SPECIFIKATION	

CARELINK – TELIASONERA

MIFARE SPECIFIKATION / MAGNETKODNING

	Namn, Organisation	Datum	
Skriven av	Bertil Adolfsson, Setec TAG AB Mia Ramström, Setec TAG AB	2007-02-09	
Godkänd av			

SETEC TAG
A Gemalto Company

SPECIFIKATION	

VERSIONS HANTERING

DATUM	ÄNDRAD DEL (Sektion & sida)	Nytt versions nummer	Ändring Typ av ändring oc beskrivning
2007-02-09	Hela	1.0	Skapande av dokument
2007-03-02		1.1	Ändring av vad som ska kodas och var
2007-04-02		1.2	Ändring av vilka tecken ska kodas Komplettering av magnetrandskodning
2007-06-27		1.3	Förklaring av version i sektorn för kortnr Uppdelning av binära kortnumret i 2x 32 bit
2007-10-30		1.4	Appendix för kodning och förtydligande av kodningstyper
2007-11-16		1.5	Korrigering av kodnings-beskrivning.

SETEC TAG
A Gemalto Company

SPECIFIKATION	

INNEHÅLL

SETEC TAG
A Gemalto Company

SPECIFIKATION	

1. BESKRIVNING

1.1 APPLIKATION

Ett SIS kort är en godkänd id-handling som är giltig på post och bank. På kortet finns också ett elektroniskt id som verifierar personens identitet på offentliga webbsidor eller interna applikationer. Denna specifikation beskriver om hur man även kan personalisera kortets beröringsfria Mifare-del för att på ett flexibelt sätt kunna använda detta kort i inpassage till fastigheten.

1.2 REFERENS

HSA-identitet är hämtad ur specifikationen HSA-Specifikation, Slutlig utgåva, Version 1.0 daterad 2000-02-21. Samt kompletterande information från Carelinks support på AU-System, 2007-02-19.

1.3 FORMATERING AV MIFARE

Det finns olika typer av Mifare-kort och det som används i de flesta SIS-kort har minnesstorleken 4Kbyte. Den första delen av ett 4Kbyte har samma formatering som ett Mifare 1Kbyte d.v.s.

Typ av kort	Sektor 0-15	Sektor 16-31	Sektor 32-39
Mifare 1Kbyte	4 block per sektor	--	--
Mifare 4Kbyte	4 block per sektor	4 block per sektor	16 block per sektor

Varje block består av 16 tecken.

1.4 FORMATERING AV DATA

Se även Appendix I.

Normalt läser passagesystemet ett kort och översätter det i system- respektive kortnummer. Olika system har olika förutsättningar men genom att skriva informationen i olika format så kan respektive tillverkare läsa den del som är enklast för dem. Eftersom ett Mifare block endast består av 16 tecken så har informationen gällande kortnummer trunkerats så att det får plats i ett block.

KORTNUMMER

Block 0 – Systemnummer + Kortnummer, (ASCII, 16 tecken)
Block 1 – Systemnummer + Kortnummer, (systemnr-32 bitar | kortnr-32 bitar)
Block 2 –

Exempel på kortnummer:
975200001230000001(C)hecksiffra Trunkerat

Block nr	Data	Beskrivning
0	2000012300000017	Systemnummer + kortnummer, ASCII, 16 tecken
1	0131 2D7B 0000 0011	Systemnummer + kortnummer, DWORD + DWORD
2		

$0131\ 2D7B_{16}$ = 20000123_{10}
$0000\ 0011_{16}$ = 17_{10}

SPECIFIKATION	

HSA-ID

Block 0 – HSA-id Global del, (ASCII, 16 tecken)
Block 1 – HSA-id Lokal del , (ASCII, upp till 16 tecken)
Block 2 - HSA-id Lokal del (Ledigt)

Exempel på HSA-id:
SE165500001234-12345678901

Block nr	Data	Beskrivning
0	SE165500001234	HSA-id Global del, ASCII, 16 tecken
1	12345678901	HSA-id Lokal del, ASCII, upp till 16 tecken
2		HSA-id Lokal del fortsättning vid behov, ASCII, upp till 16 tecken

SETEC TAG
A Gemalto Company

SPECIFIKATION	

2. MIFARE PERSONALISERING

2.1 DATA

Sektor 0 – MAD 1 används

Block Nummer	*B0*	*B1*	*B2*	*B3*	*B4*	*B5*	*B6*	*B7*	*B8*	*B9*	*B10*	*B11*	*B12*	*B13*	*B14*	*B15*
Block 0	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX
Block 1	**CRC**	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX
Block 2	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX	**0C**	**0A**	**0C**	**0A**
Block 3	*KEY A =A0 A1 A2 A3 A4 A5*						**78**	**77**	**88**	**C1**	*KEY B=?? ?? ?? ?? ?? ??*					

Sektor 14

Block Nummer	*B0*	*B1*	*B2*	*B3*	*B4*	*B5*	*B6*	*B7*	*B8*	*B9*	*B10*	*B11*	*B12*	*B13*	*B14*	*B15*
Block 0	2	0	0	0	0	1	2	3	0	0	0	0	0	0	1	7
Block 1	01	31	2D	7B	00	00	00	11								
Block 2	1	.	0	K	N	R										
Block 3	*KEY A*						**07**	**8F**	**0F**	**69**	*KEY B*					

Sektor 15

Block Nummer	*B0*	*B1*	*B2*	*B3*	*B4*	*B5*	*B6*	*B7*	*B8*	*B9*	*B10*	*B11*	*B12*	*B13*	*B14*	*B15*
Block 0	S	E	1	6	5	5	0	0	0	0	1	2	3	4	-	
Block 1	1	2	3	4	5	6	7	8	9	0	1					
Block 2																
Block 3	*KEY A*						**07**	**8F**	**0F**	**69**	*KEY B*					

: To be personalised upon customer request. XX means undefined
: Personalised
: Sector Access Condition
: General Purpose Byte

Användning av sektorer

Sektor nr	*0*	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*	*12*	*13*	*14*	*15*
Block 0	**MAD1**	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX
Sektor nr	*16*	*17*	*18*	*19*	*20*	*21*	*22*	*23*	*24*	*25*	*26*	*27*	*28*	*29*	*30*	*31*
Block 0	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX
Sektor nr	*32*	*33*	*34*	*35*	*36*	*37*	*38*	*39*								
Block 0	XX	XX	XX	XX	XX	XX	XX	XX								

Sektor 0 Mad information
Sektor 14 Kortnummer information
Sektor 15 HSA information

2.1 ACCESS VILLKOR

Avslutande block Sektor 14 & 15

C1XY	C2XY	C3XY	read	write	incr	decr, transfer, restore
0	0	0	keyA|B[1]	key A|B[1]	key A|B[1]	key A|B[1]
0	**1**	**0**	**keyA|B[1]**	**never**	**never**	**never**
1	0	0	keyA|B[1]	key B[1]	never	never
1	1	0	keyA|B[1]	key B[1]	key B[1]	key A|B[1]
0	0	1	keyA|B[1]	never	never	key A|B[1]
0	1	1	Key B[1]	key B[1]	never	never
1	0	1	Key B[1]	never	never	never
1	1	1	never	never	never	never

			KEYSECXA		ACCESS COND.		KEYSECXB	
C1X3	C2X3	C3X3	read	Write	read	write	Read	Write
0	0	0	never	key A	key A	never	key A[1]	key A
0	1	0	never	Never	key A	never	key A[1]	Never
1	0	0	never	key B	key A|B	never	Never	key B
1	**1**	**0**	**never**	**Never**	**key A|B**	**never**	**Never**	**Never**
0	0	1	never	key A	key A	key A	key A[1]	key A
0	1	1	never	key B	key A|B	key B	Never	key B
1	0	1	never	Never	key A|B	key B	Never	never
1	1	1	never	Never	key A|B	never	Never	never

2.3 TRANSPORT NYCKLAR

Sektor 0 kommer att låsas så att endast godkänd leverantör får ändra i MAD.

KEY A	:	*A0 A1 A2 A3 A4 A5*	Läs-rättigheter
KEY B	:	*xx xx xx xx xx xx*	Skriv-rättigheter (Ej officellt)

Sektor 14 & 15 som innehåller informationen med kortnummer och HSA-ID kommer att låsas

KEY A	:	*HEMLIG NYCKEL – ÄGS AV CARELINK*
KEY B	:	-- -- -- -- -- --

Alla sektorer kommer att vara orörda med standard access vilkor och nycklar

KEY A	:	Standard nyckel *FF FF FF FF FF FF*
KEY B	:	Standard nyckel *FF FF FF FF FF FF*

2.4 AID CARELINK

Carelink kommer att registrera sig för att erhålla en AID från NXP (www.nxp.com) för att kunna flytta applikationen på valfri sektor. Specifikationen beskriver att informationen läggs på en sektor med 4 block men skulle likaväl läggas på en sektor med 16 block. I detta fall så kommer MAD2 att användas.

Carelink har fått följande AID tilldelad: A00C

A00C - health services Carelink AB Carelink AB Sweden 3 30.06.2007 Health services Carelink AB

3. MAGNETRANDEN

3.1 KODNING AV MAGNETRAND

Magnetrandens spår 2 kommer att kodas med motsvarande information som återfinns i Mifare sektor 14 block 0, d.v.s. kortnumret.

För de olika korten innebär detta:

SIS-kortet

16 siffror av kortnumret läggs in. De tre först i kortnumret kodas ej. (975)
(2 2583 357 XXXX XXXX)

2583 = Utfärdarnummer = Vilket Landsting kortet tillhör
357= SIS Företagskort med chip & kontaktlöst chip

Reservkortet

16 siffror av kortnumret läggs in. De tre först i kortnumret kodas ej. (975)
(2 2583 957 XXXX XXXX)

2583 = Utfärdarnummer = Vilket Landsting kortet tillhör eller 0000, Landstinget har inget utfärdarnummer.
957= Grått kort med chip & kontaktlöst chip

"Det tredje kortet"

16 siffror av kortnumret läggs in. De tre först i kortnumret kodas ej. (975)
(2 0000 857 XXXX XXXX)

0000, Landstinget har inget utfärdarnummer eller 2583 = Utfärdarnummer = Vilket Landsting kortet tillhör
857= Grått kort med chip & kontaktlöst chip

4. ELEKTRISKT TEST

4.1 ON LINE TEST (UNDER PERSONALISERING)

- Läsning av serienummer
- Kontroll av access villkor
- Kodning av kortnummer och HSA-ID samt låsning av sektor
- Skrivning i MAD för att registrera applikationen

APPENDIX

I. KODNINGSSPECIFIKATION

Exemplen på kodning nedan utgår från ovanstående kort. HSA-id för certifikaten på kortet är ”SE196310262628-1”.

Block 0 Sektor 14

Kodat i sektorn finns de 16 sista tecknen i kortnumret, i testkortets fall är kortnumret 628083 5254 01105970 2. De tre första tecknen trunkeras bort, övriga ASCII-kodas och skrivs på blocket.

```
Block0Sector14 = 30 38 33 35 32 35 34 30 31 31 30 35 39 37 30 32
ASCIIDecode(Block0Sector14) = 0835254011059702
```

Block 1 Sektor 14

Kodat i sektorn finns samma information som i block 0, här representeras den dock som två binära integers.

```
Block1Sector14 = 00 7F 73 1C 00 A8 C1 F6 00 00 00 00 00 00 00 00
SystemNo = Int32(00 7F 73 1C)
CardNo = Int32(00 A8 C1 F6)
SystemNo + CardNo = 0835254011059702
```

Block 0 Sektor 15
Kodat i sektorn finns globalt HSA-id kodat som ASCII. Om HSA-id inte tar upp 16 bytes på sektorn nullternineras strängen med 0x00.

```
Block1Sector15 = 53 45 31 39 36 33 31 30 32 36 32 36 32 38 00 00
ASCIIDecode(Block0Sector15) = SE196310262628\0
```

Block 1 Sektor 15
Kodat i sektorn finns lokalt HSA-id kodat som ASCII. Om HSA-id inte tar upp 16 bytes på sektorn nullternineras strängen med 0x00.

```
Block1Sector15 = 31 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
ASCIIDecode(Block1Sector15) = 1\0
```

END OF DOCUMENTATION