Tarnowska Karta Miejska – dokumentacja techniczna

Zawartość

Tarnowska Karta Miejska – wstęp

Tarnowska Karta Miejska jest kartą imienną. Kartę można podzielić na dwa rodzaje:

- Kartę premium - przeznaczoną dla osób fizycznych na stałe zameldowanych w Tarnowie (Gminie Miasta Tarnowa),
- Kartę standard - przeznaczoną dla osób fizycznych zameldowanych poza Tarnowem oraz dla firm,

Obie karty są wyposażone w interfejs zbliżeniowy, natomiast karta premium posiada dodatkowo interfejs stykowy, dzięki czemu jej posiadacze mogą wgrywać bilety okresowe na kartę z dowolnego komputera wyposażonego w czytnik stykowy.

Funkcjonalności wspólne dla obu typów karty to:

- nośnik biletów okresowych tarnowskiej komunikacji miejskiej,
- elektroniczna portmonetka,
- dostęp do internetowego systemu doładownia ekarty - sdk.umt.tarnow.pl,
- każdej karcie poza głównym numerem ekarty widocznym na jej awersie, jest przypisany drugi numer (rewers) zaprezentowany w postaci dziesiętnej oraz kodu kreskowego. W przyszłości numer ten będzie wykorzystywany do identyfikacji w systemach innych jednostek miejskich zintegrowanych z tarnowską kartą miejską.

Tarnowska Karta Miejska - struktura

Karta premium	**Karta standard**
Karta Javowa oko 20 kB pamięci z emulacją Mifare Classic (16 sektorow)	Mifare Classic - sektorowa (16 sektorów)
System szyfrowania i modułów SAM w celu zabezpieczenia danych karty.	System szyfrowania i modułów SAM w celu zabezpieczenia danych karty.

Tutaj można dograć aplikację sektorową lub javową.	Tylko aplikację sektorową
Zajęte 6 kB , zajęte 6 sektorów	Zajęte 6 sektorów
Wolne ok. 14 kB na aplet javy i 8 sektorów na aplikację sektorową	Wolne 8 sektorów na aplikację sektorową
Nieużywana powierzchnia apletowa i sektorowa jest zablokowana, ale z możliwością odblokowania dla innego podmiotu.	Nieużywana powierzchnia sektorowa jest zablokowana, ale z możliwością odblokowania dla innego podmiotu.
Możliwa integracja pod warunkiem że to nie będzie technologia ani DesFire ani Mifare plus. Możliwość dograna apletu java lub aplikacji sektorowej MifareClassic.	Możliwa integracja pod warunkiem że to nie będzie technologia ani DesFire ani Mifare plus. Możliwość aplikacji sektorowej MifareClassic.
Możliwość dołożenia drugiego modułu SAM do kontrolerki oraz implementacji aplikacji obsługującej kilka modułów SAM.	

Są dwa typy kart, dostarczone przez BULL wraz z oprogramowaniem:

Karta Premium:

Na bazie karty dwu-interfejsowej (stykowej i bezstykowej w jednym plastiku) Obertur ID Cosmo 7.0.1 Karta z systemem operacyjnym Java 20kB

- aplikacja ogólna – 1 blok;
- aplet e-portmonetki - 2 bloki.

Na Emulację Mifare Clasic 1kB, 16 sektorów dla produktów:

- administracyjne/personalizacyjne – 2 sektory;
- 2 bilety okresowe - 2 sektory;
- e- portmonetka miejska (na np. parkometry) – 2 sektory;
- t-portmonetka (transportowa na bilety punktowe) – 2 sektory.

Stosowane jest sprzętowe zabezpieczenie dostępu do karty poprzez moduły SAM typu J2A080GX0-JCOP-2.4.1-PVC SIM w urządzeniach.

Karta Standard

Karta Mifare Clasic 1kB, 16 sektorów dla produktów:

- administracyjne/personalizacyjne – 2 sektory;
- 2 bilety okresowe – 2 sektory;

- e- portmonetka miejska (na np. parkometry) – 2 sektory;
- t-portmonetka (planowana transportowa na bilety punktowe) – 2 sektory.

Stosowane jest sprzętowe zabezpieczenie dostępu do karty poprzez moduły SAM typu J2A080GX0-JCOP-2.4.1-PVC SIM w urządzeniach.

Karta Premium – dualna - zbliżeniowa oraz stykowa – dane techniczne

1. Układ scalony (nie dopuszczamy rozwiązania hybrydowego)

a) Pamięć EEPROM, minimum 12kB

b) Minimum 2kB pamięci RAM

c) Wbudowany procesor kryptograficzny obsługujący algorytm RSA (długość klucza minimum 1024 bitów) oraz algorytmy 3DES lub AES

d) Wbudowany system zarządzania pamięcią

e) Trwałość zapisu informacji w pamięci EEPROM – nie mniej niż 10 lat

f) Liczba cykli programowania (zapis-odczyt) pamięci EEPROM: minimum 100.000

2. Komunikacja

a) Podwójny interfejs: stykowy i bezstykowy

b) Interfejs bezkontaktowy zgodny z ISO/IEC 14443 A:

a. częstotliwość nośna 13,56 MHz

b. pełna antykolizja

c) Interfejs stykowy zgodny z ISO/IEC 7816-1; -2; -3;

3. Karta

3.1. Charakterystyka fizyczna

a) Wymiary karty zgodnie z normą ISO/IEC 7810, format ID-1

b) Wykonana z tworzywa sztucznego nie zawierającego szkodliwych składników chemicznych i przyjazna dla środowiska zgodnie z Rozporządzeniem Ministra Przemysłu i Handlu z dnia 30.11.1994 r. w sprawie wymagań, jakie powinny spełniać wyroby ze względu na potrzebę ochrony zdrowia środowiska (Dz.U. 133 Poz. 690 z późniejszymi zmianami)

c) Antena wykonana z drutu miedzianego izolowanego, zgodnego z normami: IEC 60317-20, IEC 60317-4 oraz NEMA: MW 79, MW2 i MW 75, wtopiona w rdzeń karty

3.2. Parametry wytrzymałościowe

a) Wilgotność względna środowiska pracy karty do 90%

b) Wytrzymałość mechaniczna, temperaturowa bez utraty funkcjonalności i walorów estetycznych oraz wytrzymałość chemiczna muszą spełniać co najmniej wymagania zawarte w normie ISO/IEC 10373

4.Wymagania dotyczące Systemu Operacyjnego (SO) dostarczonego i zainstalowanego na karcie.

4.1. Wieloaplikacyjny system operacyjny

4.2. Certyfikaty zgodności, zaświadczające spełnienie wymagań określonych w normach:

4.3. Struktura danych zgodna z normą ISO/IEC 7816-4 lub Java Card/GP lub równoważna,

4.4. Bezpieczeństwo:

(1) Zewnętrzne i wewnętrzne wzajemne uwierzytelnianie zgodne z normą ISO/IEC 7816-4 i -8 lub równoważne

(2) Zabezpieczenie komunikacji zgodnie z normą ISO/IEC 7816-4 lub równoważne

(3) Spełnienie wymagań obsługi PIN zgodnie z normą ISO/IEC 7816-4 lub równoważne

(4) Elementy systemu PKI zgodne z normą CWA 14890-1; -2 lub w równoważne.

4.5. Aplikacje

System Operacyjny powinien gwarantować możliwość dopisania nowych aplikacji do karty elektronicznej już wyemitowanej. Dopisanie nowych aplikacji powinno być zrealizowane w bezpiecznym otoczeniu karty, przy zachowaniu instrukcji/poleceń zgodnych z normą ISO/IEC 7816-4; - 8; -9 lub w sposób równoważny

Karta Standard – zbliżeniowa - dane techniczne

1. Układ scalony

a) Trwałość zapisu informacji w pamięci EEPROM – nie mniej niż 10 lat

b) Liczba cykli programowania (zapis-odczyt) pamięci EEPROM: minimum 100.000

2. Komunikacja

a) Komunikacja między kartą a czytnikiem odbywa się drogą radiową

b) Częstotliwość nośna: 13,56 MHz.

c) Interfejs bezkontaktowy musi spełniać warunki normy „ISO/IEC 14443 typ A części 1-3

d) Szybkość komunikacji:106 Kbit/s.

e) Zasięg operacyjny: do 10 cm.

f) Pełna antykolizja

3. Charakterystyka fizyczna

a) Karta musi być wykonana z tworzywa sztucznego nie zawierającego szkodliwych składników chemicznych i być przyjazna dla środowiska zgodnie z Rozporządzeniem Ministra Przemysłu i Handlu z dnia 30.11.1994 r. w sprawie wymagań jakie powinny spełniać wyroby ze względu na potrzebę ochrony zdrowia i środowiska (Dz. U. 133/94 poz. 690 z późniejszymi zmianami).

b) Dostawca musi zagwarantować wysoką jakość połączeń elektrycznych pomiędzy anteną, a układem elektronicznym w całym okresie eksploatacji karty.

c) Wymiary zgodne z normami ISO 7816-7810 jak karty płatnicze ID-1 (85,8 x 54 x 0,76 mm

d) Antena wykonana z drutu miedzianego izolowanego, zgodnego z normami: IEC 60317-20, IEC 60317-4 oraz NEMA: MW 79, MW2 i MW 75, wtopiona w rdzeń karty. Nie dopuszcza się innych technologii wykonania anteny.

4. Parametry wytrzymałościowe

a) Wytrzymałość: mechaniczna, temperaturowa (od -20°C do +50°C) bez utraty funkcjonalności i walorów estetycznych oraz wytrzymałość chemiczna muszą spełniać co najmniej standardy opisane w normie ISO 10373.

b) Trwałość całkowita 10 lat w warunkach normalnej eksploatacji.

c) Wilgotność względna środowiska pracy karty do 90%

5 Charakterystyka techniczna

Karta wykonana zostanie na bazie układu scalonego IC MF1S5030X lub układu równoważnego. Wysokość procentowa tak zwanych "zwrotów z pola" (FRR) kart zbliżeniowych nie będzie przekraczać 0,70 %.

6. Zabezpieczenia

a) Karty muszą zawierać skuteczne zabezpieczenia zgodne z w/w normą.

b) Każda karta musi zawierać unikalny i niezmienny numer zapisany na 32 bitach, programowany trwale przez producenta układu pamięciowego.

c) Karty muszą umożliwiać wzajemne uwierzytelnienie z czytnikiem zgodnie z normą ISO/IEC DIS 9798-2.

d) Komunikacja między kartą i czytnikiem odbywająca się drogą radiową musi być szyfrowana z wykorzystaniem generowanej na karcie liczby losowej i 48 bitowego klucza.

e) Dostęp do każdego z 16 sektorów musi być zabezpieczony za pomocą kluczy (do każdego sektora oddzielna para (2) kluczy).

f) Integralność danych w karcie chroniona z użyciem 16 bitowego CRC,

g) Musi istnieć możliwość wyłączania programowanych funkcji zapisu dla kart wycofywanych z obiegu.

7. Pamięć

a) Technologia: CMOS EEPROM.

b) Pojemność kart imiennych i na okaziciela : 1kB

c) Podzielona na 16 niezależnych sektorów po 4 bloki każdy.

d) Ilość cykli zapisu: minimum 100 000 (wg specyfikowanego przez producenta zakresu warunków pracy).

e) Ilość cykli odczytu: nielimitowana.

f) Okres przechowywania danych: 10 lat.

8. Zasilanie

Karta zasilana jest indukcyjnie przez czytnik. Karta nie posiada własnego źródła zasilania.