Handling Mifare Classic with BlueBox Show

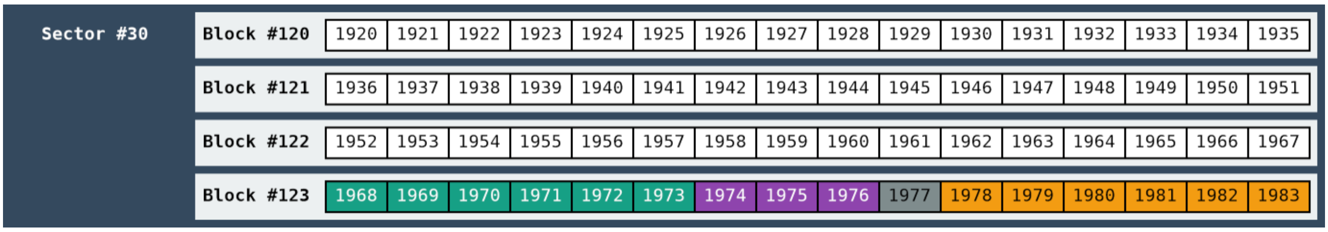
1 Memory Layout of a Mifare Classic

1.1 General Overview

There are 3 types of Mifare Classic:

- S20: 320 Bytes, organized in 5 sectors with 4 blocks of 16 Bytes each
- S50: 1024 Bytes, organized in 16 sectors with 4 blocks of 16 Bytes each
- S70: 4096 Bytes, organized in 32 sectors with 4 blocks of 16 Bytes each and, 8 sectors with 16 blocks

Example: Sector #30



Sector #30	Block #120	1920	1921	1922	1923	1924	1925	1926	1927	1928	1929	1930	1931	1932	1933	1934	1935
	Block #121	1936	1937	1938	1939	1940	1941	1942	1943	1944	1945	1946	1947	1948	1949	1950	1951
	Block #122	1952	1953	1954	1955	1956	1957	1958	1959	1960	1961	1962	1963	1964	1965	1966	1967
	Block #123	1968	1969	1970	1971	1972	1973	1974	1975	1976	1977	1978	1979	1980	1981	1982	1983

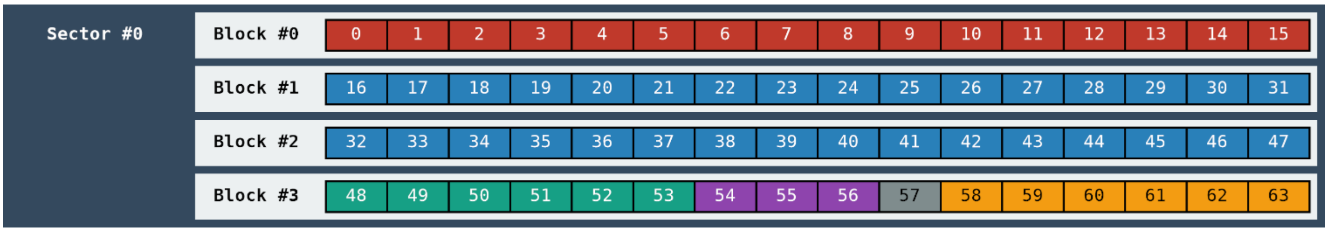
The first three blocks in this sector (#120, #121, #122) are intended to store data. These are 48 Bytes in 3 Blocks.

The last block in each sector (#123) is intended to store both passwords Key A (turquoise), Key B (orange) and, the access bits (violet). This is also called the trailing sector. The passwords are always active in most configurations. So, to read or write data, you always have to select and send one Key.

The access bits are stored in 3 Bytes. The 4th Byte (grey) is not used for this an can be filled with any random value.

Note: you can only read or write a complete memory block of 16 Bytes.

Small difference: Sector #00

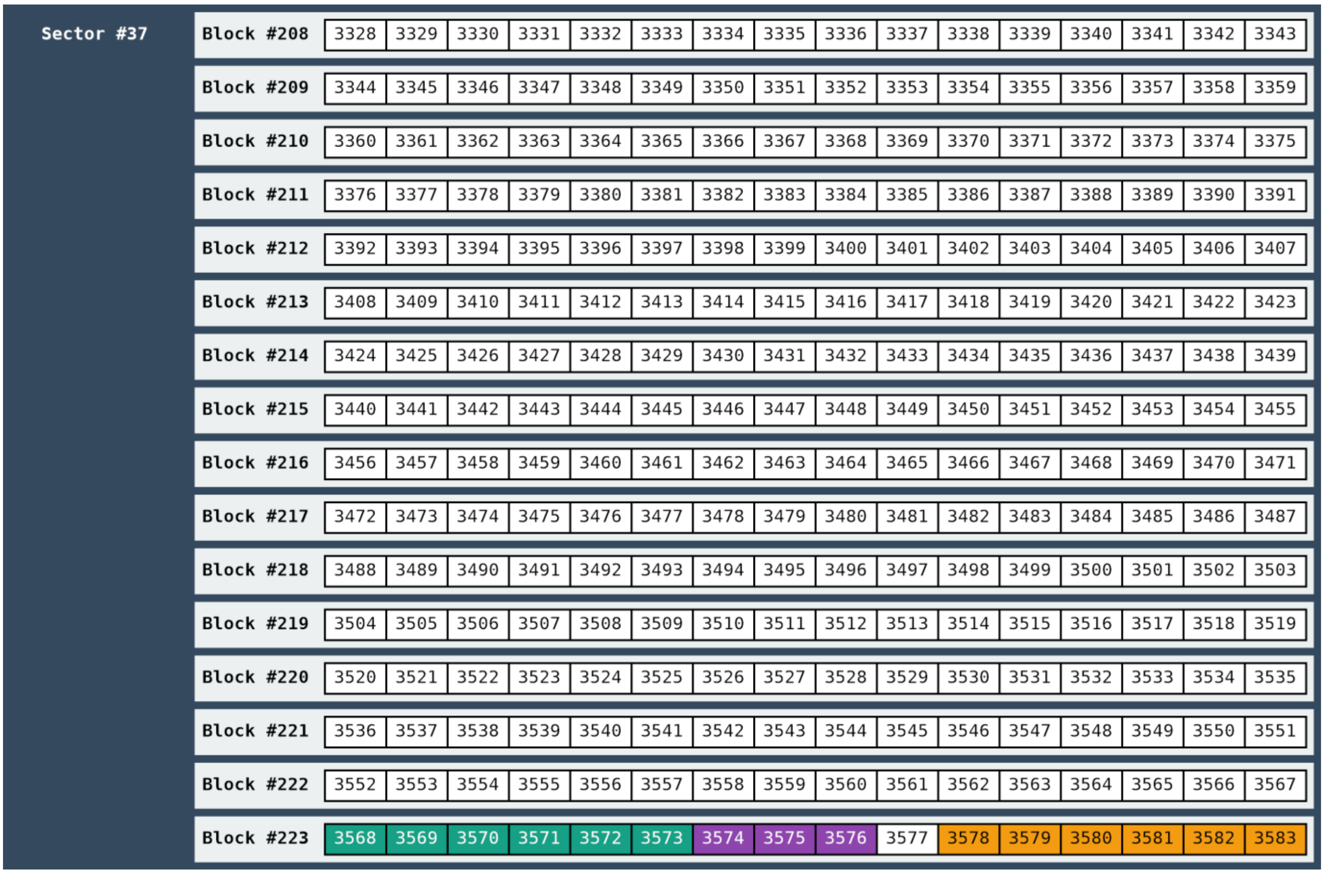


Sector #0	Block #0	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
	Block #1	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	Block #2	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47
	Block #3	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63

In the first sector, the first memory block #0 is preprogrammed by the manufacturer with the UID and configuration information. This contents of this memory block cannot be changed.

Blocks #1 and #2 can be used for a special purpose, the Mifare Application Directory (MAD). But you can also use them as standard memory blocks and store data here.

Example: Sector #37



Sector #37	Block #208	3328	3329	3330	3331	3332	3333	3334	3335	3336	3337	3338	3339	3340	3341	3342	3343
	Block #209	3344	3345	3346	3347	3348	3349	3350	3351	3352	3353	3354	3355	3356	3357	3358	3359
	Block #210	3360	3361	3362	3363	3364	3365	3366	3367	3368	3369	3370	3371	3372	3373	3374	3375
	Block #211	3376	3377	3378	3379	3380	3381	3382	3383	3384	3385	3386	3387	3388	3389	3390	3391
	Block #212	3392	3393	3394	3395	3396	3397	3398	3399	3400	3401	3402	3403	3404	3405	3406	3407
	Block #213	3408	3409	3410	3411	3412	3413	3414	3415	3416	3417	3418	3419	3420	3421	3422	3423
	Block #214	3424	3425	3426	3427	3428	3429	3430	3431	3432	3433	3434	3435	3436	3437	3438	3439
	Block #215	3440	3441	3442	3443	3444	3445	3446	3447	3448	3449	3450	3451	3452	3453	3454	3455
	Block #216	3456	3457	3458	3459	3460	3461	3462	3463	3464	3465	3466	3467	3468	3469	3470	3471
	Block #217	3472	3473	3474	3475	3476	3477	3478	3479	3480	3481	3482	3483	3484	3485	3486	3487
	Block #218	3488	3489	3490	3491	3492	3493	3494	3495	3496	3497	3498	3499	3500	3501	3502	3503
	Block #219	3504	3505	3506	3507	3508	3509	3510	3511	3512	3513	3514	3515	3516	3517	3518	3519
	Block #220	3520	3521	3522	3523	3524	3525	3526	3527	3528	3529	3530	3531	3532	3533	3534	3535
	Block #221	3536	3537	3538	3539	3540	3541	3542	3543	3544	3545	3546	3547	3548	3549	3550	3551
	Block #222	3552	3553	3554	3555	3556	3557	3558	3559	3560	3561	3562	3563	3564	3565	3566	3567
	Block #223	3568	3569	3570	3571	3572	3573	3574	3575	3576	3577	3578	3579	3580	3581	3582	3583

1.2 Password Protection

There are no special commands to configure the read/write passwords. The last block of every sector contains Key A (6 bytes), the access control bits (4 bytes) and Key B (6 bytes). To change the Keys from the factory preset, simply write the complete last block of the sector.

It is intended, that Key B can have higher rights than Key A. Thus, Key A can only have the right to read out a memory block, while Key B may also write to this memory block.

Since the subject is arbitrarily complicated and unmanageable by hand, you can use this dynamic view to play through possibilities:

http://calc.gmss.ru/Mifare1k/

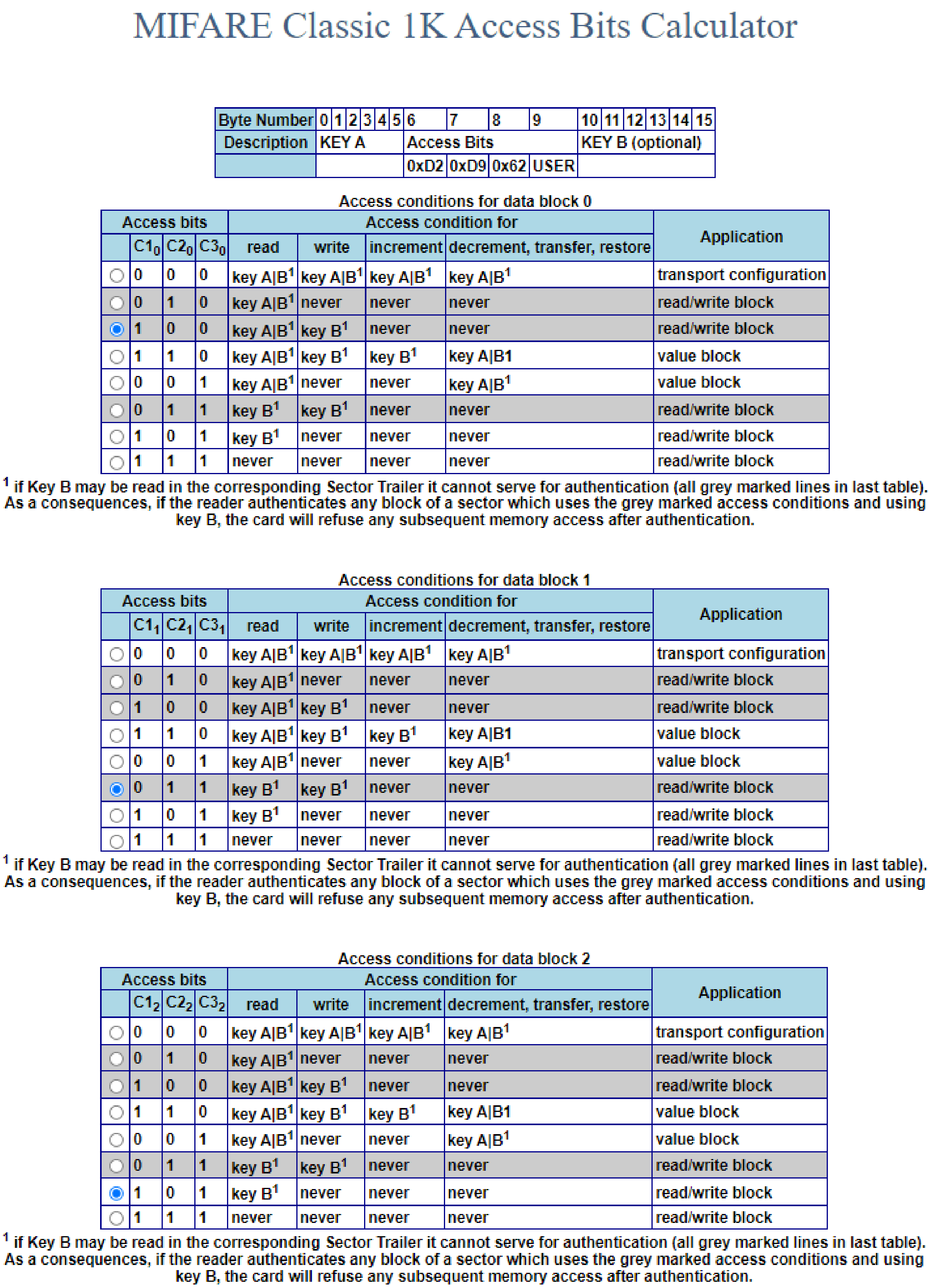
Example Settings of the Access Bits

In the following example, Key A is allowed to read the 1st block in the sector, but not to change it. Only Key B is allowed to do this.

In the 2nd block, only Key B is allowed to read or write. Key A is not allowed to do anything.

In the 3rd block, Key B is only allowed to read. Key A is not allowed to do anything.

In the 4th block, Key B may overwrite, but not read. Only the access bytes can be read by both keys, but they can no longer be changed.



MIFARE Classic 1K Access Bits Calculator

Byte Number	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Description	KEY A						Access Bits				KEY B (optional)					
							0xD2	0xD9	0x62	USER						

Access conditions for data block 0

	Access bits			Access condition for				Application
	$C1_0$	$C2_0$	$C3_0$	read	write	increment	decrement, transfer, restore	
○	0	0	0	key A|B[1]	key A|B[1]	key A|B[1]	key A|B[1]	transport configuration
○	0	1	0	key A|B[1]	never	never	never	read/write block
●	1	0	0	key A|B[1]	key B[1]	never	never	read/write block
○	1	1	0	key A|B[1]	key B[1]	key B[1]	key A|B1	value block
○	0	0	1	key A|B[1]	never	never	key A|B[1]	value block
○	0	1	1	key B[1]	key B[1]	never	never	read/write block
○	1	0	1	key B[1]	never	never	never	read/write block
○	1	1	1	never	never	never	never	read/write block

[1] if Key B may be read in the corresponding Sector Trailer it cannot serve for authentication (all grey marked lines in last table). As a consequences, if the reader authenticates any block of a sector which uses the grey marked access conditions and using key B, the card will refuse any subsequent memory access after authentication.

Access conditions for data block 1

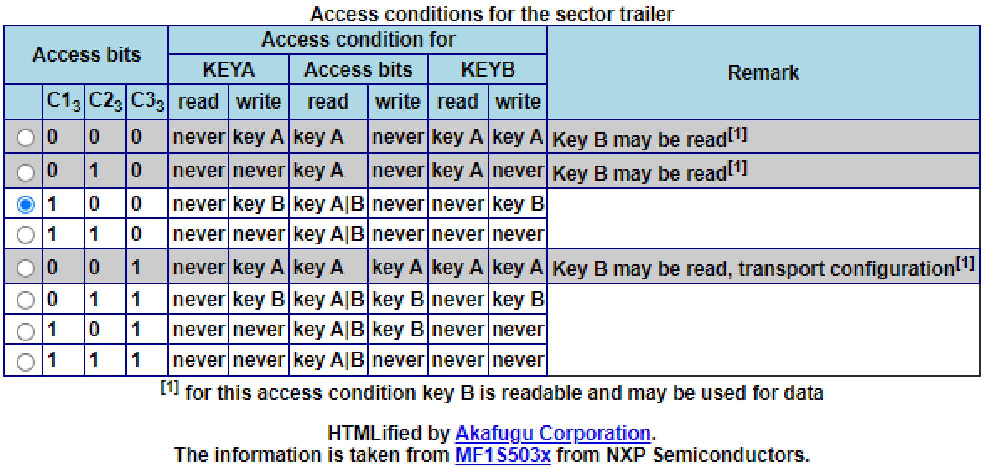
	Access bits			Access condition for				Application
	$C1_1$	$C2_1$	$C3_1$	read	write	increment	decrement, transfer, restore	
○	0	0	0	key A|B[1]	key A|B[1]	key A|B[1]	key A|B[1]	transport configuration
○	0	1	0	key A|B[1]	never	never	never	read/write block
○	1	0	0	key A|B[1]	key B[1]	never	never	read/write block
○	1	1	0	key A|B[1]	key B[1]	key B[1]	key A|B1	value block
○	0	0	1	key A|B[1]	never	never	key A|B[1]	value block
●	0	1	1	key B[1]	key B[1]	never	never	read/write block
○	1	0	1	key B[1]	never	never	never	read/write block
○	1	1	1	never	never	never	never	read/write block

[1] if Key B may be read in the corresponding Sector Trailer it cannot serve for authentication (all grey marked lines in last table). As a consequences, if the reader authenticates any block of a sector which uses the grey marked access conditions and using key B, the card will refuse any subsequent memory access after authentication.

Access conditions for data block 2

	Access bits			Access condition for				Application
	$C1_2$	$C2_2$	$C3_2$	read	write	increment	decrement, transfer, restore	
○	0	0	0	key A|B[1]	key A|B[1]	key A|B[1]	key A|B[1]	transport configuration
○	0	1	0	key A|B[1]	never	never	never	read/write block
○	1	0	0	key A|B[1]	key B[1]	never	never	read/write block
○	1	1	0	key A|B[1]	key B[1]	key B[1]	key A|B1	value block
○	0	0	1	key A|B[1]	never	never	key A|B[1]	value block
○	0	1	1	key B[1]	key B[1]	never	never	read/write block
●	1	0	1	key B[1]	never	never	never	read/write block
○	1	1	1	never	never	never	never	read/write block

[1] if Key B may be read in the corresponding Sector Trailer it cannot serve for authentication (all grey marked lines in last table). As a consequences, if the reader authenticates any block of a sector which uses the grey marked access conditions and using key B, the card will refuse any subsequent memory access after authentication.



Access conditions for the sector trailer

Access bits				Access condition for						Remark
				KEYA		Access bits		KEYB		
	$C1_3$	$C2_3$	$C3_3$	read	write	read	write	read	write	
○	0	0	0	never	key A	key A	never	key A	key A	Key B may be read[1]
○	0	1	0	never	never	key A	never	key A	never	Key B may be read[1]
●	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	key A	Key B may be read, transport configuration[1]
○	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	

[1] for this access condition key B is readable and may be used for data

HTMLified by Akafugu Corporation.
The information is taken from MF1S503x from NXP Semiconductors.

Example: Composing the Trailing Sector

Key A:	A1 A2 A3 A4 A5 A6
Access bits:	D2 D9 62 00
Key B:	B1 B2 B3 B4 B5 B6

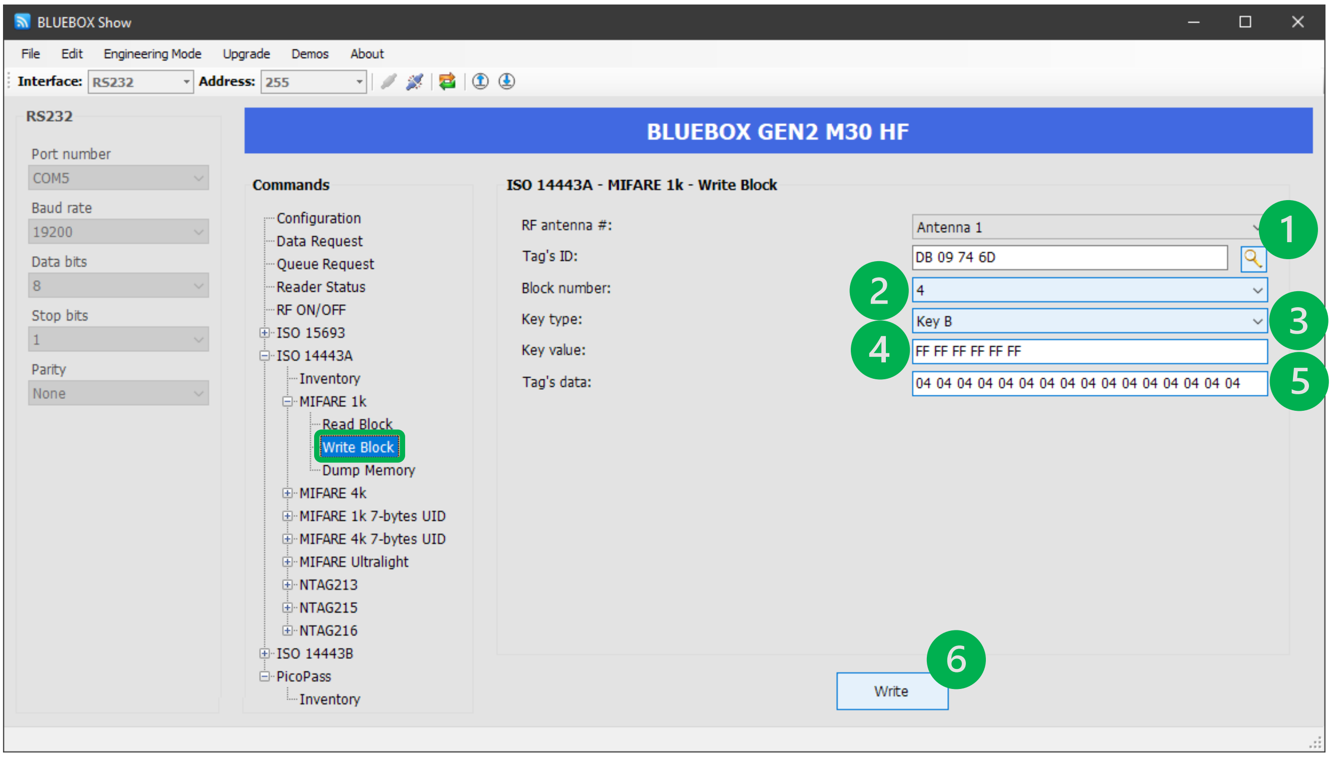
So, you have to write this data into the trailing block:

A1 A2 A3 A4 A5 A6 D2 D9 62 00 B1 B2 B3 B4 B5 B6

2 Using Bluebox Show

2.1 Write Data onto a Mifare Classic with Bluebox Show

In this example we want to write the 16 Bytes of block number 4.



Interface: RS232 Address: 255

RS232

Port number: COM5

Baud rate: 19200

Data bits: 8

Stop bits: 1

Parity: None

BLUEBOX GEN2 M30 HF

ISO 14443A - MIFARE 1k - Write Block

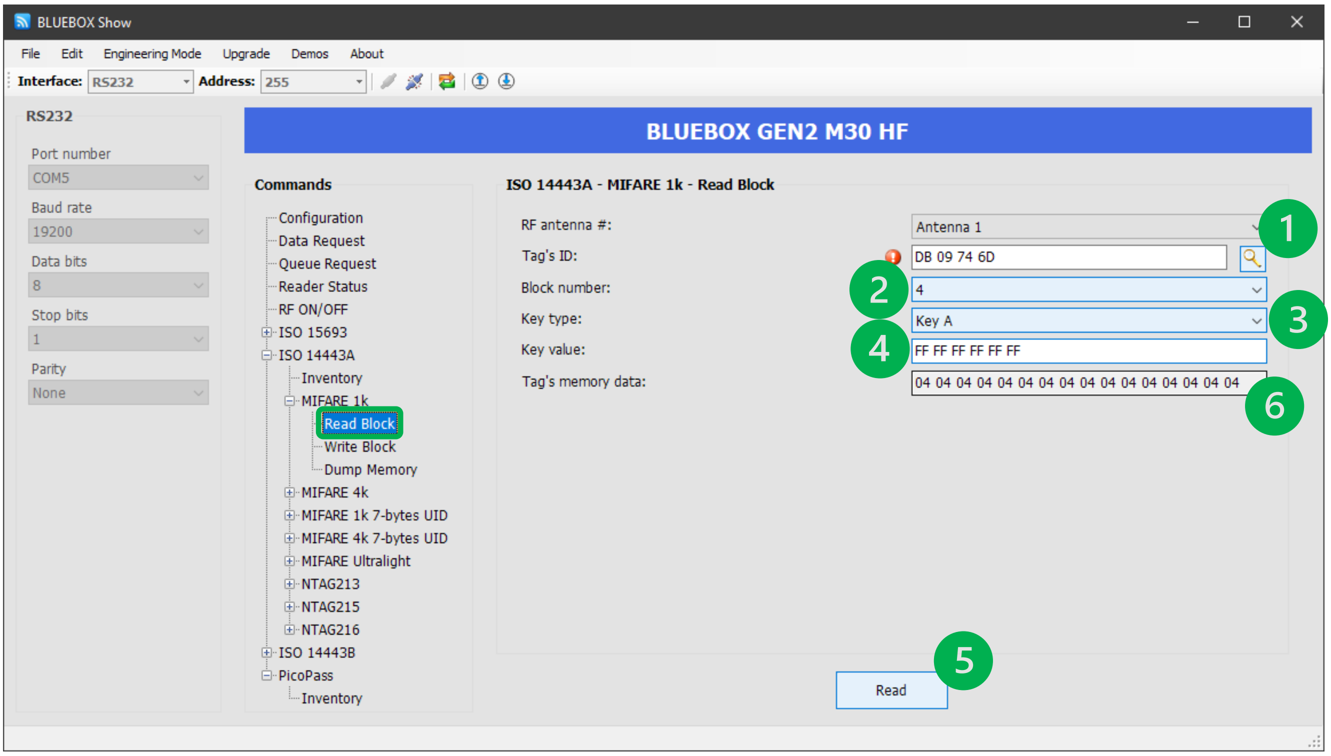
1. RF antenna #: Antenna 1

Tag's ID: DB 09 74 6D

2. Block number: 4
3. Key type: Key B
4. Key value: FF FF FF FF FF FF
5. Tag's data: 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04
6. Write

1: Use the Magnifying Glass to do an inventory to find RFID tags. If only one tag is in the antenna field, it is shown directly as in the example above.
2: Chose the target block number. In the example this is block number 4, which is the first block of the second sector on the RFID tag.
3: Select Key B. If the RFID tag is new, you can choose any key you like.
4: Type in the needed Key value. If the RFID tag is new, the factory pre-set value is already in the input field.
5: Type in the 16 Bytes of the block data to be written.
6: Click on [Write] to store the data onto the RFID tag.

2.2 Read Data from a Mifare Classic with Bluebox Show



Interface: RS232 Address: 255

Port number: COM5
Baud rate: 19200
Data bits: 8
Stop bits: 1
Parity: None

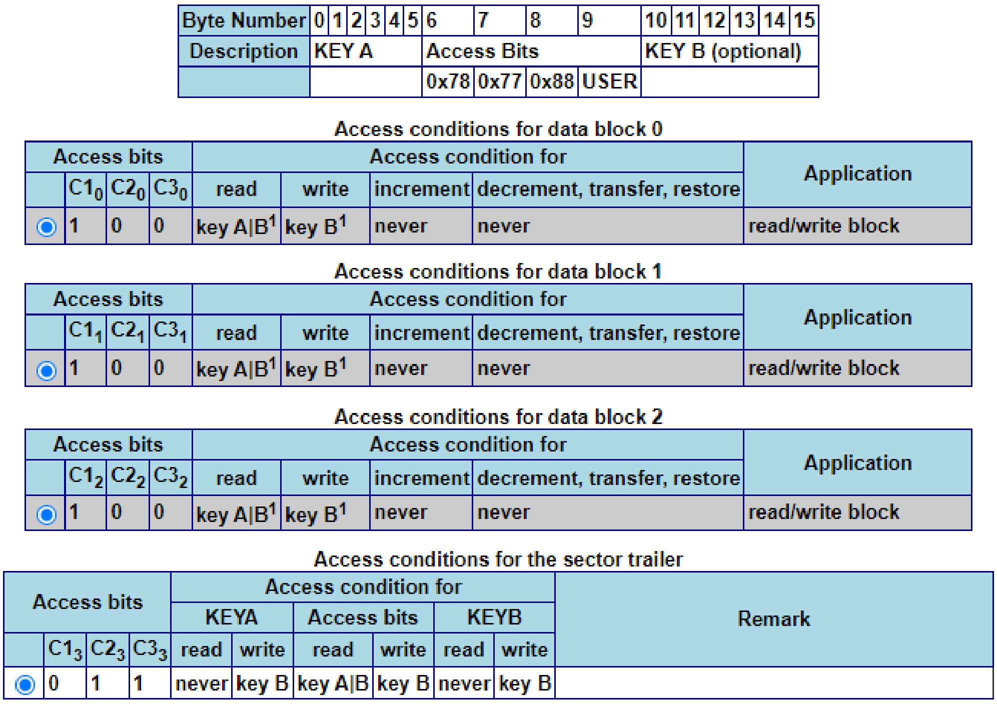
RF antenna #: Antenna 1
Tag's ID: DB 09 74 6D
Block number: 4
Key type: Key A
Key value: FF FF FF FF FF FF
Tag's memory data: 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04

1: Use the Magnifying Glass to do an inventory to find RFID tags. If only one tag is in the antenna field, it is shown directly as in the example above.
2: Chose the target block number. In the example this is block number 4, which is the first block of the second sector on the RFID tag.
3: Select Key A. If the RFID tag is new, you can choose any key you like.
4: Type in the needed Key value. If the RFID tag is new, the factory pre-set value is already in the input field.
5: Click on [Read] to read the data from the RFID tag.
6: Now the 16 Bytes of the block data are shown in this line.

2.3 Set Password Protection

Here we want to have full access with Key B, read-only access with Key A in every block of the sector.

Using the online calculator gives the value 0x78 77 88 for the access bits.
http://calc.gmss.ru/Mifare1k/



Byte Number	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Description	KEY A						Access Bits				KEY B (optional)					
							0x78	0x77	0x88	USER						

Access conditions for data block 0

Access bits				Access condition for				Application
	$C1_0$	$C2_0$	$C3_0$	read	write	increment	decrement, transfer, restore	
●	1	0	0	key A|B[1]	key B[1]	never	never	read/write block

Access conditions for data block 1

Access bits				Access condition for				Application
	$C1_1$	$C2_1$	$C3_1$	read	write	increment	decrement, transfer, restore	
●	1	0	0	key A|B[1]	key B[1]	never	never	read/write block

Access conditions for data block 2

Access bits				Access condition for				Application
	$C1_2$	$C2_2$	$C3_2$	read	write	increment	decrement, transfer, restore	
●	1	0	0	key A|B[1]	key B[1]	never	never	read/write block

Access conditions for the sector trailer

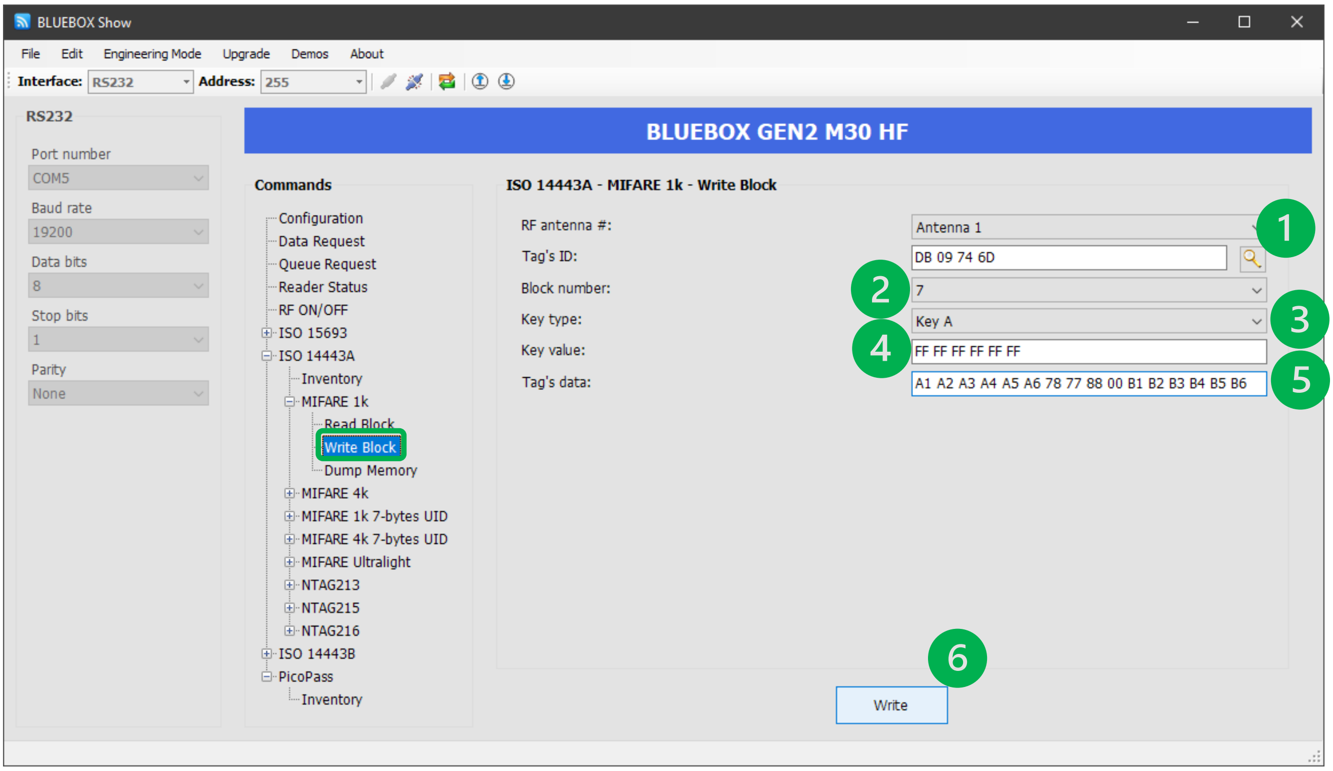
Access bits				Access condition for						Remark
				KEYA		Access bits		KEYB		
	$C1_3$	$C2_3$	$C3_3$	read	write	read	write	read	write	
●	0	1	1	never	key B	key A|B	key B	never	key B	

This picture is edited to show only the chosen configuration for the access bits.

Example: Composing the Trailing Sector

Key A:	A1 A2 A3 A4 A5 A6
Access bits:	78 77 88 00
Key B:	B1 B2 B3 B4 B5 B6

So, you have to write this data into the trailing block: A1 A2 A3 A4 A5 A6 78 77 88 00 B1 B2 B3 B4 B5 B6



Interface: RS232 Address: 255

RS232

Port number: COM5

Baud rate: 19200

Data bits: 8

Stop bits: 1

Parity: None

ISO 14443A - MIFARE 1k - Write Block

RF antenna #: Antenna 1

Tag's ID: DB 09 74 6D

Block number: 7

Key type: Key A

Key value: FF FF FF FF FF FF

Tag's data: A1 A2 A3 A4 A5 A6 78 77 88 00 B1 B2 B3 B4 B5 B6

1: Use the Magnifying Glass to do an inventory to find RFID tags. If only one tag is in the antenna field, it is shown directly as in the example above.

2: Chose the target block number. In the example this is block number 7, which is the trailing sector of the of the second sector on the RFID tag. Writing the trailing sector can change the passwords and access rights.

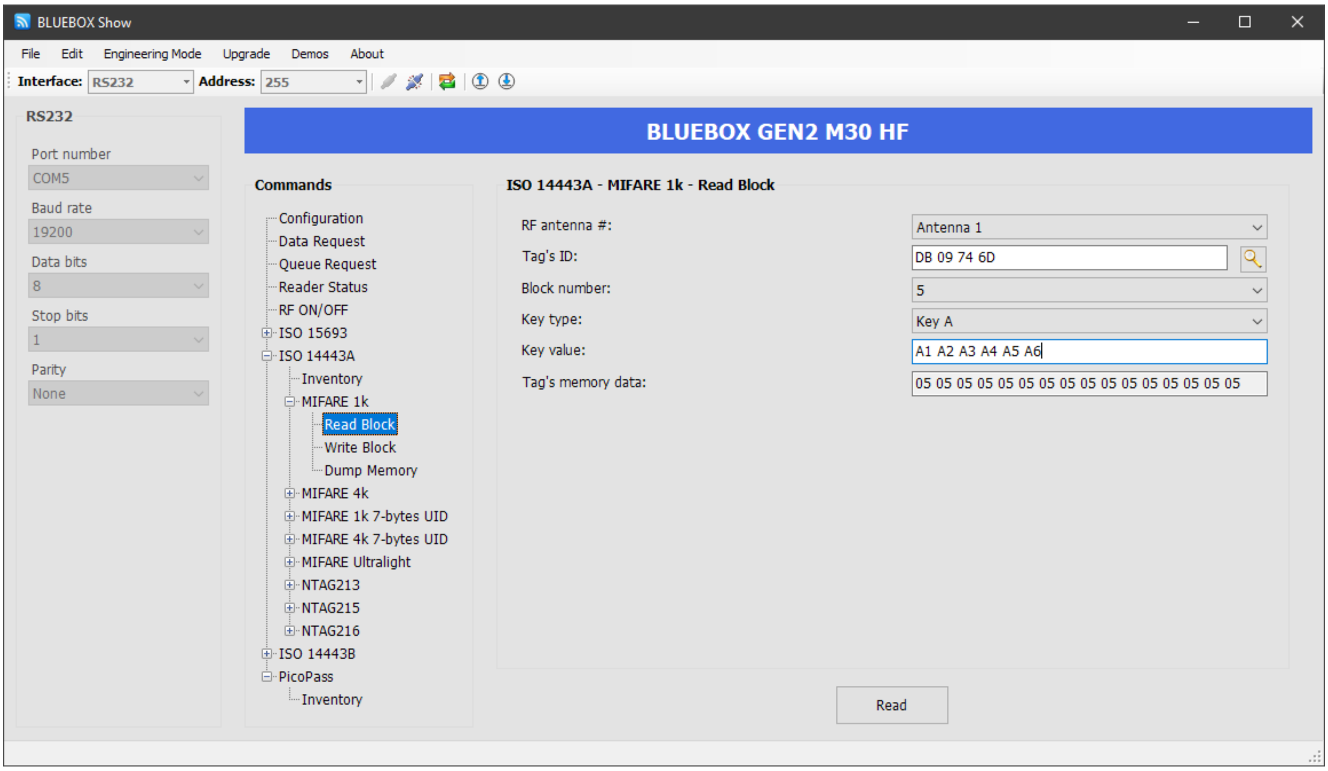
3: Select Key A. This RFID tag is new, so you can choose any key you like.

4: Type in the needed Key value. If the RFID tag is new, the factory pre-set value is already in the input field.

5: Type in the 16 Bytes of the block data to be written.

6: Click on [Write] to store the data onto the RFID tag.

2.4 Read Back using the new Password



Interface: RS232 Address: 255

RS232

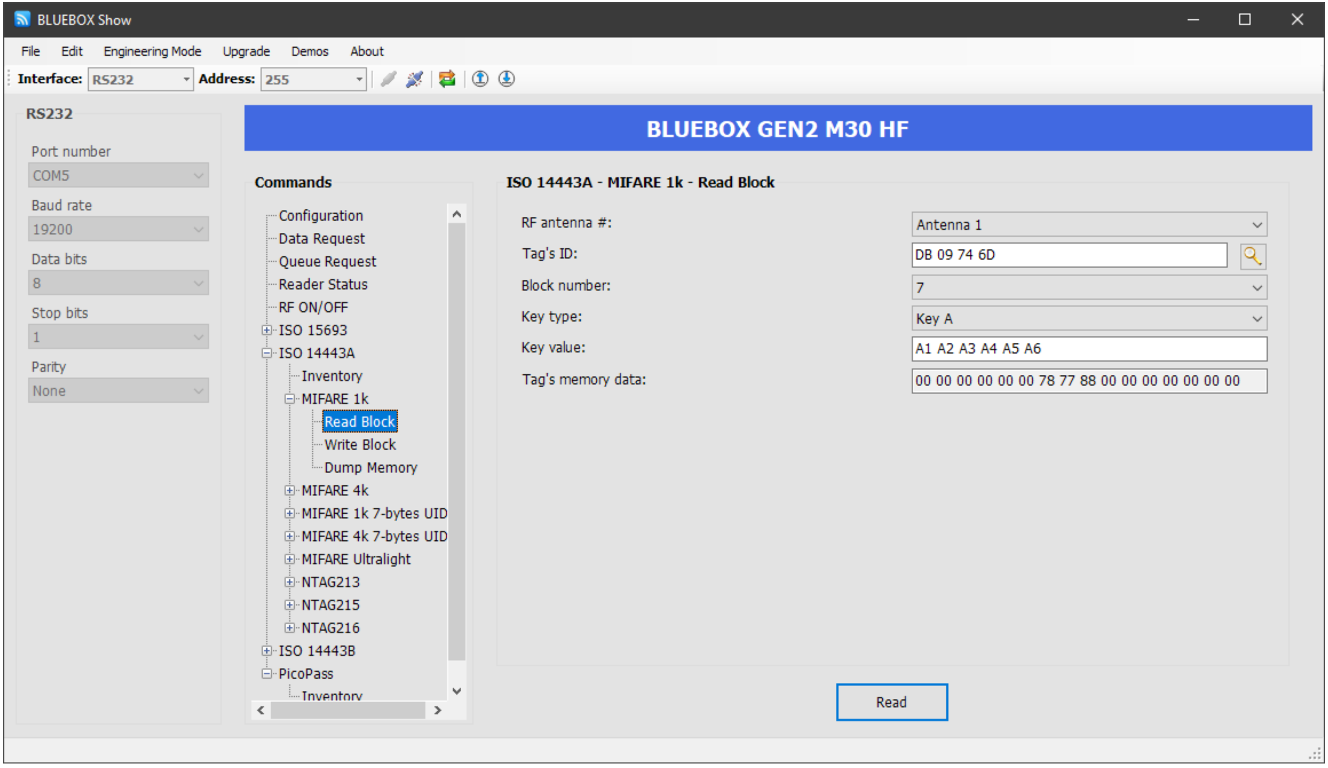
Port number: COM5
Baud rate: 19200
Data bits: 8
Stop bits: 1
Parity: None

ISO 14443A - MIFARE 1k - Read Block

RF antenna #: Antenna 1
Tag's ID: DB 09 74 6D
Block number: 5
Key type: Key A
Key value: A1 A2 A3 A4 A5 A6
Tag's memory data: 05 05 05 05 05 05 05 05 05 05 05 05 05 05 05 05

2.5 Reading the Trailing Sector

You may also want to read the trailing sector. But, both passwords are not shown. This is a security feature.



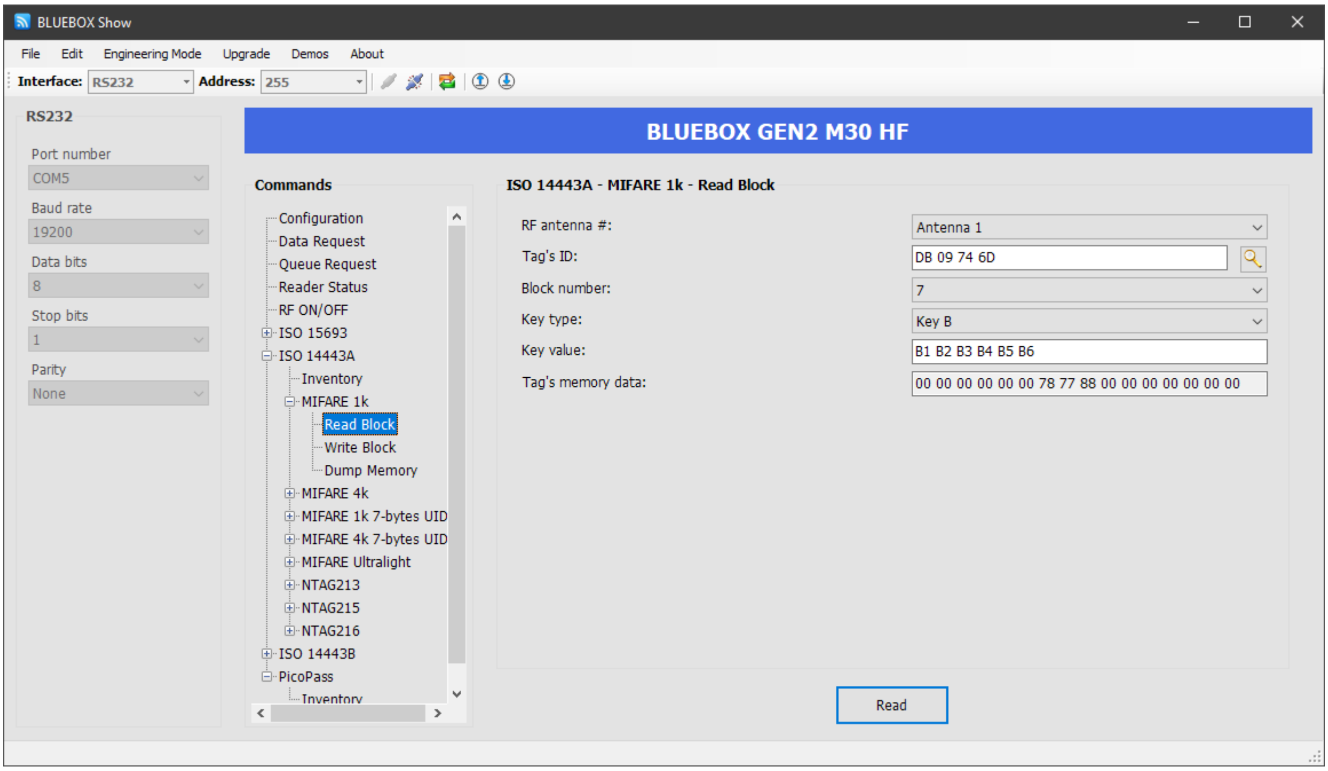
Interface: RS232 Address: 255

RS232

Port number: COM5
Baud rate: 19200
Data bits: 8
Stop bits: 1
Parity: None

ISO 14443A - MIFARE 1k - Read Block

RF antenna #: Antenna 1
Tag's ID: DB 09 74 6D
Block number: 7
Key type: Key A
Key value: A1 A2 A3 A4 A5 A6
Tag's memory data: 00 00 00 00 00 00 78 77 88 00 00 00 00 00 00 00



Interface: RS232 Address: 255

RS232

Port number: COM5

Baud rate: 19200

Data bits: 8

Stop bits: 1

Parity: None

BLUEBOX GEN2 M30 HF

ISO 14443A - MIFARE 1k - Read Block

RF antenna #: Antenna 1

Tag's ID: DB 09 74 6D

Block number: 7

Key type: Key B

Key value: B1 B2 B3 B4 B5 B6

Tag's memory data: 00 00 00 00 00 00 78 77 88 00 00 00 00 00 00 00