



eCitizen

NORTH East South West
INTERREG III C



PROJECT PART-FINANCED
BY THE EUROPEAN UNION

Aldata

Aldata Smart Card Oy

Mifare-selvitys
Tampereen kaupunki

Versio
Hyväksytty

Vastuhenkilö
Ari Saapunki

TALLENNUSPAIKKA:

Sopimusarkisto: Sopimukset/Tampereen kaupunki/Mifare_raportti/ Mifare_selvitys

MUUTOSHISTORIA

Versio	Päiväys	Laatija	Muutoksen kuvaus / hyväksyjä
1.0	4.7.2005	JK-V	Hyväksytty
0.8	30.6.2005	JK-V	Hyväksynnälle Tampereelle
0.7	29.6.2005	Henri Otava	Tehty tarkennuksia
0.6	29.6.2005	Henri Otava	Lisätty Mifare sarjanumeron UID tarkempi kuvaus
0.5	22.6.2005	ASa	Hyväksynnälle Tampereelle
0.4	21.6.2005	ASa	Sisäinen hyväksyntä
0.3	20.6.2005	Henri Otava	Lisätty Mifare numero selvitystä
0.2	13.6.2005	ASa	Lisätty sektoreiden tarkastelu
0.1	11.6.2005	Ari Saapunki	Selvityksen runko-osat

JAKELU

Aldata Smart Card Oy
Tampereen kaupunki

1. Mifare –kortti	2
2. Sarjanumero	3
3. Sektoreiden käyttö	4
3.1. Sektori 0 / Lohko 0	5
3.2. Lohkot 1,2,4,5,6,8,9,10	5
3.3. Lohkot 3, 7, 11, 15,	5
4. MAD (Mifare Application Directory)	5
4.1. Tietoelementit sovellushakemistoja varten	5
4.1.1 Sovellus ID	5
4.1.2 Kiertoredundanssikoodi tavu (CRC)	6
4.1.3 Info tavu	6
4.1.4 Yleistavu (GPB)	6
4.1.5 Luku-avain A	6
4.1.6 Kirjoitusavain B	6
4.2 Sovellushakemistojen koodaus	7
4.2.1 MAD versio numero	7
4.2.2 MAD tyypit	7
4.2.3 Toiminnallisuusryhmä	7
4.2.4 Ohjauskoodit	7
4.2.5 Kortin lukija informaatio	7

1. Mifare –kortti

Yleistä:

Mifare –kortti on yleisesti maailmalla käytetty RF ID (Radio Frequency Identification) teknologiaan pohjautuva ISO 14443 type A:n mukainen teknologia. Kortin keskeisiä toiminnallisuuksia tarjoavia elementtejä ovat:

-
- Globaalisti yksilöllinen sarjanumero
 - 1 tai 4 kilotavun sektoreihin jaettu muisti
 - Turvamenettelyt rinnakaisten sovellusten käsittelyyn kortilla
 - Laskuritoiminnallisuus maksu – ja lipputuotekäyttöön
 - Etäluettavuus (proximity < 10 cm)

2. Sarjanumero

Mifaren standardi kortti (1 kilotavu)

Mifare tukee ISO/IEC standardin 14443-3A määrittelemää tapaa hoitaa törmäyksenestoa ja sirun valikointia. Tämä tapahtuu lyhyesti seuraavasti.

1. Lukija tutkii onko siruja lukuetaisyydellä
2. Jos lukuetaisyydellä useampia siruja lähetetään ANTCOLLISION – komentoja muille kuin valitulle sirulle kunnes vain yksi siru valikoitavassa tilassa.
3. Suoritetaan SELECT komento, joka palauttaa Mifare sirutyypin koodin SAK (Select Acknowledge, Type A), joka on esim. 1K kortilla hex 08 ja 4K kortilla hex18. Samalla saadaan UID (Unique identifier), jonka ensimmäinen tavu UID0 sisältää valmistajan tiedon ISO/IEC 7816-6 / AM1 IC Manufacturer registration standardin mukaisesti, joka on esim. Philipsillä hex04.
4. UID:n seuraavat tavut UID1-UID9 sisältävät itse Mifaren sarjanumeron. Mifaren tyypistä määräytyy sitten itse sarjanumeron pituus, joka 1K/4K Mifareissa 4 tavua (32 bittiä).

Edelliset tiedot sijaitsevat kortilla sektorilla 0 lohkoissa 0. Tämä tieto generoidaan ja kirjoitetaan sirulle sirunvalmistajan toimesta tehtaalla ja kirjoitussuojataan. Samassa sektorissa on myös muuta valmistajan tallentamaa tietoa 12 tavua.

Riippuen käytettävästä lukijasta/ohjelmistosta 4 - tavuinen sarjanumero voidaan tulkita ja esittää eritavoin. Alla yleisimmät tavat:

- 32-bit, MIFARE Kortin sarjanumero. UID1 UID2 UID3 UID4 heksana. Esim A0 A1 A2 A3
- 32-bit, MIFARE Kortin sarjanumero käänteinen. Sama kuin edellinen, mutta tavut käänteisessä järjestyksessä. UID4 UID3 UID2 UID1 heksana. Esim A3 A2 A1 A0
- 26-bit, MIFARE Kortin sarjanumero. Jolloin luetaan vain osa sarjanumerosta esim. Kulunvalvonnan rajoitteiden takia. Tässä tapauksessa kaksoiskappaleet mahdollisia, jolloin on tavallista, että itse lukija lisää siihen oman tunnisteensa.
- 34-bit, MIFARE Kortin sarjanumero ja alku/loppupariteetti tarkisteella.

- 40-bit, MIFARE Kortin sarjanumero ja 8-bit tarkistesumma. Tarkiste laskettu Philips standardin mukaisesti. Tämä tarkistesumma on sirulla heti sarjanumeron perässä.

Useat Mifare kortit käyttävät Philipsin MF1 S50 eli klassista yhden kilotavun sirua. Siitä on tullut uusi silikoniversio 1998, jonka tunnistaa myös sarjanumerosta seuraavasti.

Sarjanumero, revision 03/04 : XX XX XX X2 tai esim. käänteisesti X2 XX XX XX XX

3. Sektoreiden käyttö

Mifare Standard
Sektori 0 (Lohko: 0 – 3)
Sektori 1 (Lohko: 4 – 7)
Sektori 2 (Lohko: 8 – 11)
...
Sektori 15 (Lohko: 60 – 63)
Sektori 2 (Esimerkki)
Lohko 8: Data tai lukuarvo (16 tavua)
Lohko 9: Data tai lukuarvo (16 tavua)
Lohko 10: Data tai lukuarvo (16 tavua)
Lohko 11: Avain A, Käyttöoikeudet (4 tavua), Avain B (12 tavua)

Jokaisen sektorin viimeinen lohko sisältää avaimet A ja B sekä käyttöoikeus tavut, joilla määritellään ko. sektorin lohkojen käyttöoikeudet. Oikeusbitit määrittelevät myös "data" lohkojen tyyppin (luku/kirjoitus tai lukuarvo).

- Luku/kirjoitus lohkot on tarkoitettu esim. langatonta pääsynhallintaa varten
- Lukuarvo lohkot on tarkoitettu esim. elektronista kukkaroa varten, jolloin tallennettua arvoa voidaan käsitellä lisäkomennoilla (mm. increment, decrement)

Tiedot tallentuvat luku/kirjoituslohkoille tavuina eli heksalukuina. Tällöin tekstipohjaisten tietojen tallennuksessa tulee käyttää jotain tiettyä merkistöä, jota ohjelmisto sitten tukee. Esimerkiksi ASCII 850. Tällöin yksi merkki vie kortilta yhden tavun.

Lukuarvolohkoilla arvo tallentuu tietyllä turvamenetelmällä käyttäen koko lohkon.

Järjestelmän turvatasoa voidaan nostaa käyttämällä sektorikohtaisia avaimia, jolloin varmentamattomat henkilöt eivät voi käyttää suojattuja sektoreita. Koska avaimet

ovat sektorikohtaisia, jokainen sektori voidaan suojata eri avainparilla. Toisin sanoen jokainen sovellus voidaan suojata omilla avaimilla.

Yleisohjeena personoinnille voidaan pitää seuraavaa:

- A) Tunnistaminen, pääsyn hallinta, datan tallennus sovellukset
Mifare kortit toimitetaan toimitusavaimilla ja korttia voidaan käyttää niillä avaimilla. Myöskään pääsyoikeuksia ei tarvitse muuttaa.
- B) Maksaminen, lippusovellukset
Turvallisuuden kannalta on suositeltavaa vaihtaa pääsyoikeudet sekä avaimet..
Vaihtelevat avaimet: Avaimet voidaan modifioida käyttäen kortin sarjanumeroa sekä kortin muistisisältöä, joten jokainen kortti käyttää eri avaimia.

3.1. Sektori 0 / Lohko 0

Sarjanumero (4 tavua)	Tarkistus tavu (1 tavu)	Valmistaja tiedot (11 tavua)
-----------------------	-------------------------	------------------------------

Tämä lohko on kirjoitussuojattu.

3.2. Lohkot 1,2,4,5,6,8,9,10 ...

Tietolohko (16 tavua)

Sektoreiden 3 ensimmäistä lohkoa

3.3. Lohkot 3, 7, 11, 15, ...

Avain A (6 tavua)	Käyttöoikeudet (4 tavua)	Avain B (6 tavua)
-------------------	--------------------------	-------------------

Sektoreiden 4. eli viimeinen lohko

4. MAD (Mifare Application Directory)

Rekisteröity sovellus ID sektorissa 0 kaikilla Mifare korteilla mahdollistaa kaikkien rekisteröityjen korttisovellusten tunnistamisen.

MAD1 (Käytössä 1k korteilla).

MAD2 (käytössä > 1k korteilla), on täysin yhteensopiva MAD1 kanssa.

4.1. Tietoelementit sovellushakemistoja varten

4.1.1 Sovellus ID

Yksilöllinen 16 bittinen koodi, joka on jaettu kahteen osaan.

Toiminnallisuusryhmä koodi (8 bittiä)	Sovelluskoodi (8 bittiä)
---------------------------------------	--------------------------

Toiminnallisuusryhmäkoodin käyttö mahdollistaa sovellusten luokittelun.

4.1.2 Kiertoredundanssikoodi tavu (CRC)

8 bittiä sisältää kiertoredundanssikoodin CRC lisäproessorin mukaan. Lisäproessori tulee uudelleen käynnistää, jonka jälkeen sekä Info tavu ja ID1 – ID15 tavut tulee välittää CRC lisäproessorille juuri tässä järjestyksessä. Tämä koodi sallii hakemistolohkon eheystarkistuksen.

4.1.3 Info tavu

Tiedot kortin julkaisija sektorissa on erityisen käyttökelpoisia silloin, kun halutaan selvittää organisaatio, joka on vastuussa vapaiden korttisektoreiden jakamisesta uusille sovelluksille. Vapaita korttisektoreita voidaan helposti käyttää lisäsovelluksille.

Bit 0 – 5 Osoitin kortin julkaisijan sektoriin
Bit 6 – 7 RFU

4.1.4 Yleistavu (GPB)

Yleistavu käyttöoikeus kentässä sektorissa nolla kuvaa seuraavia yksityiskohtia MAD standardissa. Se on kymmenes tavu kolmannessa lohossa. Koodia 0x69 ei tule käyttää standardoiduissa korteissa, koska se viittaa ei-personoituihin kortteihin.

bit 7						bit 1	bit 0
DA	MA	RFU	RFU	RFU	RFU		ADV

ADV (MAD versio koodi)	01	MAD versio 1 (sektorit 1 – 15)
	10	MAD versio 2 (sektorit 1 – 39)
MA (monisovelluskortti)	1	on
	0	ei
DA (MAD saatavilla)	1	on
	0	sektori 0 ei sisällä MAD koodia

4.1.5 Luku-avain A

Avain A sektorilla 0 tulee olla julkinen ja asetettu seuraavaksi heksa koodiksi:

tavu 5					tavu 0
a5	a4	a3	A2	a1	a0

4.1.6 Kirjoitusavain B

Avain B sektorilla 0 on ohjelmoitu kortinantajan toimesta ja tulee pitää salassa.

4.2 Sovellushakemistojen koodaus

4.2.1 MAD versio numero

Standardi esittelee versiot 1, 2 ja 3.

MAD1 ja MAD2 versio numerot on koodattu yleistavuun (GPB).

MAD3 versio numero on koodattu erillisessä dokumentissa.

4.2.2 MAD tyypit

Standardi sallii 3 MAD tyyppiä

- yksisovellus kortti ilman hakemistomääreitä
- yksisovelluskortti hakemusmääreillä
- monisovelluskortti hakemusmääreillä

MAD tyyppi on koodattu yleistavuun (GPB).

4.2.3 Toiminnallisuusryhmä

Toiminnallisuusryhmä koodi mahdollistaa sovellusten luokittelun. Uutta sovellus ID:tä hakevat yrityksen voivat ehdottaa koodia olemassa olevalta listalta. Jos tieto puuttuu rekisteröijä määrittää koodin.

4.2.4 Ohjauskoodit

Toiminnallisuusryhmäkoodi 00 hex ilmoittaa tietyn ohjauskoodia vastaavalle sektorille:

00 00 hex	sektori on vapaa
00 01 hex	sektori on vioittunut, esim. avaimet on tuhottu tai ei ole tiedossa
00 02 hex	sektori on varattu
00 03 hex	sektori sisältää täydentävää hakemisto tietoa (käyttökelpoinen vain tulevilla korteissa)
00 04 hex	sektori sisältää kortin lukija infoa ASCII formaatissa.
00 05 hex	sektori ei ole käyttökelpoinen (yli muistin koon)

4.2.5 Kortin lukija informaatio

Ohjauskoodit 0x00 0x04 viittaa yleiseen kortin lukija tietoon vastaavalla sektorilla. Tähän ei ole sitovia sääntöjä, mutta seuraavat suositukset on annettu kortin lukija tiedon tallennusta varten.

byte n 00	byte n-1 last character	...	Byte 1 Character 1	Byte 0 Type length <n>
--------------	----------------------------	-----	-----------------------	---------------------------