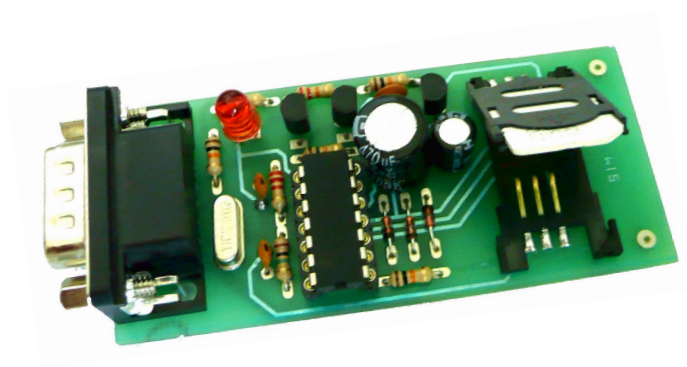




Cuprins

Prezentare Proiect

Fișa de Asamblare

1. Funcționare	2
2. Schema	2
3. PCB	3
4. Lista de componente	3
5. Instalare	4 - 5
6. Tutorial - Smart card GSM	6 - 8

SMART CARD GSM

- Avantaj Pret/Calitate
- Livrare rapida
- Design Industrial
- Proiecte Modificabile
- Adaptabile cu alte module
- Module usor de asamblat
- Idei Interesante

Idei pentru afaceri

Hobby & Proiecte Educationale

www.epsicom.com/kits.php

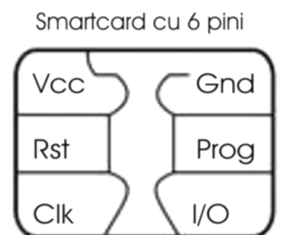
a division of EPSICO Manufacturing

Sisteme de operare recomandate: Windows 98, Windows 2000, Windows XP, Windows Vista (versiunea 32 biti), Windows 7 (versiunea 32 biti), Windows ME.

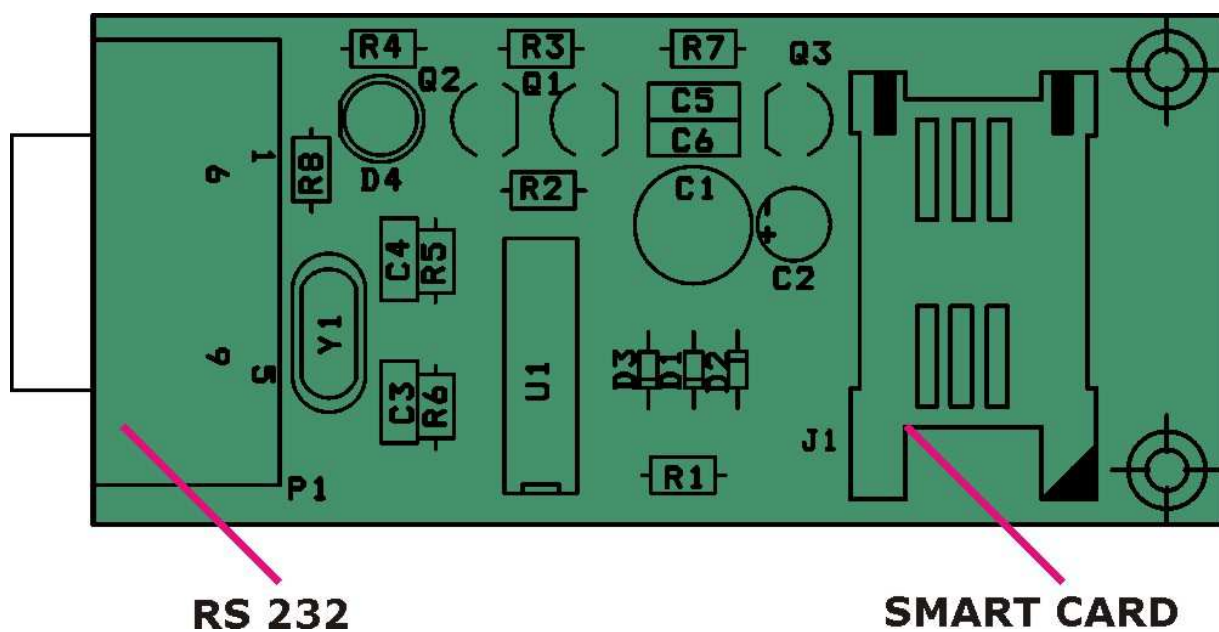
Circuitul nu necesită folosirea unei surse de alimentare externe, aceasta este formată din semnalele de pe pinii DTS și RTS ale portului serial, semnale ce devin active la lansarea programului de interogare prin portul serial RS232 (Serial Port).

pySIMReader script (pentru Linux, Mac și Windows);
SimScan 2.01
WoronScan 1.06
IC-Prog 1.05
Configured files SimEmu 6.01

Pin	Denumire	Descriere
1	Vcc	+5V sau 3.3Vcc
2	Reset	Card Reset (Optional)
3	CLOCK	Card Clock
4	GND	Masa
5	VPP	+21V [Programare]
6	I/O	In/Out [Data]



31 Sararilor Street | 200570 Craiova, Dolj, Romania | 0723.377.426, 0743.377.426



Amplasarea componentelor

Lista de componente

Nr.Crt.	Componenta	Denumire	Valoare	Cant
1	C1	Condensator POL	470μF	1
2	C2	Condensator POL	47μF	1
3	C3,C4	Condensator NP	33pF	2
4	C6,C5	Condensator NP	100nF	2
5	D1,D2,D3	Diodă	1N4148	3
6	D4	Led	LED	1
7	J1	Conector	SMART CARD	1
8	P1	Conector	DB9 tată	1
9	Q1,Q2,Q3	Tranzistor	BC239C	3
10	R1,R2,R7,R8	Rezistență	10KΩ	4
11	R3	Rezistență	22KΩ	1
12	R4	Rezistență	15KΩ	1
13	R5	Rezistență	2,2KΩ	1
14	R6	Rezistență	1MΩ	1
15	U1	C.I.	74HC04	1
16	Y1	Quartz	3.579545MHZ	1

Instalarea

Se lansează programul cu "install.bat". Se va crea directorul "C: Sim_Scan" și se vor instala fișierele corespunzătoare. Pornim programul sim_scan.exe și selectăm portul COM și viteza portului COM. Viteza de transfer trebuie să coincidă cu frecvența cititorului. Apăsați Find Ki, acest proces poate dura până la 2 ore.

Dacă procesul de identificare a trecut cu succes, programul va crea în directorul "c: Sim_Scan" un fișier "imsi_ki.dat", în care vor fi înregistrate datele IMSI și Ki.

Important !!!

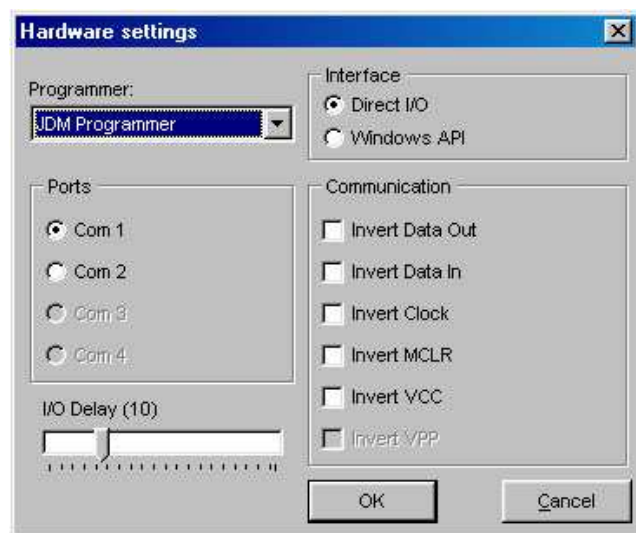
Informațiile de pe card pot fi pierdute utilizând acest program !!!

Clonarea este interzisă !!!

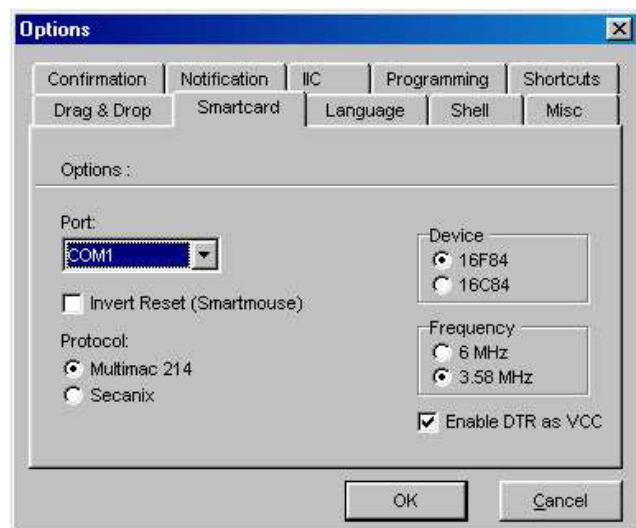
Scanarea cartelelor SIM cu programul Sim Scan se face numai în scopuri educaționale !!!

Responsabilitatea pentru orice probleme, pierderi sau daune aparțin exclusiv utilizatorului !!!

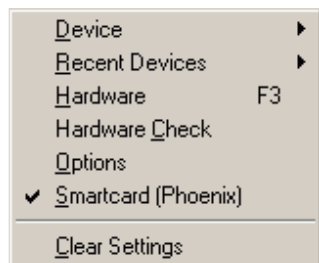
Start icprog.exe și selectați portul COM:



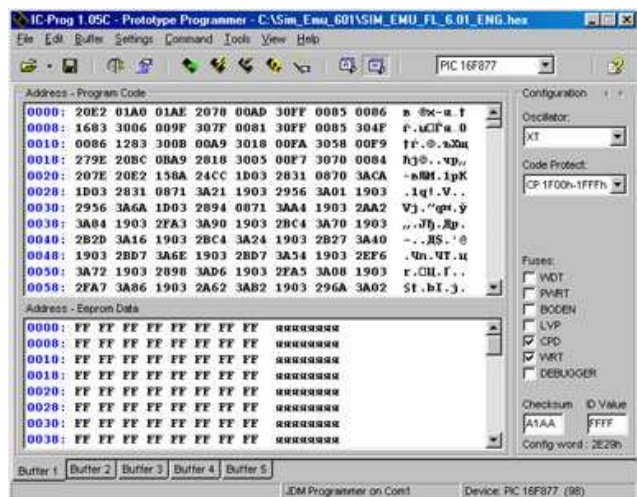
Ok-> Settings-> Options> smartcard, selectați portul COM și frecvența.



Ok -> Settings -> SmartCard (Phoenix):



Alegeți microcontrollerul PIC 16F877 (carduri Silver, Green și Green2) în IC-Prog și deschideți fișierul SIM_EMU_FL_6.01_ENG.hex din folderul SimEmu 6,01:



Dacă doriți să atașați cardului o protecție suplimentară împotriva citirii, selectați CP 1F00h-1FFFh în meniul Cod Protect și bifați CPD în Fuses (recomandat).

Alegeți modul pe Sim Reader/Writer - "Programul Pic".

Ceas Sim: "Program Pic".

Sim Reset: "Program Pic".

Date Sim: "Program Pic".

După setări apăsați butonul Programare și așteptați până ce PIC-procesorul cardului va fi programat.

După ce procesorul PIC este programat se selectează următoarele moduri Sim Reader:

Ceas Sim: 3.579

Sim Reset: "Reset Low" sau "Reset de mare".

Date Sim: "Sim Reader".

Carduri Silver, Green sau Green2.

Selectam în IC-Prog-ul circuitul 24C64 (pentru card de argint), 24C128 (pentru Green Card) sau 24C256 (pentru cardul de Green2):

Deschidem fișierul corespunzător cardului nostru, de exemplu SIM_EMU_EP_6.00_ENG.hex, cu un utilitar EEPROM. După ce apăsați butonul programare vom aștepta până când zona memoriei EEPROM de pe card va fi programată.

Când vom introduce cardul în telefon va apărea un nou meniu "SimEmu". Cu acest meniu putem citi codurile preliminare IMSI și Ki de pe card și multe alte lucruri.

Smart card GSM



GSM - Global System for Mobile communications

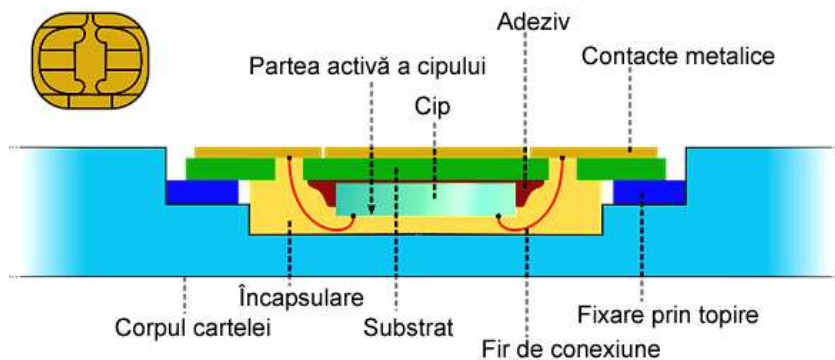
Scurt Remember

Prima cartelă smart-card SIM (**S**ubscriber **I**dentify **M**odule for a mobile phone) a fost realizată în 1991 de firma Giesecke & Devrient din Munchen, care a vândut primele 300 de cartele SIM operatorului finlandez de rețea wireless Radiolinja.

Cartela SIM a fost specificată de către Institutul European de Standarde în Telecomunicații care a și descris realizarea fizică și logica de funcționare a cartelei SIM. Evoluția a fost ultrarapidă și nu se poate uita cum telefoanele cu fise au fost înlocuite, cu o viteză uluitoare, cu cele cu cartelă.

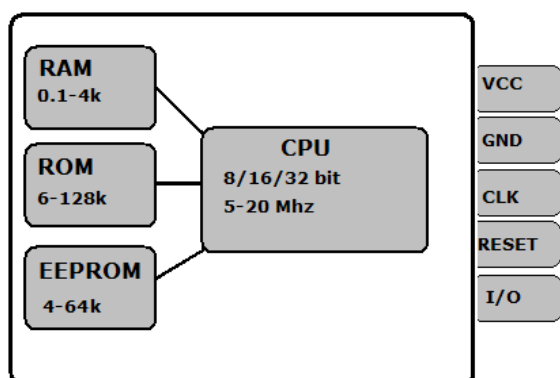
Ce este un Smart Card ?

Un smart card este o cartelă de plastic ce conține un cip încorporat, o arhitectură cu un procesor de 8-biți, RAM (256 bytes), ROM (6 - 8 KB), și EPROM sau EEPROM (câțiva kilobytes). Cardul are propriul său sistem de operare, programe și date iar alimentarea se face direct prin pinii de la cititor.



Structura cip SIM și ambalare

Ce conține un Smart Card ?



Caracteristicile hardware ale unui smart card

CPU: se folosesc procesoare de 8 biți derivate din Motorola 6805 sau Intel 8051, de 16-biți cu procesoare Java Card 3 și 32-bit RISC. Procesorul poate intra în standby pentru a economisi energie.

RAM –ul este de obicei de 1-4 kilobytes. Există uneori două tipuri de memorie RAM, interne, unul utilizat de sistemul de operare și altul extern (XRAM), utilizat de alte aplicații.

ROM: Acesta conține bibliotecile sistemului de operare al cardul de bază și suportul inteligent. Dimensiunea variază de la 6 kilobytes de până la câteva sute de kilobytes.

EEPROM/Flash: memorii programabile nevolatile în care se stochează datele fișierelor pe perioada când cipul nu este alimentat, dar scrierea este foarte lentă (de 100-1000 ori mai lent decât RAM). Capacitatea este de la 4 la 64K (până la 2 GB pe carduri recente, adesea înscrisă pe card ("32K" sau similar).

Comunicație: Serială semi-duplex 9600 bps (până la 115kbps pentru carduri moderne) interfață cu protocol de comunicare între card și gazda. Duplex înseamnă că fie cardul fie gazda trimite date, nu ambele simultan. Unele cartele recente oferă, de asemenea, suport pentru USB (pana la 12Mb/s) și/sau NFC (Near Field Communications) și RFID (Radio Frequency Identification).

Contactele și utilizările lor pe un card inteligent

C1: Sursa de alimentare (V_{CC})

C2: **Reset** - Ștergere (RST)

C3: **Clock** - Ceas (CLK)

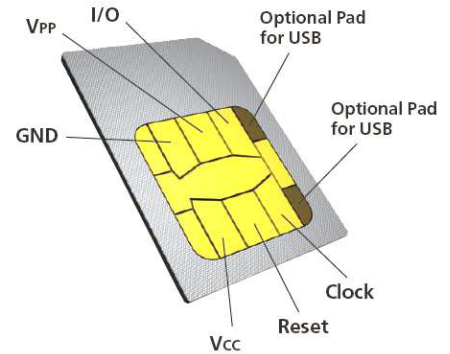
C4: Rezervat (RFU)

C5: Ground (**GND**)

C6: Tensiunea de programare (V_{PP})

C7: Intrare/ieșire (**I/O**)

C8: Rezervat (RFU)

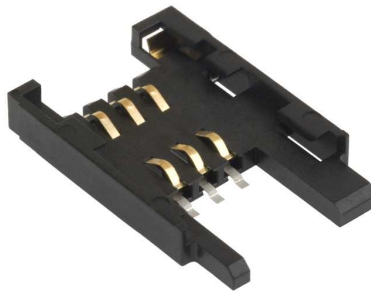
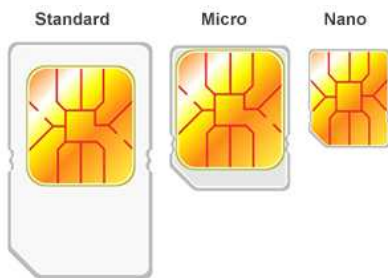


Comunicarea cu cardul presupune următoarele etape:

1. Activarea cipului intern prin cuplarea la cititorul de carduri.
2. Resetarea cardului de cititor
3. Răspunde-la-reset de pe cartelă
4. Selecția opțională a unui tip de protocol
5. Prelucrarea de comenzi succesive
6. Dezactivarea cipului prin cititorul de carduri.

Transferul de date intrare/ieșire presupune transmiterea de caractere asincrone în modul semi-duplex. Fiecare caracter este compus din zece biți consecutivi: un bit de start, opt biți de date și un bit de paritate. Un timp scurt de așteptare, numit "timp de gardă", între caractere succesive permite sincronizarea în transmisiei asincrone de date.

Ce tipuri de SIM există și cum se conectează



Datele

Cartele SIM stochează informații specifice de rețea, utilizate pentru autentificarea și identificarea abonaților în rețea. Cele mai importante dintre acestea sunt numărul unic de serie (ICCID), IMSI, autentificarea cu cheie (K_i), numărul personal de identificare (PIN) pentru utilizarea obișnuită și un cod personal de deblocare (PUK) pentru deblocare PIN, zonă de identitate locală (LAI) și operator de numere de urgență. Cartela SIM stochează și alte date, specifice operatorului de comunicație, cum ar fi SMSC (Short Message Service Center) număr, numele furnizorului de servicii (SPN), numere de servicii de apelare (SDN) și de servicii (VAS) aplicații.

Cartele SIM au diferite capacități de date, de la 32 KB la 128 KB. Toate permit stocarea a maxim 250 de contacte, cele de 32KB au spațiu pentru 33 de Coduri de rețele mobile (MNC) sau "identificatori de rețea" iar cele de 64 KB au spațiu rezervat pentru 80 de CMN.

Autentificarea unui telefon celular cu rețeaua GSM

Procesul de autentificare se face prin cartela SIM (mai precis prin aplicația GSM ce rulează pe card) și se bazează pe un model de întrebare-răspuns. Elementele de bază sunt prezentate mai jos:

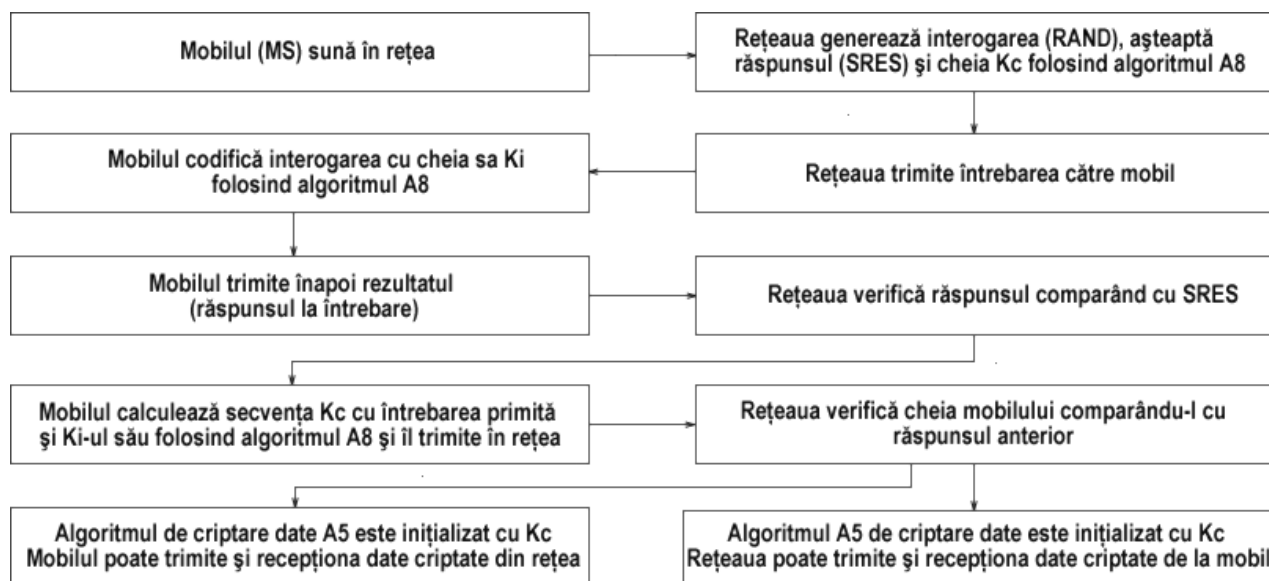


Diagrama simplificată pentru autentificarea terminalului GSM cu rețeaua

Un telefon (echipament mobil sau stație mobilă MS) contactează rețeaua sa. Rețeaua contactează apoi registrul de localizare domiciliu (HLR) pentru operatorul în cauză. HLR verifică contul utilizatorilor de telefon MSISDN. În contul corespunzător este stocat, printre altele, Ki. HLR generează apoi un set de chei (pe baza MSISDN/IMSI și Ki). Acestea sunt trimise înapoi ca întrebare (o întrebare de tip "trimite-mi rezultatul dacă criptezi datele aleatoare cu cheia ta").

Cartela SIM trimite înapoi răspunsul său semnat către rețeaua care verifică cu ceea ce a calculat anterior HLR. Dacă este acceptat, SIM-ul generează o cheie ca o secvență cheie de 64 de biți, numită Kc, calculată prin algoritmul A8. Această se bazează pe Ki și secvența de interogare primită anterior. Aceasta cheie de sesiune este folosită pentru a inițializa algoritmul de criptare A5 (de ambele părți), care este utilizată mai departe pe perioada transmisiei.

GSM-ul suferă de limitarea că este doar receptor, care este verificat de rețea, și nu invers. Un impostor (care are nevoie de o stație falsă) ar putea încerca astfel să identifice Ki-ul receptorului prin emiterea de interogări și analizând răspunsul primit.

Comunicarea între SIM și telefon

Practic, comunicarea între cartela SIM și receptorul (ME) se face printr-o linie de comunicație serie. Există patru protocoale utilizate pentru a transfera date (cu toate acestea protocoalele TPDU și APDU se suprapun).

- TPDU (unitate de protocol transmisie de date) Aceasta este baza protocolului standard de carduri inteligente pentru a trimite și a primi date prin conexiunea de serie. Un SIM modern acceptă mai multe (patru sau mai multe) tranzacții în curs de desfășurare la un moment dat, acestea sunt administrate de așa-numitele canale.

- APDU (unitate de aplicare a protocolului de date) APDU este un protocol tranzacțional de nivel superior care utilizează partea superioară a unității TPDU (piggybacks) pentru a economisi spațiu. APDU comandă înscrierea datelor în interacțiunea SIM/Receptor telefonic (ME). În mod normal, un smart card este o unitate sclav, ceea ce înseamnă că ME este cel care trimite comenzi pentru cartela SIM. Dar cartelele SIM sunt entități foarte active, astfel încât a fost implementat un sistem numit comenzi proactive pentru a rezolva această limitare. Practic, telefonul verifică SIM-ul în mod regulat; SIM-ul răspunde la ceea ce se dorește să se facă. ME procesează cererea și efectuează un transfer înapoi pe cartela SIM spunându-i rezultatul. Acest lucru se poate face asincron (SIM-ul poate prelucra și alte date pe perioada de așteptare).

Data Notes

Dacă doriți să aflați mai multe despre produsele noastre, vizitați situl www.epsicom.com

Dacă ați întâmpinat probleme cu oricare dintre produsele noastre sau dacă doriți informații suplimentare, contactați-ne prin e-mail office@epsicom.com

Pentru orice întrebări, comentarii sau propuneri de afaceri nu ezitați să ne contactați pe adresa office@epsicom.com

31 Sararilor Street | 200570 Craiova, Dolj, Romania | 0723.377.426, 0743.377.426