AN3002
Application note

Description of the M24LRxx-R and M24LRxxE-R dual interface memory's password protection mechanism

Description

The M24LRxx-R or M24LRxxE-R device is a dual-interface, electrically erasable programmable memory (EEPROM). It features an I^2C interface and can be operated from a V_{CC} power supply. It is also a contactless memory powered by the received electromagnetic carrier wave.

The M24LRxx-R or M24LRxxE-R is organized as 8192 × 8 bits in the I^2C mode and as 2048 × 32 bits in the ISO 15693 and ISO 18000-3 mode 1 RF mode.

Figure 1. M24LRxx block diagram

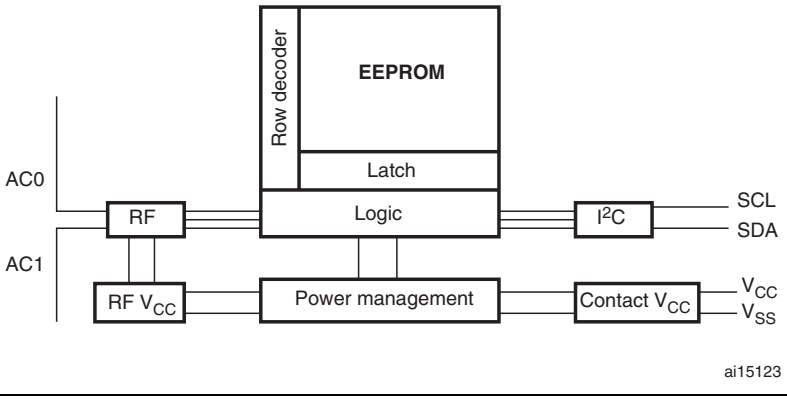


Table 1 lists the products concerned by this application note.

Table 1. Applicable products

Type	Applicable products
Dual interface EEPROMs	M24LRxx-R, M24LRxxE-R

Note: The standard M24LRxx-R and energy-harvesting M24LRxxE-R devices will be referred to as M24LRxx devices throughout the document.

Contents

List of tables

List of figures

1 User memory organization

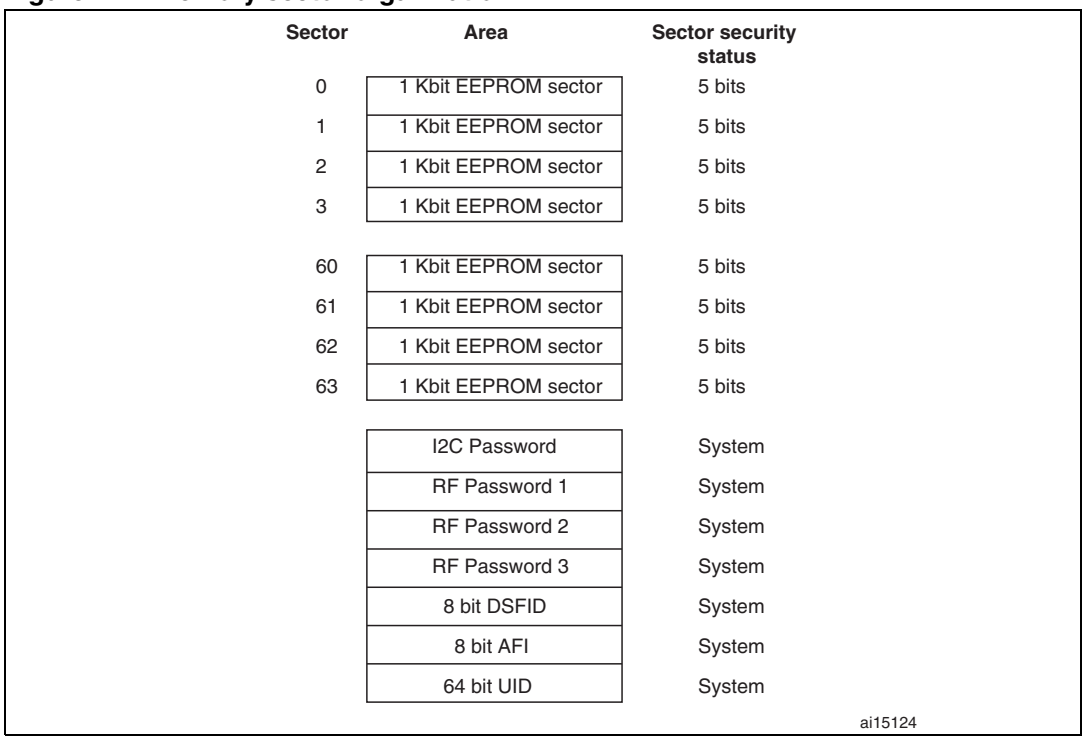
The M24LRxx is divided into 64 sectors of 32 blocks of 32 bits. *Figure 2* shows the memory sector organization. Each sector can be individually read- and/or write-protected using a specific password command. Read and write operations are possible if the addressed data is not in a protected sector.

The M24LRxx also has a 64-bit block that is used to store the 64-bit unique identifier (UID). The UID is compliant with the ISO 15963 description, and its value is used during the anticollision sequence (Inventory). This block is not accessible by the user and its value is written by ST on the production line.

The M24LRxx includes an AFI register that stores the application family identifier, and a DSFID register that stores the data storage family identifier used in the anticollision algorithm.

The M24LRxx has four additional 32-bit blocks that store an I^2C password plus three RF password codes.

Figure 2. Memory sector organization



Sector details

The M24LRxx user memory is divided into 64 sectors. Each sector contains 1024 bits.

In RF mode, a sector provides 32 blocks of 32 bits. Each read / write access is done by block. Read and write block accesses are controlled by a Sector security status byte that defines the access rights to all the 32 blocks contained in the sector. If the sector is not protected, a Write command updates all 32 bits of the selected block.

In I^2C mode, a sector provides 128 bytes that can be individually accessed in read and write modes. When protected by the corresponding I2C_Write_Lock bit, the entire sector is write-protected. To access the user memory, the device select code used for any I^2C command must have the E2 Chip Enable address at 0.

2 I²C password mechanisms

In the I²C mode only, it is possible to protect individual sectors against write operations.

This feature is controlled by the I2C_Write_Lock bits stored in the 8 bytes of the I2C_Write_Lock bit area starting from the location 2048 (see *Table 2*). Using these 64 bits, it is possible to write-protect all the 64 sectors in the M24LRxx memory.

Each bit controls the I²C write access to a specific sector as shown in *Table 2*. It is always possible to unprotect a sector in the I²C mode. When an I2C_Write_Lock bit is reset to 0, the corresponding sector is unprotected. When the bit is set to 1, the corresponding sector is write-protected.

In I²C mode, read access to the I2C_Write_Lock bit area is always allowed. Write access depends on the correct presentation of the I²C password.

To access the I2C_Write_Lock bit area, the device select code used for any I²C command must have the E2 Chip Enable address at 1.

On delivery, the default value of the 8 bytes of the I2C_Write_Lock bit area is reset to 00h.

Table 2. I2C_Write_Lock bit

I²C byte address		Bits [31:24]	Bits [23:16]	Bits [15:8]	Bits [7:0]
E2 = 1	2048	sectors 31-24	sectors 23-16	sectors 15-8	sectors 7-0
E2 = 1	2052	sectors 63-56	sectors 55-48	sectors 47-40	sectors 39-32

2.1 M24LRxx I2C password security

The M24LRxx controls the I²C sector write access using the 32-bit-long I²C password and the 64-bit I2C_Write_Lock bit area. The I²C password value is managed using two I²C commands: I²C Present Password and I²C Write Password.

2.1.1 I²C Present Password command description

The I²C Present Password command is used in the I²C mode to present the password to the M24LRxx in order to modify the write access rights of all the memory sectors protected by the I2C_Write_Lock bits, including the password itself. If the presented password is correct, the access rights remain activated until the M24LRxx is powered off or until a new I²C Present Password command is issued.

Following a Start condition, the bus master sends a device select code with the Read/Write bit ($R\overline{W}$) reset to 0 and the Chip Enable bit E2 at 1. The device acknowledges this, as shown in *Figure 3*, and waits for two I²C password address bytes, 09h and 00h. The device responds to each address byte with an acknowledge bit, and then waits for the 4 password data bytes, the validation code, 09h, and a resend of the 4 password data bytes. The most significant byte of the password is sent first, followed by the least significant bytes.

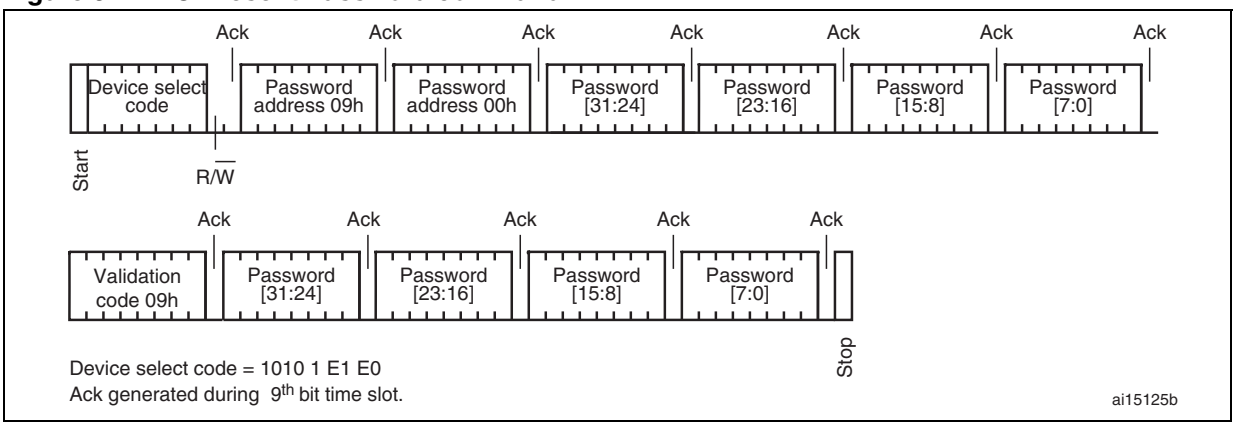
It is necessary to send the 32-bit password twice to prevent any data corruption during the sequence. If the two 32-bit passwords sent are not exactly the same, the M24LRxx does not start the internal comparison.

When the bus master generates a Stop condition immediately after the Ack bit (during the "10th bit" time slot), an internal delay equivalent to the write cycle time is triggered. A Stop condition at any other time does not trigger the internal delay. During that delay, the M24LRxx compares the 32 received data bits with the 32 bits of the stored I²C password.

If the values match, the write access rights to all protected sectors are modified after the internal delay. If the values do not match, the protected sectors remain protected.

During the internal delay, Serial Data (SDA) is disabled internally, and the device does not respond to any requests.

Figure 3. I²C Present Password command



2.1.2 I2C Write Password command description

The I²C Write Password command is used to write a 32-bit block into the M24LRxx I²C password system area. This command is used in I²C mode to update the I²C password value. It cannot be used to update any of the RF passwords. After the write cycle, the new I²C password value is automatically activated. The I²C password value can only be modified after issuing a valid I²C Present Password command.

On delivery, the I²C default password value is set to 0000 0000h and is activated.

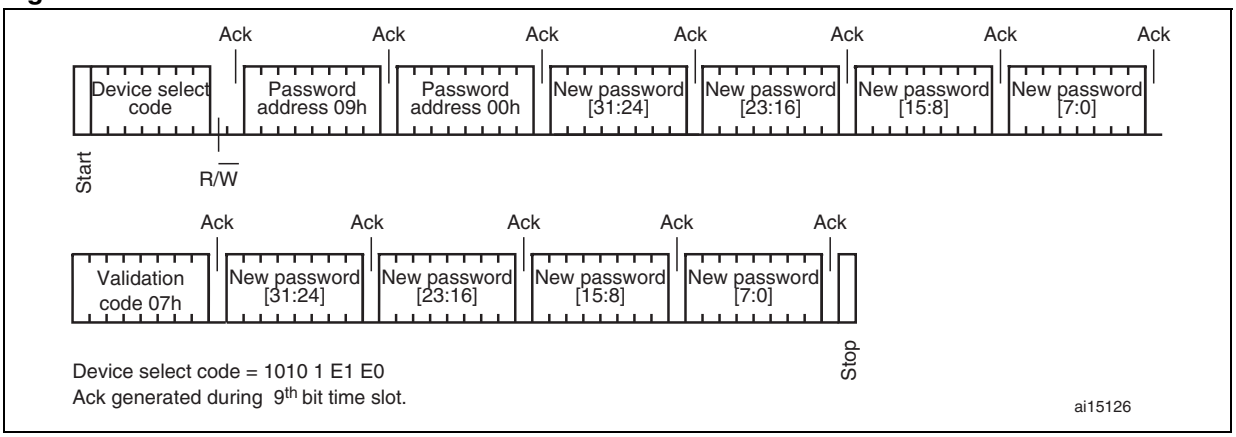
Following a Start condition, the bus master sends a device select code with the Read/Write bit ($R\overline{W}$) reset to 0 and the Chip Enable bit E2 at 1. The device acknowledges this, as shown in *Figure 4*, and waits for the two I²C password address bytes, 09h and 00h. The device responds to each address byte with an acknowledge bit, and then waits for the 4 password data bytes, the validation code, 07h, and a resend of the 4 password data bytes. The most significant byte of the password is sent first, followed by the least significant bytes.

It is necessary to send twice the 32-bit password to prevent any data corruption during the write sequence. If the two 32-bit passwords sent are not exactly the same, the M24LRxx does not modify the I²C password value.

When the bus master generates a Stop condition immediately after the Ack bit (during the 10th bit time slot), the internal write cycle is triggered. A Stop condition at any other time does not trigger the internal write cycle.

During the internal write cycle, Serial Data (SDA) is disabled internally, and the device does not respond to any requests.

Figure 4. I²C Write Password command



3 RF password mechanisms

The M24LRxx provides a special protection mechanism based on passwords. Each memory sector of the M24LRxx can be individually protected by one out of three available passwords, and each sector can also have read/write access conditions set.

Each memory sector in the M24LRxx is assigned with a Sector security status byte including a Sector Lock bit, two Password Control bits and two Read/Write protection bits as shown in *Table 3*. *Table 4* describes the organization of the Sector security status (SSS) byte. This byte can be read using the Read Single Block and Read Multiple Block commands with the Option_flag set to '1'.

On delivery, the default value of the SSS bytes is reset to 00h.

Table 3. Sector security status byte area

RF address	I^2C byte address		Bits [31:24]	Bits [23:16]	Bits [15:8]	Bits [7:0]
0	E2 = 1	0	SSS 3	SSS 2	SSS 1	SSS 0
128	E2 = 1	4	SSS 7	SSS 6	SSS 5	SSS 4
256	E2 = 1	8	SSS 11	SSS 10	SSS 9	SSS 8
384	E2 = 1	12	SSS 15	SSS 14	SSS 13	SSS 12
512	E2 = 1	16	SSS 19	SSS 18	SSS 17	SSS 16
640	E2 = 1	20	SSS 23	SSS 22	SSS 21	SSS 20
768	E2 = 1	24	SSS 27	SSS 26	SSS 25	SSS 24
896	E2 = 1	28	SSS 31	SSS 30	SSS 29	SSS 28
1024	E2 = 1	32	SSS 35	SSS 34	SSS 33	SSS 32
1152	E2 = 1	36	SSS 39	SSS 38	SSS 37	SSS 36
1280	E2 = 1	40	SSS 43	SSS 42	SSS 41	SSS 40
1408	E2 = 1	44	SSS 47	SSS 46	SSS 45	SSS 44
1536	E2 = 1	48	SSS 51	SSS 50	SSS 49	SSS 48
1664	E2 = 1	52	SSS 55	SSS 54	SSS 53	SSS 52
1792	E2 = 1	56	SSS 59	SSS 58	SSS 57	SSS 56
1920	E2 = 1	60	SSS 63	SSS 62	SSS 61	SSS 60

Table 4. Sector security status byte organization

b_7	b_6	b_5	b_4	b_3	b_2	b_1	b_0
0	0	0	Password Control bits		Read / Write protection bits		Sector Lock

When the Sector Lock bit is set to '1', for instance by issuing a Lock-sector Password command, the 2 Read/Write protection bits (b1, b2) are used to set the read/write access of the sector as described in *Table 5*.

Table 5. Read / Write protection bit setting

Sector lock	b_2, b_1	Sector access when password presented		Sector access when password not presented	
0	xx	Read	Write	Read	Write
1	00	Read	Write	Read	No Write
1	01	Read	Write	Read	Write
1	10	Read	Write	No Read	No Write
1	11	Read	No Write	No Read	No Write

The next 2 bits of the Sector security status byte (b_3, b_4) are the Password Control bits. The value of these two bits is used to link a password to the sector as defined in *Table 6*.

Table 6. Password Control bits

b_4, b_3	Password
00	No password protection: Password 0 condition
01	The sector is protected by the Password 1
10	The sector is protected by the Password 2
11	The sector is protected by the Password 3

The M24LRxx password protection is organized around a dedicated set of commands plus a system area of three password blocks where the password values are stored. This system area is described in *Table 7*.

Table 7. Password system area

Add	0 7	8 15	16 23	24 31
1	Password 1			
2	Password 2			
3	Password 3			

The dedicated password commands are:

Write-sector Password

The Write-sector Password command is used to write a 32-bit block into the password system area. This command must be used to update password values. After the write cycle, the new password value is automatically activated. It is possible to modify a password value after issuing a valid Present-sector Password command.

On delivery, the three default password values are set to 0000 0000h and are activated.

Lock-sector Password

The Lock-sector Password command is used to set the Sector security status byte of the selected sector. Bits b_4 to b_1 in the Sector security status byte are affected by the Lock-sector Password command. The Sector Lock bit, b_0, is set to '1' automatically.

After issuing a Lock-sector Password command, the protection settings of the selected sector are activated. The protection of a locked block cannot be changed in RF mode.

A Lock-sector Password command sent to a locked sector returns an error code.

Present-sector Password

The Present-sector Password command is used to present one of the three passwords to the M24LRxx in order to modify the access rights of all the memory sectors linked to that password (*Table 5*) including the password itself. If the presented password is correct, the access rights remain activated until the tag is powered off or until a new Present-sector Password command is issued. If the presented password value is not correct, all the access rights of all the memory sectors are deactivated.

Sector security status byte area access conditions in I^2C mode

In I^2C mode, read access to the Sector security status byte area is always allowed. Write access depends on the correct presentation of the I^2C password (see *I2C Present Password command description*).

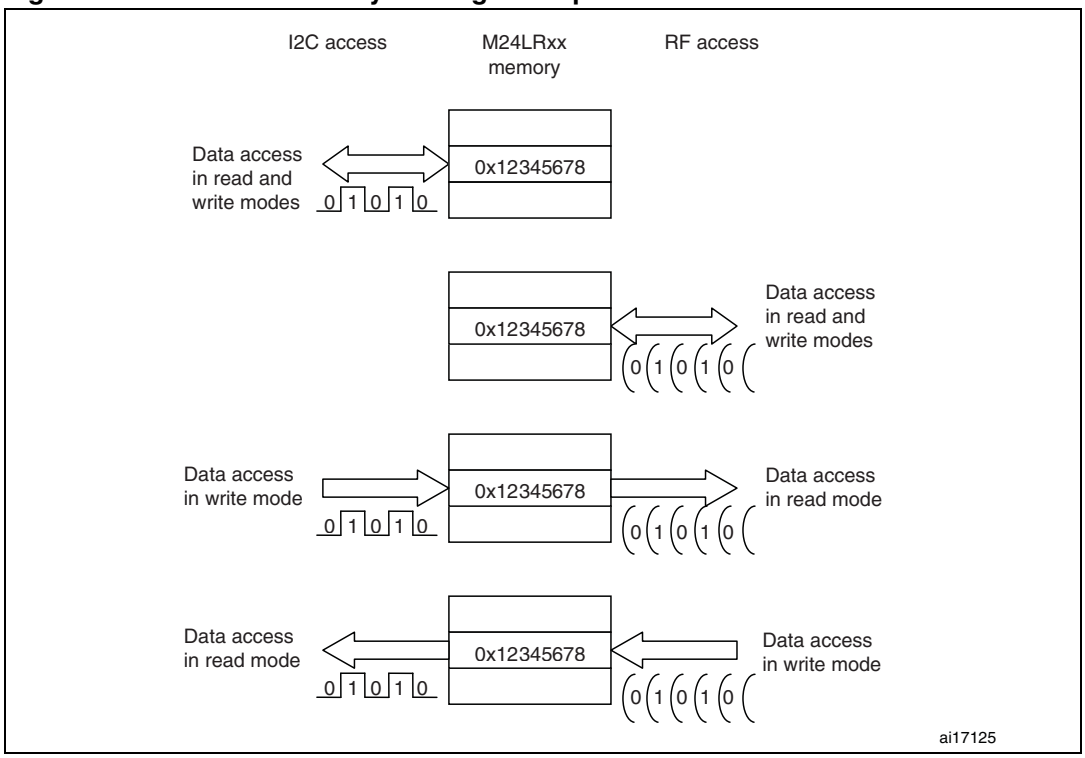
To access the Sector security status byte area, the device select code used for any I^2C command must have the E2 Chip Enable address at 1.

An I^2C write access to a Sector security status byte re-initializes the RF access condition to the given memory sector.

4 M24LRxx's conditional memory access

The 64 sectors of the M24LRxx are shared between I^2C and RF accesses. Data written in RF mode can be read in I^2C and data written in I^2C can be read in RF, if the granted access authorizes it. This feature provides an easy way of sharing data between contact access using the I^2C bus, on a PCB-based application for example, and RF access using an RFID reader/writer.

Figure 5. M24LRxx memory sharing concept



4.1 M24LRxx's conditional memory access using passwords

4.1.1 I^2C access

In the following example, the initial setting of the M24LRxx is described in the *Table 8* and *Table 9* below. Sectors 1 and 2 in the memory are protected against write accesses: bits b1 and b2 in the I2C_Write lock bit area are set to 1.

Table 8. I2C_Write_Lock bit

I^2C address	Bits[31:24]	Bits[23:16]	Bits[15:8]	Bits[7:0]
2048	0000 0000b	0000 0000b	0000 0000b	0000 0110b
2052	0000 0000b	0000 0000b	0000 0000b	0000 0000b

M24LRxx memory access after I²C power-on

After a correct I²C power-on condition, the M24LRxx offers the sector access conditions shown in *Table 9: I2C memory access condition at power on*.

All the memory sectors can be read, and write operations are allowed on all sectors except for sectors 1 & 2.

Note: The I2C_Write lock bit area can be accessed in read mode only.

Table 9. I²C memory access condition at power on

Access condition	M24LRxx user memory
Read and Write	Sector 0
Read only	Sector 1
Read only	Sector 2
Read and Write	Sector 3
Read and Write	…
Read and Write	Sector 62
Read and Write	Sector 63
Read only	I2C_Write lock bit area
Read only	Sector_Security_Status area

M24LRxx memory access after a valid I²C Present Password command

After a valid I²C Present Password command, assuming that the 32-bit password matched, the M24LRxx's sector access conditions are modified as described in *Table 10: I2C memory access condition after a valid I2C Present Password*.

All the 64 sectors of the M24LRxx are open to any write and read commands.

The I2C_Write lock bit area can also be updated to remove or add sector write protections. The write protection of the sector 2 can be removed by resetting bit b2 to 0 and the sectors 62 & 63 can be write-protected by setting the bits b62 & b63 to 1.

Note: It is also possible to update the Sector security status bytes used to define the read and write RF accesses to the M24LRxx sectors. The I²C bus gives full control over the RF sector access conditions. This feature allows the main application system connected to the I²C bus to fully control the M24LRxx access conditions for both I²C and RF.

Table 10. I^2C memory access condition after a valid I^2C Present Password

Access condition	M24LRxx user memory
Read and Write	Sector 0
Read and Write	Sector 1
Read and Write	Sector 2
Read and Write	Sector 3
Read and Write	…
Read and Write	Sector 62
Read and Write	Sector 63
Read and Write	I2C_Write lock bit area
Read and Write	Sector_Security_Status area

At the next M24LRxx power-on, the memory access conditions revert to the ones shown in *Table 11: I2C_Write_Lock bit update* and *Table 12: I2C memory access condition at next power on*.

Table 11. I2C_Write_Lock bit update

I^2C address	Bits[31:24]	Bits[23:16]	Bits[15:8]	Bits[7:0]
2048	0000 0000b	0000 0000b	0000 0000b	0000 0010b
2052	1100 0000b	0000 0000b	0000 0000b	0000 0000b

Table 12. I^2C memory access condition at next power on

Access condition	M24LRxx user memory
Read and Write	Sector 0
Read only	Sector 1
Read and Write	Sector 2
Read and Write	Sector 3
Read and Write	…
Read only	Sector 62
Read only	Sector 63
Read only	I2C_Write lock bit area
Read only	Sector_Security_Status area

4.1.2 RF access

In RF, via the ISO15693 or ISO18000-3 mode 1 contactless protocol, the M24LRxx's read and write sector access conditions are selected using the Sector security status bytes.

Through the setting of bits b1 & b2 (see *Table 5: Read / Write protection bit setting*), it is possible to:

- write-protect a sector, in which case the sector's data is read-only
- read-protect a sector, in which case the sector's data is not accessible from the RF

In the following example, the initial setting of the M24LRxx is described in *Table 13*. Sectors 0 to 3 are protected against various read and write access conditions as defined by the values of their Sector security status bits, b1 and b2.

M24LRxx memory access after RF power-on

After a correct RF power-on condition, the M24LRxx offers the sector access conditions shown in *Table 13: RF memory access conditions at power-on*. All the memory sectors can be read except for sectors 2 & 3, and write operations are allowed on all the sectors except for sectors 0, 2 & 3.

Table 13. RF memory access conditions at power-on

Access condition	M24LRxx user memory	SSS byte
Read only	Sector 0	0000 1001b
Read and Write	Sector 1	0000 1011b
Not accessible	Sector 2	0000 1101b
Not accessible	Sector 3	0000 1111b
Read and Write	…	0000 0000b
Read and Write	Sector 62	0000 0000b
Read and Write	Sector 63	0000 0000b
Not accessible in RF	I2C_Write lock bit area	Not applicable
Write once in RF	Sector_Security_Status area	Not applicable

M24LRxx memory access after a valid Present-sector Password command

After a valid Present-sector Password command, the memory sector accesses are changed as shown in *Table 14: RF memory access condition after a valid Present-sector Password*. The sector 0 can be updated by a write command, the sector 3 is now accessible in read mode, and the sector 2 is accessible in both read and write modes.

Table 14. RF memory access condition after a valid Present-sector Password

Access condition	M24LRxx user memory	SSS byte
Read and Write	Sector 0	0000 1001b
Read and Write	Sector 1	0000 1011b
Read and Write	Sector 2	0000 1101b
Read only	Sector 3	0000 1111b
Read and Write	…	0000 0000b
Read and Write	Sector 62	0000 0000b
Read and Write	Sector 63	0000 0000b
Not accessible in RF	I2C_Write lock bit area	Not applicable
Write once in RF	Sector_Security_Status area	Not applicable

This protection mechanism is submitted to an RF password value. The example above uses the password value 1 as defined by the Sector security status bits b3 & b4. The M24LRxx provides 3 different passwords, so that 3 different applications can manage its memory access conditions.

In the multiple RF password protection scheme, the M24LRxx memory can be divided into 6 different areas using the 4 different passwords conditions listed below:

- The public EEPROM area, no password protection
- The public ROM area, controlled by the password 0 condition
- The non-accessible area controlled by the password 0 condition
- The “application 1” area protected by the password 1
- The “application 2” area protected by the password 2
- The “application 3” area protected by the password 3

It is not mandatory to have contiguous sectors affected to the same area as each individual sector in the M24LRxx can be set to any one of the 4 password conditions.

Figure 6. RF multiple password memory access condition at power-up

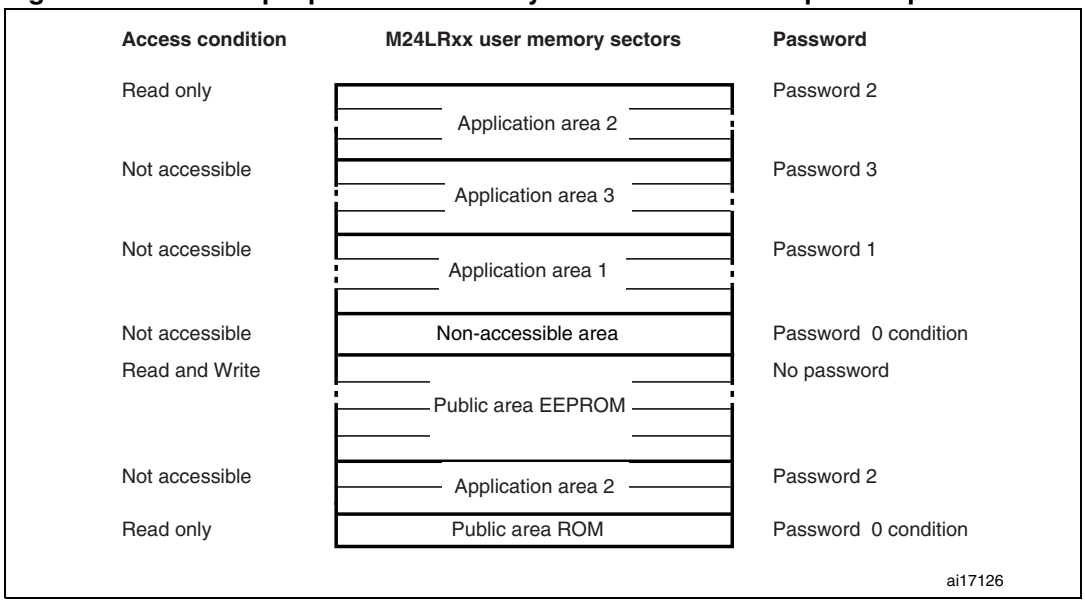


Figure 7. RF multiple password memory access condition after password 1 presentation

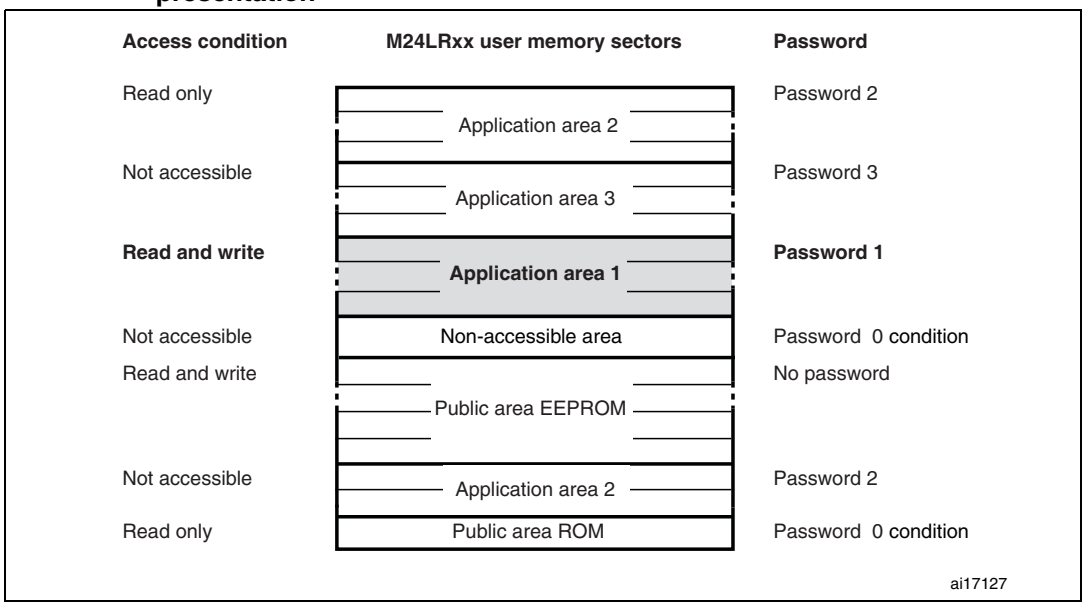
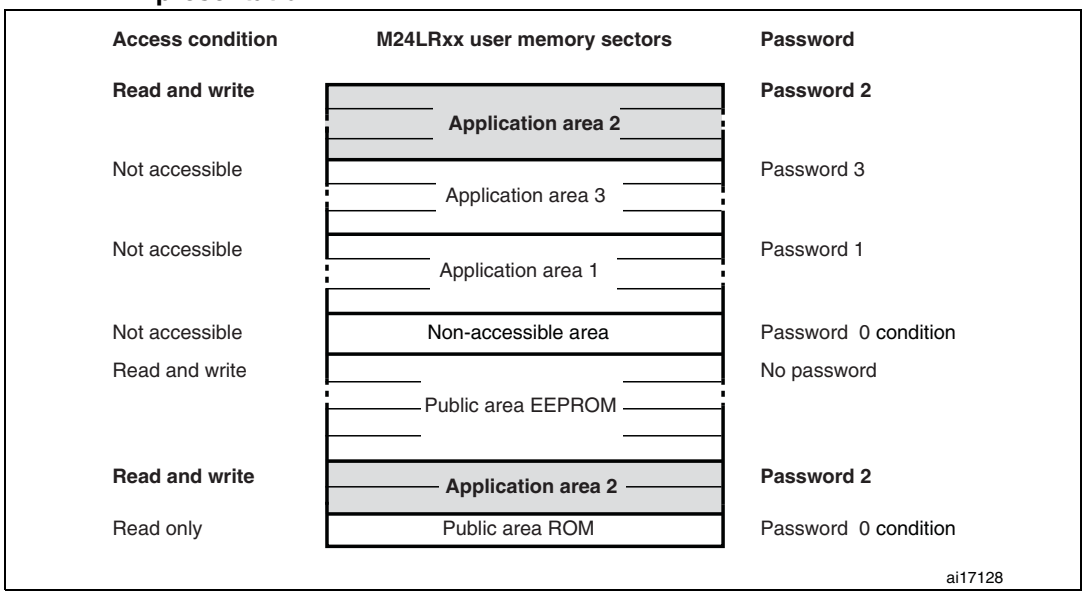


Figure 8. RF multiple password memory access condition after password 2 presentation



Using the password 0 condition

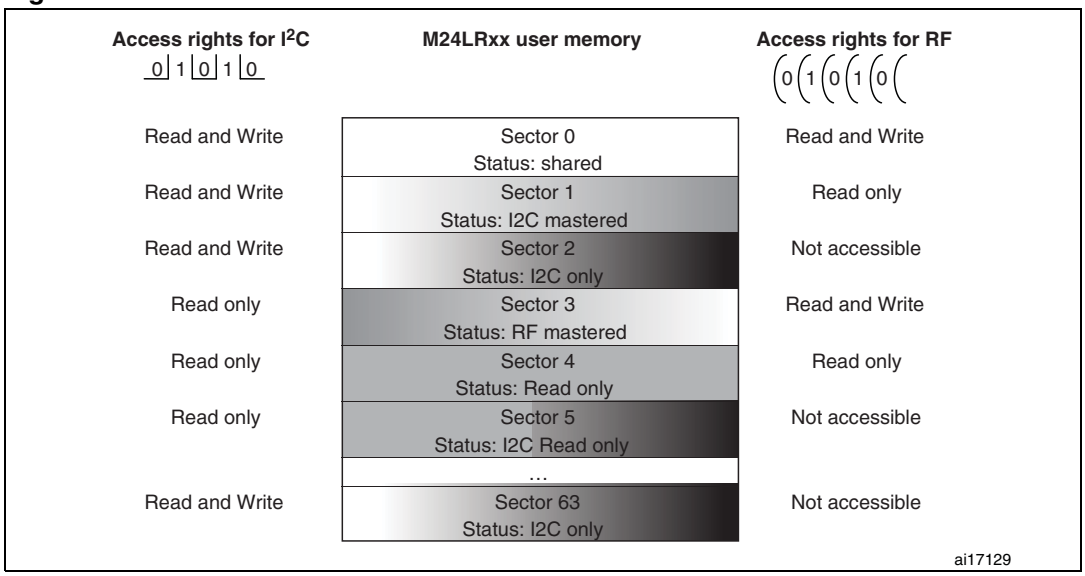
The M24LRxx offers the possibility of permanently locking the RF read/write access rights of a sector. The password 0 condition is applied by resetting (to '0') the bits b4 and b3 in the Sector security status byte (see *Table 6: Password Control bits*), and then by issuing the RF Lock-sector Password command. The access rights defined by bits b2 and b1 (see *Table 5: Read / Write protection bit setting*) are then applied in a permanent way. Indeed, since the RF Present-sector Password command does not allow the use of Password 0, the sector access rights once applied can no longer be modified.

4.1.3 Mixed RF and I^2C access

Mixed data access conditions between the main application (using the I^2C bus) and the RF environment (using the RFID reader/writer) can be defined on the basis of the I^2C and RF access conditions described in *Section 4.1.1: I2C access* and *Section 4.1.2: RF access*.

The M24LRxx offers flexibility, allowing the sharing of data or restricting their access as illustrated in *Figure 9: M24LRxx RF and I2C access condition mix*.

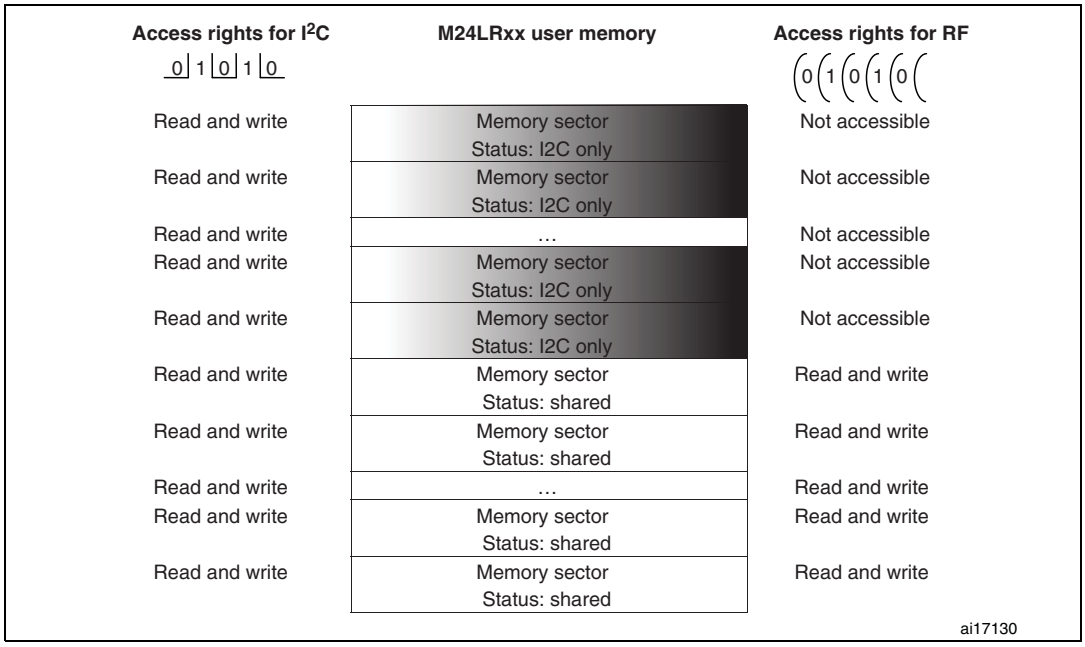
Figure 9. M24LRxx RF and I²C access condition mix



1. The lighter the shade the more rights, the darker the shade, the less rights (so that white indicates both read and write access rights whereas black means neither).

It is simple to extend the RF capability of existing serial EEPROM memory applications by using the scheme given in *Figure 10*.

Figure 10. Example of an RF capability extension in an application running with an EEPROM



1. The lighter the shade the more rights, the darker the shade, the less rights (so that white indicates both read and write access rights whereas black means neither).

In *Figure 10*, the first part of the memory is limited to I²C access to ensure backward compatibility with the existing I²C serial access. The rest of the memory is shared between I²C and RF, making it possible to transfer data in both a "contact" and a "contactless" way, between the I²C interface application and the RFID reader.

5 Revision history

Table 15. Document revision history

Date	Revision	Changes
26-Jun-2009	1	Initial release.
24-Oct-2012	2	M24LR64-R replaced by M24LRxx-R and M24LRxxE-R on the cover page, then by M24LRxx (see *Note:*). Added *Table 1: Applicable products*.