Opis protokołu Mbus v2 dla telefonów Nokia 3210, 33xx, 3410, 51xx, 61xx, 62xx, 7110, 82xx, 9110, 9210

Programowanie telefonów komórkowych, część 2

Programowanie telefonów komórkowych jest z jednej strony „sztuką magiczną“, natomiast z drugiej można je przeprowadzić za pomocą dowolnego komputera i odpowiedniego oprogramowania. Podstawą jest znajomość protokołu Mbus, który przedstawiamy w artykule.

Blokady (locks)

Telefony komórkowe są wyposażone w systemy bezpieczeństwa, spośród których najczęściej użytkownicy spotykają się z tzw. *simlockiem*. Blokada ta ma za zadanie uniemożliwić eksploatację telefonu poza siecią określonego operatora. Telefon z aktywną blokadą nie będzie więc działał z kartą SIM pochodzącą od innego operatora.

Stwierdzenie które z blokad są aktywne jest możliwe po wysłaniu ramki:

1F – 00 – 10 – 40 – 00 – 04 – 00 – 01 – 8A – 00 – 13 – D3

W odpowiedzi telefon przesyła potwierdzenie przyjęcia ramki:

1F – 10 – 00 – 7F – 33 – 63

następnie przesyła odpowiedź:

1F – 10 – 00 – 40 – 00 – 1A – 01 – 01 – 8A – 00 – 0A – 01 – 10 – 00 – 00 – 00 – 00 – 00

00 – 00 – 00 – 00 – 00 – 00 – 00 – 10 – 00 – 00 – 00 – 00 – 00 – 0D – D9

Odebrane dane należy potwierdzić przesyłając do telefonu ramkę:

1F – 00 – 10 – 7F – 0D – 7D

Bajt 10h zaznaczony kolorem w odebranej ramce danych zawiera informację o aktywnych blokadach. Najistotniejszą informację niosą cztery mniej znaczące bity bajtu:

Bit na pozycji (2^0)= 0/1 - brak/aktywna blokada LOCK1 (simlock)

Bit na pozycji (2^1)= 0/1 - brak/aktywna blokada LOCK2

Bit na pozycji (2^2)= 0/1 - brak/aktywna blokada LOCK3

Bit na pozycji (2^3)= 0/1 - brak/aktywna blokada LOCK4

Przykładowa odpowiedź telefonu, który ma aktywną blokadę simlock:

1F – 10 – 00 – 40 – 00 – 1A – 01 – 01 – 8A – 00 – 0A – 01 – 01 – 00 – 00 – 26 – 00

1F – FF – FF – FF – FF – F0 – 00 – 00 – 00 – 00 – 00 – 00 – 00 – 00 – 00 – 03 – 1F

Kod operatora, dla którego jest założona blokada simlock znajduje się w 16, 17 i 18 bajcie odebranej ramki danych. Kod ma długość 2,5 bajtu:

26 – 00 – 1F

Pokazany ciąg bajtów niesie informację o aktywnej blokadzie simlock założoną na operatora Plus GSM - 260-01 (**tab. 4**).

Tab. 3. Blokady stosowane w większości współczesnych telefonów komórkowych

Blokada	Oznaczenie	Długość
LOCK1 (simlock)	MCC+MNC	2 bajty + półbajt
LOCK2	GID1	2 bajty
LOCK3	GID2	2 bajty
LOCK4	MSIN	5 bajtów

Tab. 4. Kody operatorów sieci komórkowych

Operator	Kod MCC+MNC
PLUS GSM	260 - 01
ERA GSM	260 - 02
IDEA CENTERTEL	260 - 03

Monitor sieci

Monitor sieci to specjalny tryb, w którym mamy możliwość monitorowania większości parametrów sieci oraz telefonu. Funkcja ta jest zazwyczaj ukryta i chcąc mieć do niej dostęp należy ją aktywować.

Większość danych obserwowanych w Net-Monitorze jest dla „zwykłych“ ludzi niezrozumiała - jest to po prostu seria zmieniających się cyfr i liter.

Tab. 5. Kody rozkazów związanych z obsługą Net-Monitora

Polecenie	Rozkaz binarny
Aktywacja Net-Monitora	0x7E, 0xF2
Usunięcie Net-Monitora	0x7E, 0xF1
Rozwinięcie menu Net-Monitora	0x7E, 0xF3

Dane te dla specjalistów są w pełni zrozumiałe i dzięki nim mogą oni dowiedzieć się prawie wszystkiego o działaniu sieci i jej stanie.

Aktywacja Net-Monitora wymaga wysłania ramki:

1F – 00 – 10 – 40 – 00 – 04 – 00 – 01 – 7E – F2 – 14 – D2

Telefon potwierdza jej odbiór za pomocą ramki:

1F – 10 – 00 – 7F – 14 – 64

następnie przesyła odpowiedź:

1F – 10 – 00 – 40 – 00 – 38 – 01 – 01 – 7E – 00 – 00 – EA – 00 – 10 – CC – D8 – 00 – 00 – 00

00 – 00 – 00 – 00 – 00 – 00 – 10 – CC – D8 – 00 – 09 – 00 – 00 – 00 – 09 – 00 – 00 – 02 – FF

00 – 00 – 01 – 43 – 01 – 11 – 00 – 00 – 00 – 00 – 01 – 00 – 00 – FF – 00 – 00 – 00 – 00 – 00

00 – 00 – 00 – 01 – 42 – 07 – F6

Odebrane dane potwierdzamy wysyłając ramkę:

1F – 00 – 10 – 7F – 0E – 7E

Pozostałe rozkazy związane z obsługą Net-Monitora zestawiono w **tab. 5**.

Logo operatora

Standardowe logo operatora ma wymiary 72 piksele x 14 pikseli i zajmuje w pamięci 126 bajtów. Nasze własne logo musimy wysłać do telefonu w określonym porządku, aby zostało prawidłowo odebrane i wyświetlone na wyświetlaczu telefonu. Każdy wiersz wyświetlacza zajmuje w pamięci 72 bity, na które składa się 9 ko-

Rys. 3. Wygląd projektowanego logo

Rys. 4. Wygląd wyświetlacza telefonu z wyświetlonym nowym logo

lejnych bajtów. Będziemy wiec wstawiać kolejne bajty grafiki poruszając się zawsze z lewej do prawej w każdym z wierszy. „Świecący" piksel ma wartość „1", natomiast „zgaszony" wartość „0". Dla przykładu, zapis bitowy grafiki pokazanej na **rys. 3** wygląda następująco:

W1 - 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
W2 - 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000001
W3 - 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000001
W4 - 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000001
W5 - 10010010 10010010 10010010 00001110 01111000 00011100 01110011 10110000 01111001
W6 - 10010010 10010010 10010010 00010001 01000100 00100010 10001010 01001000 01000101
W7 - 10101010 10101010 10101010 00011111 01000100 00100000 10001010 01001000 01000101
W8 - 10101010 10101010 10101010 00010000 01000100 00100000 10001010 01001000 01000101
W9 - 01000100 01000100 01000100 00010001 01000100 00100010 10001010 01001000 01000101
W10 - 01000100 01000100 01000100 10001110 01111001 00011100 01110010 01001010 01111001
W11 - 00000000 00000000 00000000 00000000 01000000 00000000 00000000 00000000 00000000 01000000
W12 - 00000000 00000000 00000000 00000000 01000000 00000000 00000000 00000000 00000000 01000000
W13 - 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
W14 - 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000

Wx - wartości poszczególnych bitów w określonym wierszu (x - numer wiersza).

Format wysyłanej ramki jest następujący:

1F – 00 – 1D – 05 – 00 – 8C – 00 – 01 – 00 – 30 – 00 – 62 – F0 – 30 – 00 – 82 – 00 – 48 – 0E – 01 – 00 – 00 – 00 – 00 – 00
00 – 00 – 00 – 00 – 00 – 00 – 00 – 00 – 00 – 00 – 00 – 00 – 00 – 01 – 00 – 00 – 00 – 00 – 00 – 00 – 00 – 01 – 00 – 00 – 00
00 – 00 – 00 – 00 – 00 – 01 – 92 – 92 – 92 – 0E – 78 – 1C – 73 – B0 – 79 – 92 – 92 – 92 – 11 – 44 – 22 – 8A – 48 – 45 – AA
AA – AA – 1F – 44 – 20 – 8A – 48 – 45 – AA – AA – AA – 10 – 44 – 20 – 8A – 48 – 45 – 44 – 44 – 44 – 11 – 44 – 22 – 8A – 48
45 – 44 – 44 – 44 – 8E – 79 – 1C – 72 – 4A – 79 – 00 – 00 – 00 – 00 – 40 – 00 – 00 – 00 – 40 – 00 – 00 – 00 – 00 – 40 – 00
00 – 00 – 40 – 00 – 00 – 00 – 00 – 00 – 00 – 00 – 00 – 00 – 00 – 00 – 00 – 00 – 00 – 00 – 00 – 00 – 00 – 0F – A6

Po wysłaniu powyższej ramki do telefonu, na wyświetlaczu telefonu zostanie wyświetlone nowe logo (przykład pokazano na **rys. 4**).

Regulacja kontrastu wyświetlacza LCD (profil)

Wartości wszystkich parametrów wchodzących w skład ustawień profili użytkowych, są określone przez 4 bajty. Każdy z bajtów określa inne parametry. Wartość czwartego bajtu odpowiedzialna jest między innymi za wartość kontrastu wyświetlacza LCD.

Kontrast wyświetlacza LCD w telefonie może być regulowany w granicach 0...21h. Typowa wartość kontrastu dla w pełni sprawnego wyświetlacza, zapewniająca najlepszą widoczność to 0Fh lub 10h.

Zmiana kontrastu wymaga wysłania do telefonu ramki:

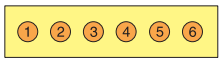
1F – 00 – 1D – 40 – 00 – 07 – 00 – 01 – 6B – 00 – 00 – 00 – XX – Seq – CheckSum

XX - wartość kontrastu wyświetlacza LCD (wartość szesnastkowa)

Złącza wybranych telefonów firmy Nokia

Nokia 3210

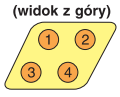
(widok z góry)



1 - BTEMP
2 - TX
3 - GND
4 - Mbus
5 - RX
6 - Vpp

Nokia 3310, 3330, 5110

(widok z góry)



1 - Mbus
2 - GND
3 - RX
4 - TX

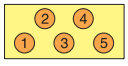
Nokia 51xx, 61xx, 62xx, 71xx

(klawiatura do góry)

6 - Mbus
7 - RX
8 - TX
9 - GND

Nokia 5210, 8210, 8250, 8850

(widok z góry)



1 - Mbus
2 - GND
3 - RX
4 - TX

Tab. 6. Kody poleceń związanych z testowaniem telefonu

Polecenie	Rozkaz binarny
Test LCD -1	0xD3, 0x03, 0x02
Test LCD -2	0xD3, 0x03, 0x01
Wyczyszczenie wyświetlacza LCD	0xD3, 0x02, 0x03
Test Buzzera	0x8F

Seq - numer sekwencji ramki
CheckSum - Suma kontrolna dla ramki

Po wysłaniu takiej ramki telefon należy wyłączyć następnie ponownie włączyć aby przeprowadzona operacja odniosła skutek.

Zmiana kodu zabezpieczającego

Kod zabezpieczający to 5-cyfrowy kod, który zabezpiecza nasz telefon przed niepowołanym dostępem. Wcześniej opisana była procedura odczytu kodu zabezpieczającego, poniżej opiszę procedurę zmiany tzw. *Security Code*. Aby zmienić kod zabezpieczający należy wysłać ramkę z rozkazem jego zmiany na inny:

1F – 00 – 10 – 40 – 00 – 09 – 00 – 01 – 6F – 01 – X1 – X2 – X3 – X4 – X5 – 00 – SeqNumber – CheckSum

X1, X2, X3, X4, X5 - kolejne cyfry nowego kodu

Po bajtach zawierających nowe wartości dla określonego parametru występuje zawsze bajt zerowy „00". Nie dotyczy to edycji profilu!

Przykład:

Aby zmienić kod zabezpieczający na 22222 należy wysłać do telefonu ramkę w poniższym formacie (znaki kodowane w ASCII):

32h = 2

Ramka z rozkazem ustawienia kodu zabezpieczającego na 2222:

1F – 00 – 10 – 40 – 00 – 0A – 00 – 01 – 6F – 01 – 32 – 32 – 32 – 32 – 32 – 00 – 2F – 37

Telefon potwierdza przyjęcie ramki:

1F – 10 – 00 – 7F – 2F – 5F

następnie przesyła odpowiedź:

1F – 10 – 00 – 40 – 00 – 05 – 01 – 01 – 6F – 01 – 01 – 03 – 26

Potwierdzamy odbiór danych za pomocą ramki:

1F – 00 – 10 – 7F – 0F – 7F

Po wysłaniu powyższej ramki do telefonu, kod zabezpieczający w telefonie zostanie ustawiony na 22222.

Test wyświetlacza LCD i buzzera

Istnieje możliwość wysłania ramek z rozkazem przeprowadzenia testów określonych podzespołów naszego telefonu np. buzzera, wyświetlacza LCD, silniczka wibratora itp.

Przedstawię jedynie rozkazy odpowiedzialne jedynie za test wyświetlacza LCD i buzzera (**tab. 6**).

Tab. 7. Kody poleceń umożliwiających przywrócenie ustawień domyślnych

Polecenie	Rozkaz binarny
Przywrócenie ustawień fabrycznych	0x65, 0x38
Zerowanie telefonu bez ponownego pytania o kod PIN	0x64, 0x03
Zerowanie telefonu z pytaniem o kod PIN	0x64, 0x04

Przykłady:

Test1 LCD:

1F – 00 – 10 – 40 – 00 – 05 – 00 – 01 – D3 – 03 – 02 – SeqNum – CheckSum

Czyszczenie wyświetlacza LCD:

1F – 00 – 10 – 40 – 00 – 05 – 00 – 01 – D3 – 02 – 03 – SeqNum – CheckSum

Test Buzzera:

1F – 00 – 10 – 40 – 00 – 03 – 00 – 01 – 8F – SeqNum – CheckSum

Po wyłączeniu telefonu i ponownym włączeniu, wszystkie ustawienia przyjmą wartości takie jak przed wykonaniem testu!

Zerowanie telefonu i ustawienia fabryczne

Po przywróceniu ustawień fabrycznych wszystkie ustawienia telefonu przyjmą standardowe wartości (logo, dzwonki, kod zabezpieczający itp.). Kody poleceń zestawiono w **tab. 7**.

Po przywróceniu ustawień fabrycznych należy wykonać zerowanie telefonu!

Przykład:

Ramka z rozkazem przywrócenia ustawień fabrycznych w telefonie

1F – 00 – 10 – 40 – 00 – 04 – 00 – 01 – 65 – 38 – 00 – 17

Nokia potwierdza przyjęcie ramki:

1F – 10 – 00 – 7F – 00 – 70

Potwierdzamy odbiór

1F – 00 – 10 – 7F – 10 – 60

Po przywróceniu ustawień fabrycznych w telefonie, wszystkie parametry telefonu przyjmą domyślne wartości (kod zabezpieczający - 12345, ustawienia połączeń itd.).

Informacje zawarte w artykule z pewnością nie są kompletne, ponieważ standard komunikacji z telefonami marki Nokia nie został publicznie przedstawiony przez jego producenta.

Marcin Czerniawski
SimKom@wp.pl

Pragnę gorąco podziękować mojej dziewczynie Agnieszce za duchowe wsparcie podczas zdobywanie informacji na temat protokołu oraz podczas pisania artykułu. Bez jej pomocy artykuł nigdy by nie powstał.