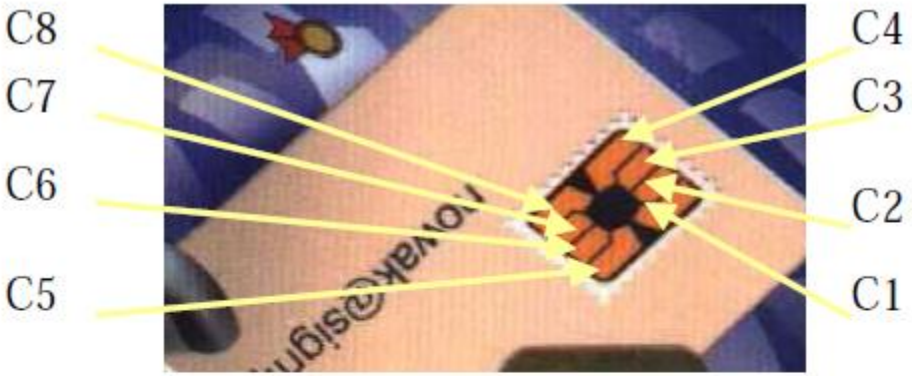
Specifications subject to change without notice

PHILIPS

Przykład architektury sprzętowej dualnej karty procesorowej (MIFARE PRO - PHILIPS)



Przykład architektury sprzętowej karty procesorowej z potrójnym interfejsem (P5CT072 - PHILIPS)



Contact No.	Assignment	Contact No.	Assignment
C1	VCC (Supply voltage)	C5	GND (Ground)
C2	RST (Reset signal)	C6	VPP Variable supply voltage (e.g. programming voltage)
C3	CLK (Clock signal)	C7	I/O (Data input/output)
C4	AUX1	C8	AUX2

NOTE Insert below table 1:

In addition to the contacts assigned in this part, the contact AUX1 is assigned to function code (FCB) for type 2 synchronous cards (ISO/IEC 7816-10).

If an interface device provides a USB interface, VBUS shall be connected to VCC, D+ to AUX1 and D- to AUX2.

Przyporządkowanie styków karty elektronicznej

ZASTOSOWANIA KART ELEKTRONICZNYCH

- Karty SIM (GSM, UTMS) i telefoniczne
  (jednorazowe i wielokrotnego użytku dla telefonii publicznej)
- Kontrola dostępu fizycznego i logicznego
- Karty płatnicze (w tym elektroniczne portmonetki)
- Karty „subskrybenta" usług ubezpieczeniowych
- Karty „zdrowia" (pacjentów i personelu medycznego)
- „Tokeny" uwierzytelniające
- Podpis elektroniczny (biernie i czynnie) i szyfrowanie danych
- Obsługa głosowań
- Dokumenty (prawo jazdy, paszport, dowód osobisty, legitymacja studencka, itp.)
- Karty „lojalnościowe"
- Transport publiczny i parkingi
- Karty miejskie i regionalne
- e-commerce
- Uwierzytelnianie w „bezpiecznym internecie"

- Identyfikacja bagażu, zwierząt, towarów w handlu, zasobów bibliotecznych (RFID)

NORMALIZACJA KART ELEKTRONICZNYCH

ISO (International Organization for Standardization)
+ IEC (International Electrotechnical Commission)

ISO		IEC
TC 68 Banking	ISO/IEC JTC 1 Information technology	
SC 6 Transaction cards	SC 17 Cards and Personal Identification	
WG 5 messages and data contents	WG 1 physical characteristics and test methods	WG 3 machine readable travel documents
WG 7 security architecture	WG 4 ICC with contacts	WG 5 Register Management Group
	WG 7 financial transaction cards	WG 8 contactless ICC
ICAO	WG 9 optical memory cards	WG 10 motor vehicle driver licences and related documents
	WG 11 biometrics	OWG technology co-existence on identification cards

CEN (European Committee for Standardization)

TC 224 Personal identification and related personal devices with secure element, systems, operations and privacy in a multi sectorial environment		
WG 6 Man-machine interface	WG 11 Surface transport applications	WG 15 European Citizen Card (ECC)
WG 9 - Telecommunication applications	WG 19 Breeder documents	WG 16 Application interface for smart cards used as Secure Signature Creation Devices
	WG 18 Biometrics	WG 17 Protection Profiles in the context of electronic signature

“Konkurencyjne” dla ISO/IEC JTC 1 SC 17 WG 8 zespoły w ISO/IEC i ISO

ISO/IEC JTC 1 SC 31 WG 4 – Automatic Data Capture RFID

ISO TC 204 – Inteligent Transport Systems

WG 4 – Automatic Vehicle and Equipment ID

WG 15 – Dedicated Short Range Communications for TICS applications

ISO TC 104 SC 4 WG 2 – Automatic ID for Freight Containers (Microwave)

ISO TC 23 SC 19 WG 3 – RFID of Animals, Agricultural Equipment

Aktywność normalizacyjna International Civil Aviation Organization (ICAO)

MRTD (Machine Readable Travel Documents) - paszporty, wizy, etc.:

ICAO NTWG, Development of a Logical Data Structure – LDS for optional capacity expansion technologies, Technical Report, Revision 1.7, 18 May 2004

ICAO NTWG, PKI for Machine Readable Travel Documents Offering ICC Read-Only Access, Technical Report, Version 1.1, 1 October 2004

Biometric Deployment of EU-Passports, EU-Passport Specification

Biometric Deployment of EU-Visa and EU Residence Permits, EU-Visa Specification

Advanced Security Mechanisms for MRTD, Technical Report

Najważniejsze Normy Międzynarodowe i dokumenty pokrewne

ISO/IEC 7810 Identification cards – Physical characteristics

ISO/IEC 7816-1 Cards with contacts – Physical characteristics

ISO/IEC 7816-2 Cards with contacts – Dimensions and location of contacts

ISO/IEC 7816-3 Cards with contacts – Electrical interface and transmission protocols

ISO/IEC 7816-4 Organization, security and commands for interchange

ISO/IEC 7816-6 Interindustry data elements for interchange

ISO/IEC 7816-7 Interindustry commands for Structured Card Query Language (SCQL)

Najważniejsze Normy Międzynarodowe i dokumenty pokrewne (cd.)

ISO/IEC 7816-8 Commands for security operations
ISO/IEC 7816-9 Commands for card management
ISO/IEC 7816-11 Personal verification through biometric methods
ISO/IEC 7816-12 USB electrical interface and operating procedures
ISO/IEC 7816-13 Commands for application management in multiapplication environment
ISO/IEC 7816-15 Cryptographic information application

ISO/IEC 10536-1./.3 Contactless ICC (close coupled cards)

ISO/IEC 14443-1 Contactless ICC – Proximity ICC – Physical characteristics
ISO/IEC 14443-2 Contactless ICC – Proximity ICC – Radio frequency interface
ISO/IEC 14443-3 Contactless ICC – Proximity ICC – Initialization and anticollision
ISO/IEC 14443-4 Contactless ICC – Proximity ICC – Transmission protocol

ISO/IEC 15693-1… Contactless ICC – Vicinity cards

ISO/IEC 20060 Open terminal architecture (OTA) specification – Virtual machine specification

ISO/IEC 24727-1… 6 Programming Interfaces for ICC

Najważniejsze Normy Międzynarodowe i dokumenty pokrewne (cd.)

EN 419212 -1…5 – Application Interface for Secure Elements for Electronic Identification, Authentication and Trusted Services

(poprzednio: Application interface for smart cards used as SSCD)

EN 419211 -1..6 – Protection Profiles for Secure Signature Creation Device

CEN/TS 15480-1..5- European Citizen Card (ECC)

GSM 11.11 Specification of Subscriber Identity Module – Mobile Equipment (SIM-ME) Interface

EMV v.4.3 (listopad 2011) Integrated Circuit Card Specification for Payment Systems

PKCS #11 Cryptographic Token Interface Standard

PKCS #15 Cryptographic Token Information Format Standard

PC/SC v.2.01.14 (czerwiec 2013)

Java Card v.3.0.5 (czerwiec 2015)

- **Application Programming Interface**
- **Language Subset and Virtual Machine Specification**
- **Programming Concepts**

GlobalPlatform Card v.2.3 (grudzień 2015) - Card specification from GlobalPlatform („dopinana” specyfikacja Trusted Execution Environment (TEE))

ETSI TS 102 226 Smart cards; Remote APDU structure for UICC based applications

STYKOWE KARTY PROCESOROWE

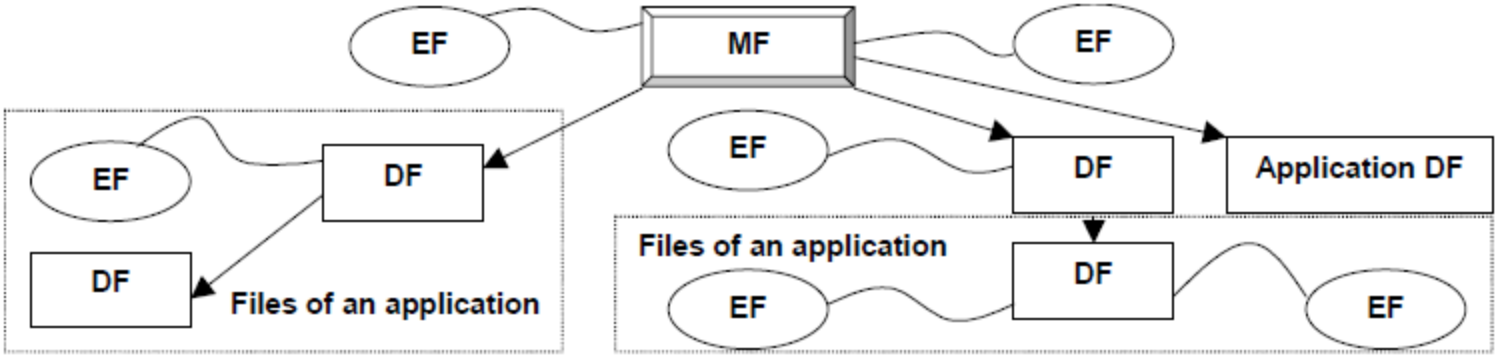
ZADANIA SYSTEMU OPERACYJNEGO KARTY

Procesy realizowane podczas sesji współpracy „świata zewnętrznego” z kartą:

- **Dwukierunkowe przesyłanie danych (polecenia i odpowiedzi: „*commands and responses*”)**
- **Przechowywanie danych**
- **Przetwarzanie danych nie wymagających ochrony**
- **Szyfrowanie i deszyfrowanie dużych strumieni danych**
- **Obliczanie kryptograficznych sum kontrolnych i funkcji skrótu**
- **Obliczanie podpisów cyfrowych**
- **Obsługa protokołów uwierzytelniania wykorzystujących parametry zależne od czasu**

LOGICZNA ORGANIZACJA PAMIĘCI

Zasoby pamięciowe karty procesorowej zorganizowane są w formie hierarchicznej struktury drzewiastej plików…

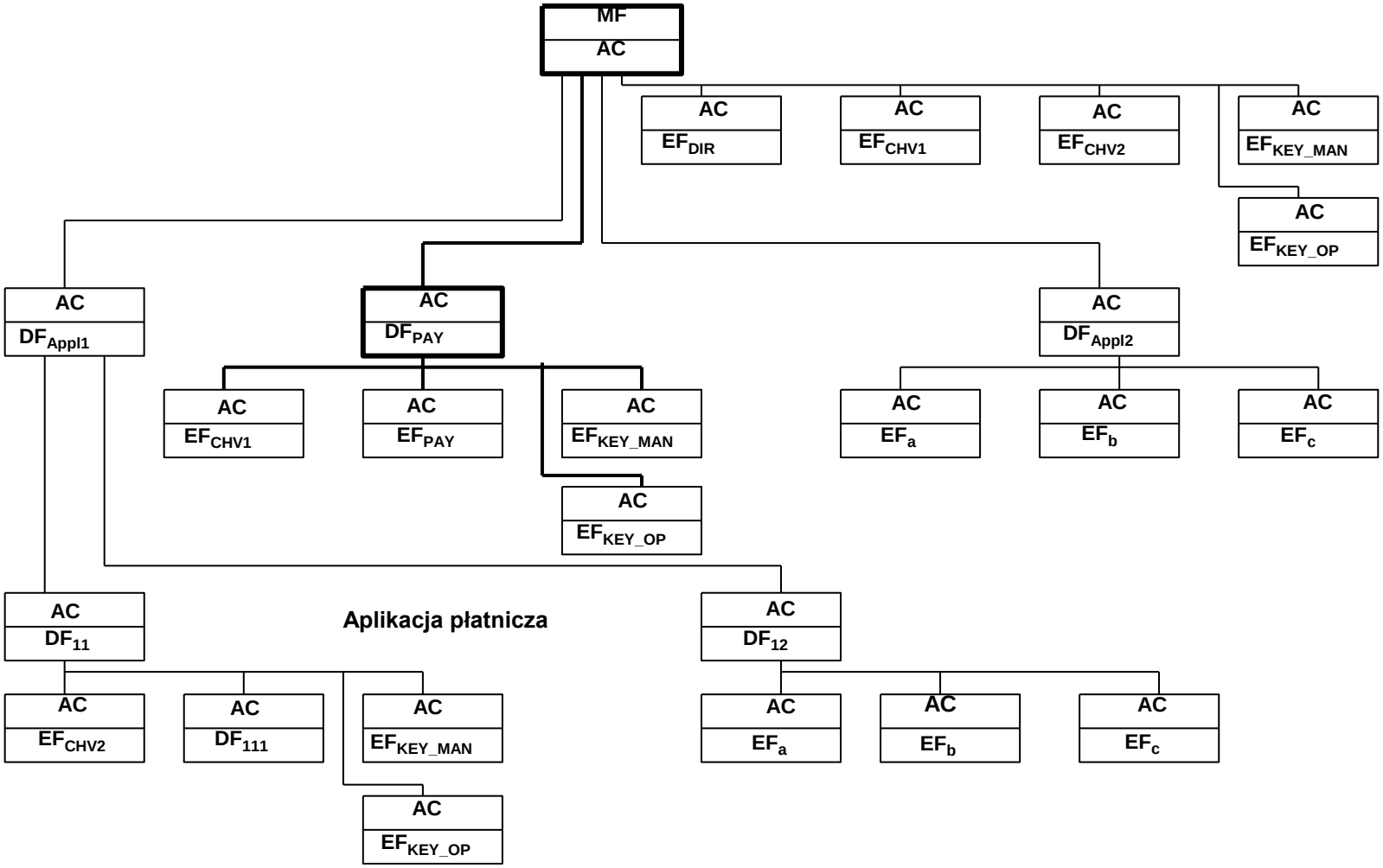


…lub niezależnych równoległych plików aplikacyjnych.

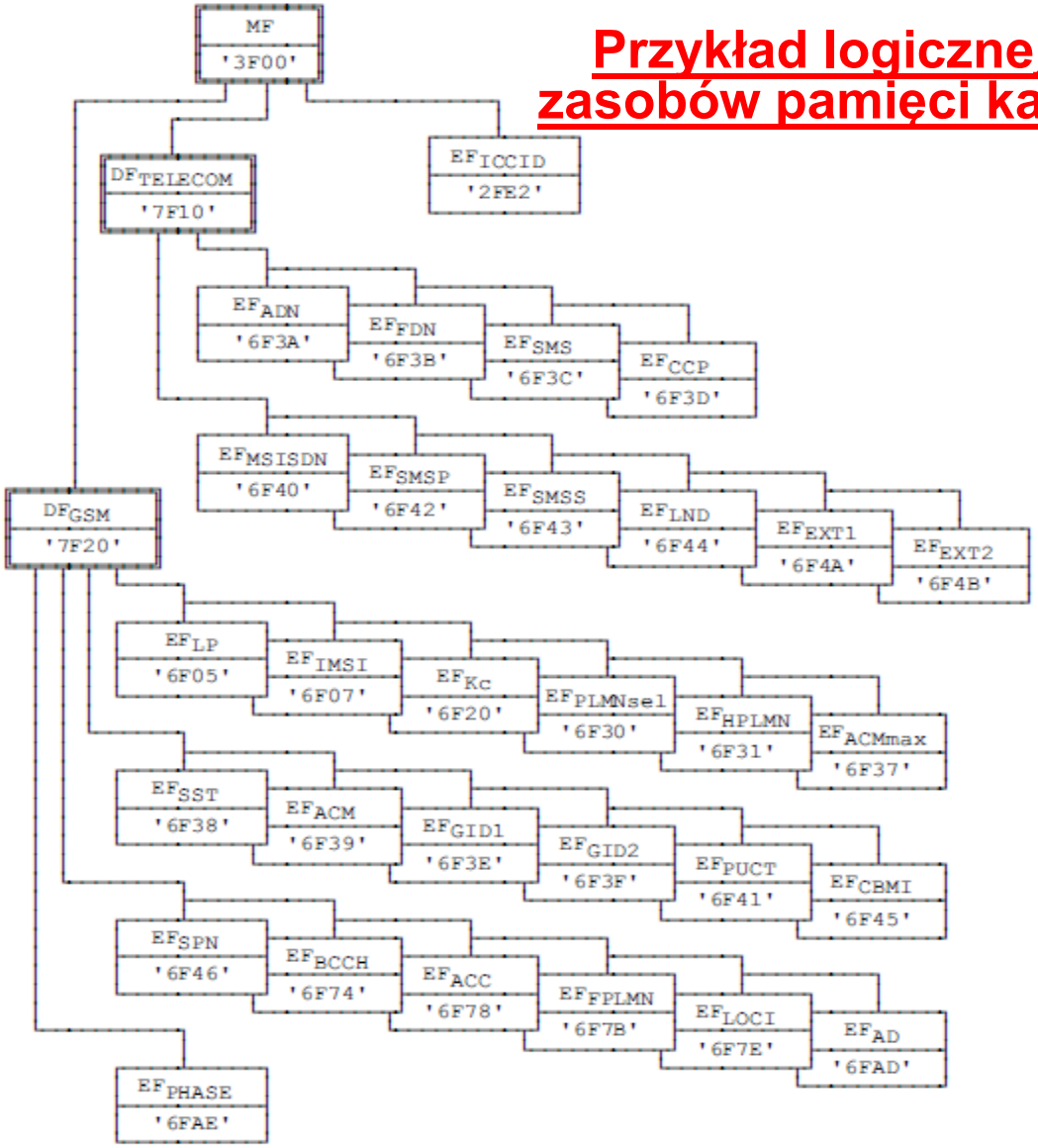
DF może być DF aplikacyjnym z opcjonalną własną wewnętrzną hierarchią innych DF-ów oraz odpowiednią architekturą zabezpieczeń.

(wg. ISO/IEC 7816-4)

Przykład logicznej „drzewiastej” konfiguracji zasobów pamięci karty procesorowej (wg. PN-EN-726-5)



Przykład logicznej „drzewiastej” konfiguracji zasobów pamięci karty SIM (wg. ETSI GSM 11-11)

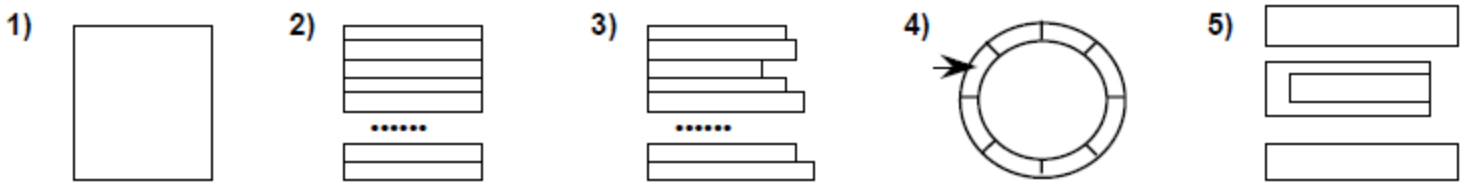


- pliki DF (za wyjątkiem MF) można wskazywać przez nazwę pliku, która może liczyć od 1-go do 16-tu bajtów (pod warunkiem, że konfigurując pamięć zdefiniowano taką nazwę);
- wszystkie pliki można wskazywać wykorzystując unikalny dwubajtowy identyfikator pliku; identyfikator '3F00' jest zastrzeżony dla pliku MF;
- identyfikator '2F00' jest zastrzeżony dla pliku zawierającego informację o DF-ach będących bezpośrednimi potomkami MF (plik EF.DIR, jeśli istnieje);
- identyfikator '2F01' jest zastrzeżony dla pliku zawierającego informacje przekazywane podczas ATR (plik EF.ATR, jeśli istnieje);
- niektóre inne identyfikatory także są zastrzeżone przez normy branżowe, np. GSM 11.11 lub EN 726-3;
- identyfikator 'FFFF' jest zarezerwowany przez ISO/IEC do przyszłego wykorzystania, zaś identyfikator '3FFF' jest zastrzeżony przez ISO/IEC do określania „ścieżek" („*paths*");
- identyfikator '0000' jest przeznaczony do wskazywania bieżącego pliku elementarnego;
- w celu uniknięcia „kolizji" należy przestrzegać zasady, że pliki będące bezpośrednimi potomkami tego samego DF muszą mieć różne identyfikatory;
- plikom EF można także nadać tzw. „krótkie identyfikatory" 5-bitowe, unikalne w obrębie DF, służą one do „niejawnego" wybierania plików, połączonego z operacjami ich odczytu lub modyfikacji; powinny być one unikalne w ramach zbioru bezpośrednich potomków tego samego DF;
- pliki można także wskazać przez tzw. „ścieżkę", będącą konkatenacją kolejnych dwubajtowych identyfikatorów (kolejność ***wyłącznie*** zstępująca).

Pliki elementarne dzielą się na dwie kategorie:

- **pliki wewnętrzne (*internal files*) – przeznaczone do przechowywania danych interpretowanych wyłącznie przez system operacyjny karty (np. dla potrzeb sterowania, kontroli i zarządzania zasobami pamięciowymi);**
- **pliki robocze (*working files*) – przeznaczone do przechowywania danych nie interpretowanych przez system operacyjny karty, a więc użytkowanych wyłącznie przez „świat zewnętrzny”.**

Według normy ISO/IEC 7816-4 dane w plikach elementarnych mogą być zorganizowane jako pojedyncze bajty (lub inne skwantowane porcje danych, np. słowa 16-bitowe) (pliki binarne – *transparent (1)*), rekordy liniowe o stałej długości lub zmiennej długości (*linear with records of fixed or variable size (2, 3)*), rekordy cykliczne o stałej długości (*cyclic with records of fixed size (4)*) lub obiekty o strukturze obiektowej zgodnej z notacją ASN.1 (*TLV (5)*).



Branżowe normy dopuszczają także pliki „wykonywalne” lub traktowane jako „portmonetka”, co ma swoje odzwierciedlenie w ich własnościach strukturalnych.

Z „zupełnie innej bajki” są pliki zajmowane przez tzw. „*cardlety*”, czyli aplety Java Card, które i tak są interpretowane przez interpreter bajt-kodu Javy (jeżeli system operacyjny ma taką opcję).

WYMIANA DANYCH MIĘDZY KARTĄ ELEKTRONICZNĄ I „ŚWIATEM ZEWNĘTRZNYM”

Bezpośrednio po zasileniu stykowej karty procesorowej należy wymusić tzw. „odpowiedź na reset” (*ATR – Answer To Reset*).

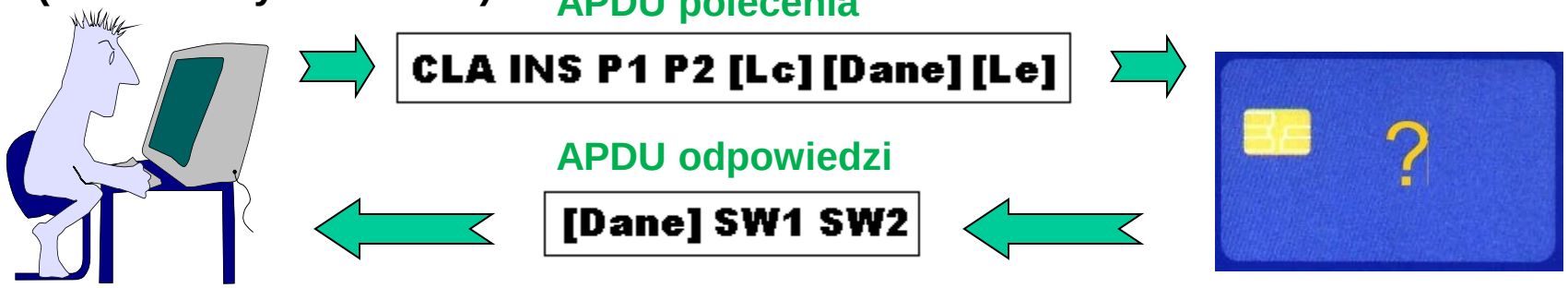
Karta powinna odpowiedzieć sekwencją bajtów określającą obsługiwane protokoły, a także inne parametry związane z komunikacją.

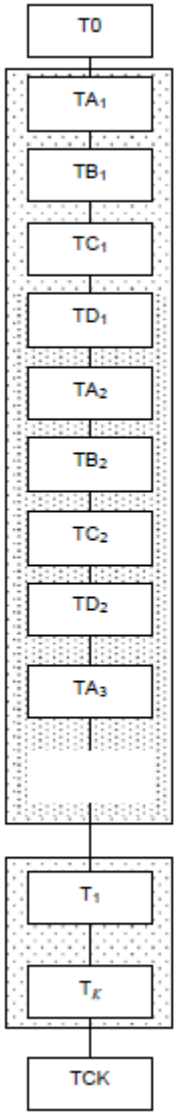
W ATR zawiera się także często informację o systemie operacyjnym (i jego wersji), producencie systemu, przeznaczeniu karty, jej możliwościach, a także stanie zasobów pamięciowych karty (karta niespersonalizowana, zablokowana całkowicie, itp.).

Reset można także wymusić w dowolnej fazie współpracy z kartą, po to by np. zmienić protokół komunikacyjny (mechanizm *Protocol and Parameters Selection - PPS*).

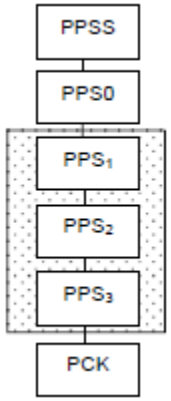
Komunikacja karty procesorowej ze „światem zewnętrznym” odbywa się w trybie dialogu „polecenie- odpowiedź” (command-responce).

Stroną inicjującą dialog (wysyłającą pakiet-ramkę polecenia) jest zawsze „świat zewnętrzny”, reprezentowany przez tzw. czytnik karty elektronicznej (wbudowany w terminal).





Format byte T0 (mandatory)		Encodes Y_1 and K
Interface bytes (optional)		
	TA_1	Global, encodes *Fi* and *Di*
	TB_1	Global, deprecated
	TC_1	Global, encodes *N*
	TD_1	Structural, encodes Y_2 and T
	TA_2	Global, specific mode byte
	TB_2	Global, deprecated
	TC_2	Specific to T=0, see 10.2
	TD_2	Structural, encodes Y_3 and T
	For $i > 2$,	
	TD_{i-1}	Structural, encodes Y_i and T
	TA_i	— Specific to T after T from 0 to 14 in TD_{i-1}
	TB_i	— Global after T=15 in TD_{i-1}
	TC_i	
	TD_i	Structural, encodes Y_{i+1} and T
Historical bytes (optional)		
	T_1	See ISO/IEC 7816-4
	T_2	
	...	
	T_K	
Check byte TCK (conditional)		



Sekwencje ATR i PPS (żądanie i odpowiedź) wg. ISO/IEC 7816-3

APDU – application protocol data unit

nagłówek (*header*)	ciało (*body*)
CLA INS P1 P2	[L_c field] [Data field] [L_e field]

Struktura APDU polecenia

ciało (*body*)	końcówka (*trailer*)
[Data field]	SW1 SW2

Struktura APDU odpowiedzi

W warstwie transportowej sposób przesyłania zależy od rodzaju protokołu.
Ramki APDU są przenoszone za pośrednictwem TPDU (transport protocol data units).

Dla procesorowych kart stykowych najczęściej stosowane są protokoły (określone w ISO/IEC 7816-3):

T = 0 – „starszy”, zorientowany na znaki (bajty), stosowany np. w kartach SIM;

T = 1 – „nowszy”, zorientowany na bloki, z korekcją błędów i „łańcuchowaniem” bloków.

Dla procesorowych kart zbliżeniowych ramki APDU przenoszone są zazwyczaj zgodnie z protokołem T= CL (wg. ISO/IEC 14443-4).

Kryptograficzna ochrona wymiany danych (SM – Secure Messaging)

CLA INS P1 P2 [Lc] [Dane] [Le]

[Dane] SW1 SW2

Niezależne klucze sesyjne do realizacji usługi poufności (K_{ENC}) i integralności (K_{MAC}) negocjowane są np. podczas procesu uwierzytelniania

CLA* INS P1 P2 T1 L1 [Lc] [Dane] T2 L2 [Le]
E_{CBC} (K_{MAC}, CLA* INS P1 P2 T1 L1 [Lc] [Dane] T2 L2)

T1 L1 [Dane] E_{CBC} (K_{MAC}, T1 L1 [Dane] SW1 SW2) SW1 SW2

CLA* INS P1 P2 T1 L1 [Lc*] C1=E_{CBC} (K_{ENC}, Dane)
T2 L2 E_{CBC} (K_{MAC}, CLA* INS P1 P2 T1 L1 [Lc*] C1)

T1 L1 C2=E_{CBC} (K_{ENC}, Dane)
E_{CBC} (K_{MAC}, T1 L1 C2 SW1 SW2) SW1 SW2

PRZYKŁADY POLECEŃ „ROZUMIANYCH” PRZEZ KARTĘ (ISO/IEC 7816 - 4,8,9,13)

Zarządzanie plikami:

CREATE FILE
DELETE FILE
ACTIVATE FILE
DEACTIVATE FILE
TERMINATE EF, DF,
TERMINATE CARD USAGE (MF)
SELECT FILE
APPLICATION MANAGEMENT REQUEST
LOAD APPLICATION
REMOVE APPLICATION

PRZYKŁADY POLECEŃ „ROZUMIANYCH” PRZEZ KARTĘ (ISO/IEC 7816 - 4,8,9,13)

Zarządzanie danymi:

READ BINARY
WRITE BINARY
ERASE BINARY
READ RECORD(S)
WRITE RECORD
UPDATE RECORD
APPEND RECORD
ACTIVATE RECORD
DEACTIVATE RECORD
GET DATA (BER-TLV, SIMPLE-TLV)
PUT DATA (BER-TLV, SIMPLE-TLV)

PRZYKŁADY POLECEŃ „ROZUMIANYCH” PRZEZ KARTĘ (ISO/IEC 7816 - 4,8,9,13)

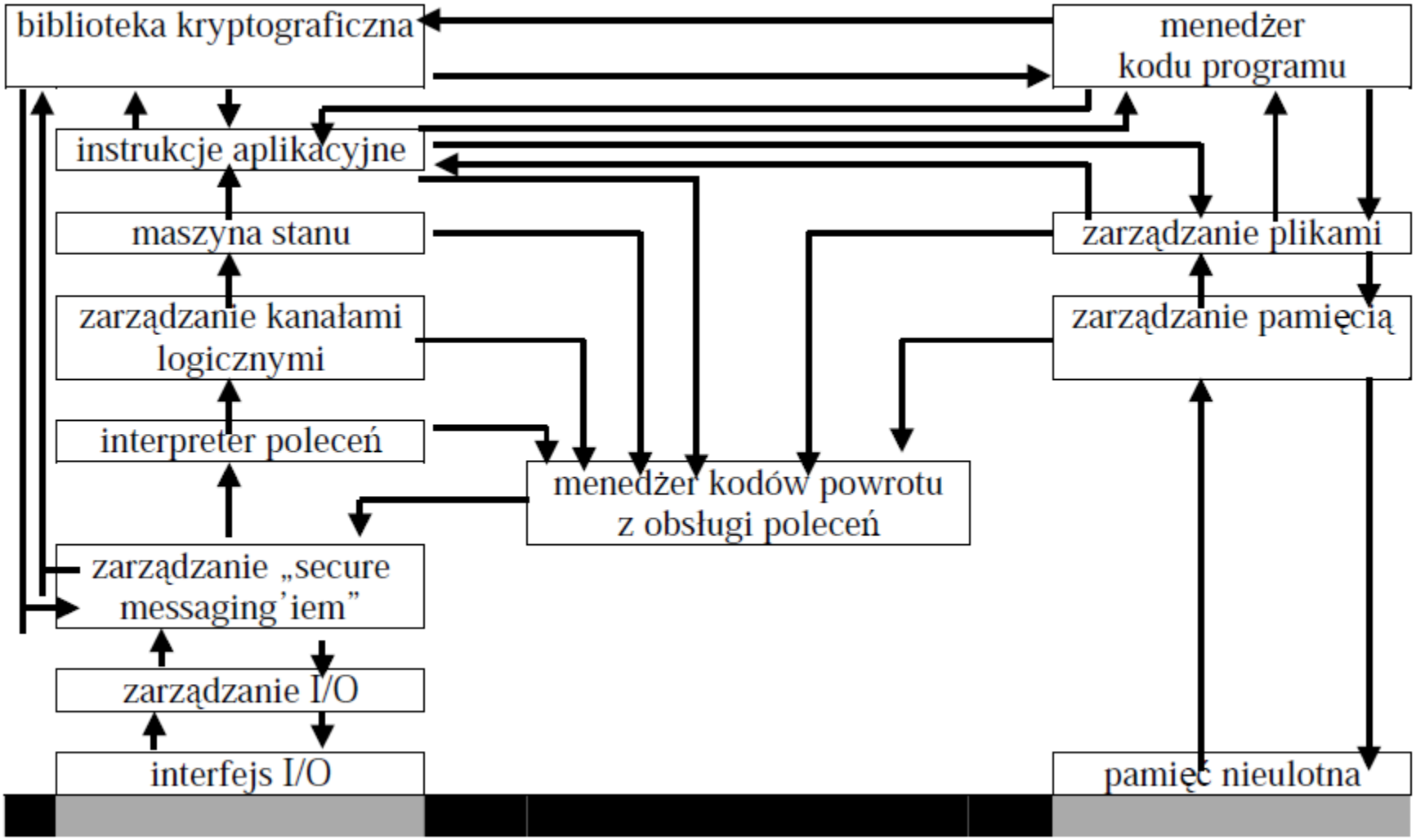
Usługi bezpieczeństwa:

VERIFY
EXTERNAL (/MUTUAL) AUTHENTICATE
INTERNAL AUTHENTICATE
GENERAL AUTHENTICATE
GET CHALLENGE
MANAGE SECURITY ENVIRONMENT
PERFORM SECURITY OPERATION
GENERATE ASYMMETRIC KEY PAIR
RESET RETRY COUNTER

PRZYKŁADY POLECEŃ „ROZUMIANYCH” PRZEZ KARTĘ (ISO/IEC 7816 – 4,8,9,13)

Operacje PSO (PERFORM SECURITY OPERATION):

COMPUTE CRYPTOGRAPHIC CHECKSUM
VERIFY CRYPTOGRAPHIC CHECKSUM
HASH
COMPUTE DIGITAL SIGNATURE
VERIFY DIGITAL SIGNATURE
VERIFY CERTIFICATE
ENCIPHER
DECIPHER



Logiczna sekwencja wydarzeń zachodzących podczas sesji komunikacyjnej z kartą procesorową (wg. W.Rankl, W.Effing, „Smart Card Handbook")

Koniec części 1.