Standard Read/Write Crypto Identification IC

Description

The e5561 is a member of the Atmel Wireless & Microcontrollers **ID**entification **IC** (IDIC®) family for applications where information has to be transmitted contactlessly. The IDIC® is connected to a tuned LC circuit for power supply and bidirectional data communication (**R**ead/**W**rite) to a base station. Atmel Wireless & Microcontrollers offers LC circuit and chip assembled in form of a transponder or tag. These units are small, smart and rugged data storage units.

The e5561 is a Read/Write crypto IC for applications which demand higher security levels than standard R/W transponder ICs can offer. For that purpose, the e5561 has an encryption algorithm block which enables a base station to authenticate the transponder. The base station transmits a random number to the e5561. This challenge is encrypted by both IC and base station. The e5561 sends back the result to the base station for comparison. As both should possess the same secret key, the results of this encryption are expected to be equal. Any attempt to fake the base station with a wrong transponder will be recognized immediately.

The on-chip 320-bit EEPROM (10 blocks of 32 bits each) can be read and written blockwise by a base station. Two or four blocks contain the ID code and six memory blocks are used to store the crypto key as well as the read/write options. The crypto key and the ID code can be protected individually against overwriting. Likewise, the crypto key can not be read out.

125 kHz is the typical operational frequency of a system using the e5561. Two read data rates are programmable. Reading occurs through damping the incoming RF field with an on-chip load. This damping is detected by the field-generating base station. Data transmission starts after power-up with the transmission of the ID code and continues as long as the e5561 is powered. Writing is carried out with Atmel Wireless & Microcontrollers' writing method. To transmit data to the e5561, the base station has to interrupt the RF for a short time to create a field gap. The information is encoded in the number of clock cycles between two subsequent gaps.

Features

- Low-power, low-voltage CMOS IDIC®
- Contactless power supply, data transmission and programming of EEPROM
- Radio Frequency (RF): 100 kHz to 150 kHz, typically 125 kHz
- Automatic programmable adaptation of resonance frequency
- Easy synchronization with special terminators
- High-security method unilink challenge response authentication by AUT64 crypto algorithm
- Encryption time < 10 ms, optional < 30 ms programmable at 125 kHz
- 320-bit EEPROM memory in 10 blocks of 32 bits each
- Programmable read/write protection
- Extensive protection against contactless malprogramming of the EEPROM
- Programming time for one block of the EEPROM 16 ms typically
- Main options set by EEPROM:
  Bitrate [bit/s]: RF/32, RF/64
  Encoding: Manchester, Biphase

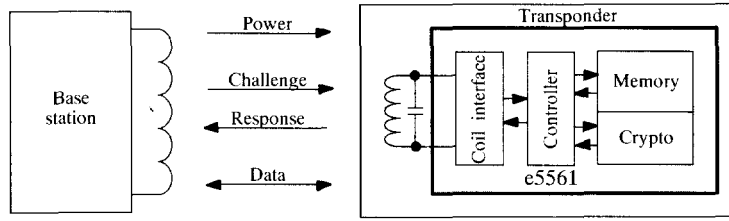


Figure 1. Transponder system example using e5561

Table of Contents

Table of Contents (continued)

Ordering Information

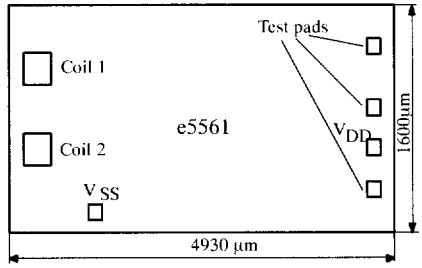
Extended Type Number	Package	Remarks
e5561A-DOW	DOW	

Pads

Name	Pad Window	Function
Coil 1	136 x 136 µm²	1st coil pad
Coil 2	136 x 136 µm²	2nd coil pad
V_{DD}	78 x 78 µm²	Positive supply voltage
V_{SS}	82 x 82 µm²	Negative supply voltage (gnd)

For normal (coil-driven) operation, the e5561 needs only Coil 1 and Coil 2.

Chip Dimensions



1 Internal Modes of the e5561

The e5561 can be operated in several internal modes, each providing a special function. These are:

- Start-up
- ID mode
- Programming mode
- Direct-access mode
- Crypto mode
- Stop mode
- Password function

The following section gives a short functional description of each mode. A more detailed description is given in the section: "Operating the e5561".

1.1 Start-up

After the power-on reset (POR) has reset the entire circuit, the e5561 is configured by reading out the configuration data bits of the EEPROM.

1.2 ID Mode

In the ID mode the e5561 transmits an identification datastream (ID code) to the base station. As the base station reads out data coming from the transponder, this direction of data transmission will be designated as 'read'.

The ID code is sent in loop as long as the RF field is applied. The single parts of the datastream and the type of modulation depend on the configuration loaded during start-up. The following options are available during ID mode:

- Two different bitrates and modulations
- Two possible lengths of ID code (64 bit or 128 bit)
- Two different terminators
- 4-bit preburst followed by terminator 1 between start-up and sending the first data bits of the ID-code

1.3 Programming Mode

The e5561 must be programmed before being used in a security system. The e5561 contains a 320-bit EEPROM which is arranged in 10 blocks of 32 bits each. Programming the e5561 is carried out blockwise, i.e., every single block has to be programmed separately. The blocks of the EEPROM are divided into 4 sections:

- Configuration
- ID code
- Crypto key
- Customer configuration

Every section consists of one or more block of the EEPROM. Programming is carried out by sending the programming data sequence to the e5561. As the base station sends data to the transponder this direction of data transmission will be designated as 'write'.

After the base station has sent the data sequence and the specified block has been programmed, the e5561 transmits the content of the programmed EEPROM block. The content is always sent in loop with terminator 1. The beginning of the datastream is indicated by a preburst.

During programming, the e5561 monitors several fault and protection mechanisms. If a fault or a protection violation is detected, the e5561 enters the ID mode.

1.4 Direct-Access Mode

If the base station transmits a special data sequence to the e5561, it will enter the direct-access mode. The base station can activate two different functions:

- Read the content of a single block of the EEPROM:

In this case, the e5561 transmits the block's content in loop, starting with a preburst followed by the terminator which is also used to indicate the beginning of the transmission of the specified block data.

- Reset the e5561 in case of all modes:

During the direct-access mode, the e5561 monitors several fault and protection mechanisms. If a fault or a protection violation is detected, the e5561 enters the ID mode.

1.5 Crypto Mode

In crypto mode, a non-linear high-security encryption algorithm called AUT64 is used to authenticate the e5561.

After the base station has identified the e5561 (i.e., read the ID code), the base station may authenticate the transponder by transmitting it a challenge. Receiving this data sequence, the e5561 enters the crypto mode.

This initiates the following actions:

- During calculating the AUT64 result, the transponder transmits the checksum of the challenge
- The e5561 generates the response from the calculated result of the AUT64
- As soon as the calculation is finished, the e5561 interrupts the transmission of the checksum by sending a terminator
- The e5561 transmits the response in loop with a terminator back to the base station

The base station can read the response and authentify the transponder. It is possible to interrupt the calculation of the AUT64 result by sending another data sequence (e.g., if the checksum was found to be wrong).

During the crypto mode, the e5561 monitors several fault and protection mechanisms. If a fault or a protection violation is detected, the e5561 enters the ID mode.

1.6 Stop Mode

If two or more transponders are used simultaneously (e.g., in a manufacturing step), it might be useful to be able to set the transponders in a passive state. To avoid a communication conflict, the base station has to transmit a special data sequence to the active transponder(s) forcing them to enter the stop mode.

In the stop mode, the e5561 switches off the damping as long as the RF field is applied. After a power-on reset, or after receiving the software-reset command the e5561 enters the start-up and the ID mode again.

During the data sequence of the stop mode, the e5561 monitors fault mechanisms. If a fault is detected, the e5561 enters the ID mode.

The stop command can be disabled.

Note: For correct operation of the stop-mode it is necessary that the field is switched off instantly.

1.7 Password Function

The password function is a separate protection mechanism to avoid that a base station can read or manipulate the internal configuration and data blocks of the e5561 without knowing the password. Only a transition to the crypto-mode is enabled. If the password function is active, the base station has to send the password before any other operations are possible.

During the password mode, the e5561 monitors several fault and protection mechanism. If a fault or a protection violation is detected, the e5561 enters the ID mode.

1.8 Mode Transitions

If the e5561 is in ID mode and the base station transmits a write sequence by interrupting the RF field, the internal mode changes according to the received write sequence. If an error has been detected or the password function has been enabled, the e5561 remains in ID mode.

A transition to and from all other modes (except the ID mode) is possible by sending the corresponding write sequence. Once the ID mode is left, returning is only possible by sending an uncorrect data sequence to the transponder.

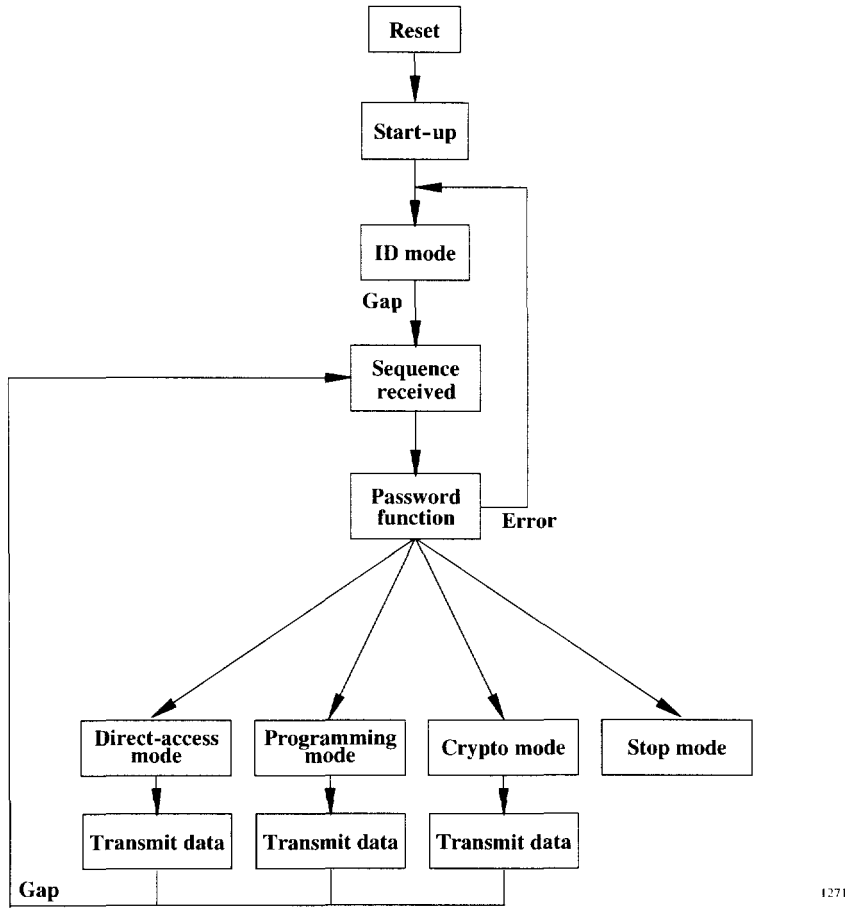


Figure 2. State diagram of the e5561 (overview)

Note: This picture is only an overview. In reality, more transitions are possible.

2 Building Blocks of the e5561

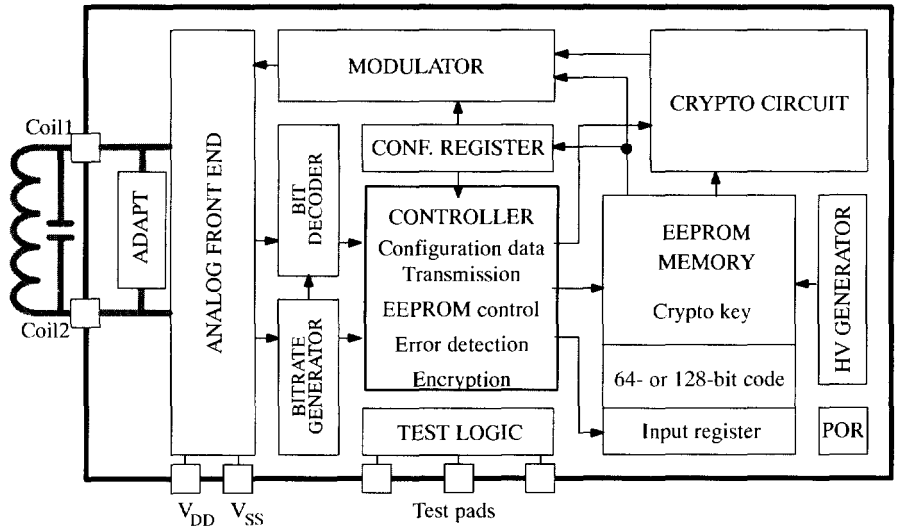


Figure 3. Block diagram

2.1 Analog Front End (AFE)

The AFE includes all circuits directly connected to the coil. It generates the IC's power supply and handles the bidirectional data communication with the base station. It consists of the following blocks:

- Rectifier to generate a DC supply voltage from the AC coil voltage
- Clock extractor
- Switchable load between Coil1/Coil2 for data transmission from the IC to the base station (read)
- Field gap detector for data transmission from the base station to the IC (write)

2.2 Controller

The controller has following functions:

- Initialize and refresh configuration register from EEPROM
- Control memory access (read, program)
- Handle correct write data transmission
- Error detection and error handling
- Control encryption operation
- Control adaptation of resonance frequency

2.3 Power-On Reset (POR)

The power-on reset is a delay reset which is triggered when the supply voltage is applied.

2.4 Configuration Register

The configuration register stores the configuration data read out from EEPROM blocks 0 and 9. It is continuously refreshed which increases the reliability of the device (if the initially loaded configuration was wrong or modified, it will be corrected by subsequent refresh cycles).

2.5 Adapt

The e5561 is able to minimize the tolerance of the resonance frequency between the base station and the transponder by switching on-chip capacitors in parallel to the LC circuit of the transponder. By using a coil of approximately 4 mH for a resonance frequency of 125 kHz it is possible to tune the resonance frequency in a range of about 5%. The active value of adapt is carried out automatically every time if the e5561 enters the RF field or the EEPROM is read out. This depends on a control bit. The automatic adaptation stops at this moment when the optimized adaptation is reached. This time is between 1.0 ms and 5.0 ms (125 kHz) depending on the capacitance value required. The voltage at Coil 1/Coil 2 after start-up is shown in figure 8.

Adapt bits: Details

In addition to the adapt mode which is executed during start up phase by the IC itself, it is possible to set the adapt bits in EEPROM manually.

Before using manual setting of adapt bits, the one bit A in block 0 must be set to 1 (see figure 9).

This content of the three bits to be defined, are determining the response frequency of the transponder in a limitted range.

Bits are set by microcontroller programming of block 0.

2.6 Bitrate Generator

The bitrate generator can deliver bitrates of RF/32 and RF/64 for data transmission from the e5561 to the base station.

2.7 Bit Decoder

The bit decoder forms the signals needed for write operation and decodes the received data bits in the write data stream.

2.8 Modulator

The modulator consists of two data encoders and the terminator generator. There are two kinds of modulation:

- Manchester mid-bit rising edge = data H;
  mid-bit falling edge = data L
- Biphase every bit creates a change, a data "0" creates an additional mid-bit change

By using biphase modulation, data transmission always starts damping on.

2.9 HV Generator

Voltage pump which generates about 18 V for programming of the EEPROM.

2.10 Memory

The memory of the e5561 is a 320-bit EEPROM which is arranged in 10 blocks of 32 bits each. All 32 bits of a block are programmed simultaneously. The programming voltage is generated on-chip.

Block 0 is reserved for basic configuration data. Blocks 1 to 9 are freely programmable. Blocks 1 to 4 are used for the ID code, blocks 5 to 8 contain the crypto key. In password mode, bits 4 to 31 of block 9 contain the password; bits 0 to 3 of block 9 contain the customer-configuration data. If no password is required, the corresponding bits can be programmed freely.

NOTE: Data from the memory is transmitted serially, starting with the least significant bit #0.

The basic configuration data in block 0 contains the following information (see figure 9):

- Type of modulation and bitrate
- Length of ID code
- Several lockbits
- Terminator set

The customer-configuration data in block 9 contains (see figure 10):

- Lockbit for ID code (blocks 1 and 4/ 1 to 4)
- Lockbit for crypto key (block 5 to 8)
- Lockbit for block 9
- Password mode enable

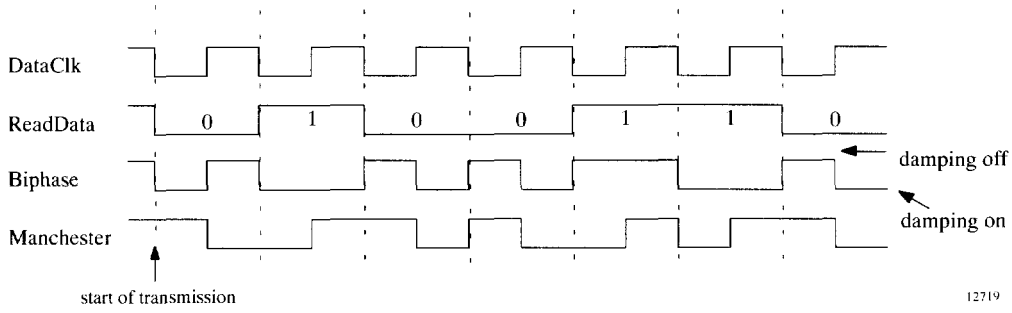


Figure 4. Types of modulation

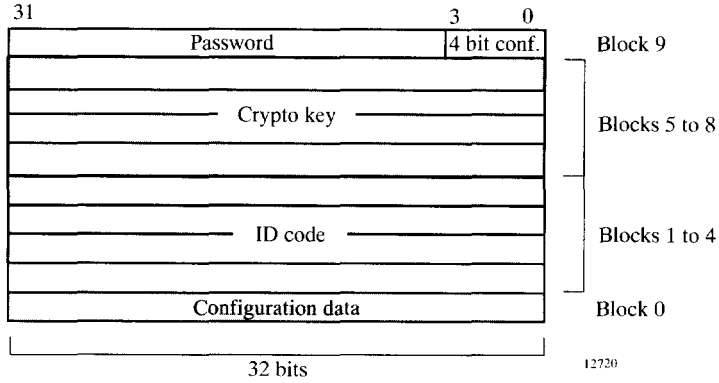


Figure 5. Memory map

2.11 Crypto Circuit

The crypto circuit uses the certified AUT64-algorithm to encrypt the challenge which is written to the e5561. The computed result can be read by the base station. Comparing the encryption results of the base station and the e5561, a high-security authentification procedure is established. This procedure requires the crypto key of the e5561 and the base station to be equal. The crypto key is stored in the blocks 5 to 8 of the EEPROM and can be locked by the user to avoid read-out or changes.

3 Protection Mechanisms of the e5561

Several protection mechanisms are implemented into the e5561. The two main groups are:

- Error mechanisms to detect a fault. These mechanisms are always enabled.
- Programmable protection mechanisms. These mechanisms are optional. When used, they provide protection against attempts to break the security system.

3.1 Password Protection

If the password protection is enabled, the e5561 remains in ID mode even if it has received a correct write sequence. The only possible operation is to modify the content of block 9 by sending the correct password bits. In all other cases, an error handling procedure is started and the e5561 enters ID mode.

3.2 Lockbit Protection

A lockbit is a physical part of the EEPROM's content and is controlled as well as by the customer. The lockbit protection mechanism has two different effects:

- Avoid programming (modifying data) of the EEPROM's blocks
- Avoid reading out the crypto key from the EEPROM using direct-access mode

If the base station tries to read out the crypto key and the corresponding lockbit is set, the e5561 will enter the ID mode immediately. Once the crypto key lockbit is set, the crypto key can neither be modified nor read out any more.

There are several lockbits available, each affecting a special data region of the EEPROM. The main groups of lockbits are:

- Lockbits to inhibit programming of the specified blocks of the EEPROM
- Lockbits to inhibit programming of the specified blocks of a specific address range

In both cases, an attempt to modify a data region protected by a lockbit will cause an error handling procedure (i.e., the e5561 enters ID mode)

3.3 Stop Mode

The stop mode can also be used as a protection mechanism, e.g., during configuration at manufacturing. The base station can configure the transponders one by one, forcing them into stop mode after programming. In this way, transponders can be programmed even if there are other transponders in the RF field at the same time.

4 Operating the e5561

4.1 General

The basic functions of the e5561 are: *supply* the IC from the coil, *read* data from the EEPROM to the base station, *authenticate* the IC, *receive* commands from the base station and *program* the received data into the EEPROM. Several *write errors* can be detected to protect the memory from being overwritten with uncorrect data. A password function is implemented ensuring that only authorized people can operate the IC.

Operating modes:

- **ID mode:** the e5561 sends ID code to the base station
- **Programming mode:** the e5561 programs the EEPROM with data bits received from the base station
- **Direct-access mode:** the e5561 sends the content of single block of the EEPROM to the base station
- **Crypto mode:** the e5561 computes a response according to the challenge received from the base station and sends the response to the base station
- **Stop mode:** the e5561 stops modulation

An additional password function enables the e5561 to be operated only by a person who knows the password programmed in the EEPROM memory.

4.2 Supply

The e5561 is supplied via a tuned LC circuit which is connected to the Coil1 and Coil2 pads. The incoming RF (actually a magnetic field) induces a current into the coil which powers the chip. The on-chip rectifier generates the DC supply voltage (V_{DD}, V_{SS} pads). Overvoltage protection prevents the IC from damage due to high field strengths (depending on the coil, the open-circuit voltage across the LC circuit can reach more than 100 V). The first occurrence of RF triggers a power-on reset pulse, ensuring a defined start-up state.

4.3 Start-up

The various modes of the e5561 are activated after the first read-out of the configuration. The modulation is on during power-on reset and is off while the configuration is read. After this initialization period of 128 + POR time FCs the e5561 starts the automatic adaptation of the resonance frequency. After the adaptation is carried out, the e5561 enters the ID mode immediately if the terminator 2 is selected, otherwise a data value of Fh in the selected configuration (modulation, bitrate) is sent followed by the optionally specified terminator 1 (see figure 8).

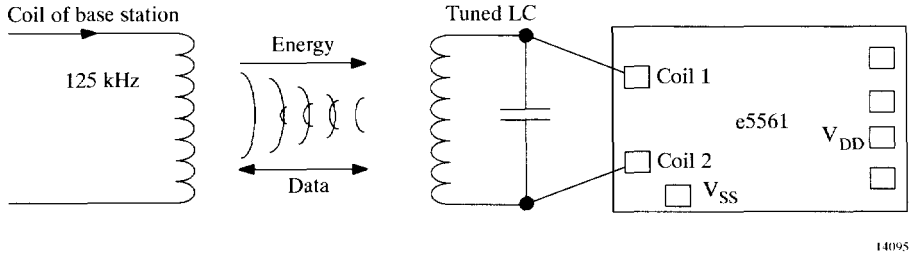


Figure 6. Application circuit

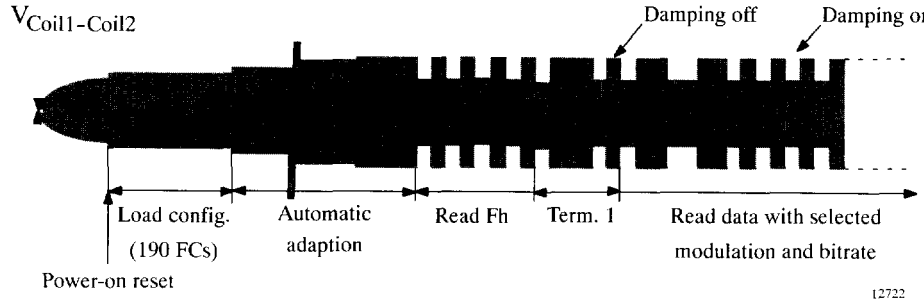


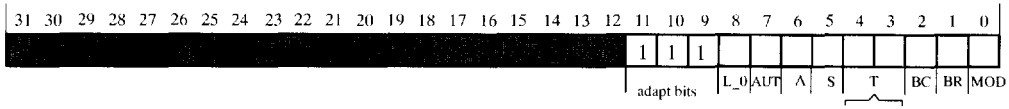
Figure 7. Voltage at Coil1/Coil2 after start-up (e.g., RF/32, Manchester, Terminator 1)

4.4 Configuration

The configuration data of the e5561 is stored in block 0 of the EEPROM which contains the following information (see figure 9):

- Type of modulation and bitrate
- Length of ID code
- Several lockbits
- Selected terminator
- Stop mode selection for short / long authentication time
- Adaptation of resonance frequency (if auto-adapt is not used)

The configuration may be changed by programming block 0. However, this is only possible if the lockbit L_0 in block 0 has not been set.



MOD	Modulation ('0' = Manchester, '1' = Biphase)
BR	Bitrate ('0' = RF/32, '1' = RF/64)
BC	Bitcount ('0' = 128 bit, '1' = 64 bit) ID
T	Terminator
S	Stop mode (0 = off, 1 = on)
A	Adapt (0 = automatic, 1 = value according to user programmed adapt bit setting
AUT	Number of AUT64-times, 0 = 24 times, 1 = 8 times
L_0	Lockbit for block 0 ('1'= active)
adapt bits	Tuning bits

	[1]	[0]
Test only	0	0
Terminator 1	1	0
Terminator 2	0	1
No terminator	1	1

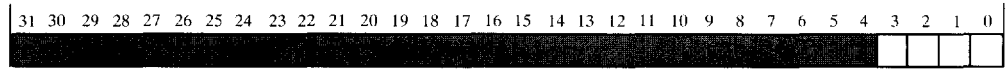
14096

Figure 8. Configuration data in block 0

Block 9 contains the customer configuration and the password (if password function is enabled). The customer-configuration data in block 9 includes (see figure 10):

- lockbit for ID code (blocks 1 and 4/ 1 to 4)
- lockbit for crypro key (block 5 to 8)
- lockbit for block 9
- password function enable

If the password function has been enabled, bits 4 to 31 represent the password of the e5561.



PWD	Password enable ('1' = active)
L_9	Lockbit for block 9 ('1' = active)
L_K	Lockbit for blocks 5 to 8 (crypto key) ('1' = active)
L_ID	Lockbit for blocks 1 and 4/ 1 to 4 (ID code) ('1' = active)

12724

Figure 9. Customer configuration data in block 9

4.5 Data Transmission to the Base Station (Read)

Data transmission from the e5561 to the base station is carried out by switching a load between the coil pads on (damping) and off. This changes the current through the IC coil which can be detected by the base station.

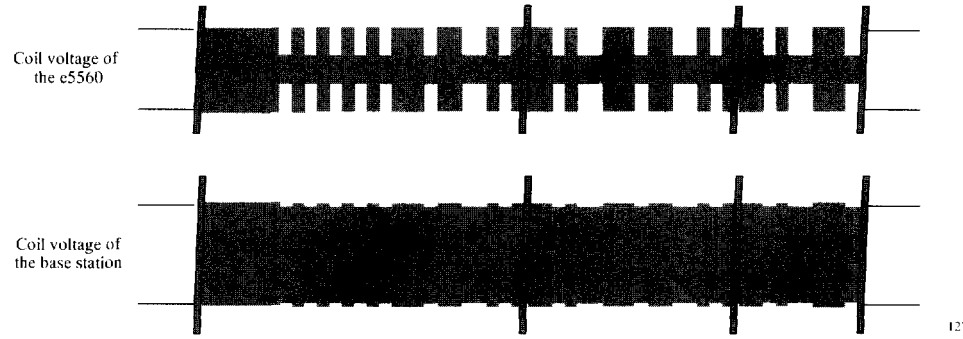


Figure 10. Signals from the transponder during reading

4.5.1 ID Mode

The ID mode is the default mode after starting-up. The ID code is read out of the EEPROM and sent to the base station.

4.5.2 Modulation and Bitrate

The different bitrates and modulators of the e5561 can be selected using the appropriate bit in block 0. Available bitrates are RF/32 and RF/64; the e5561 provides biphase and manchester modulation.

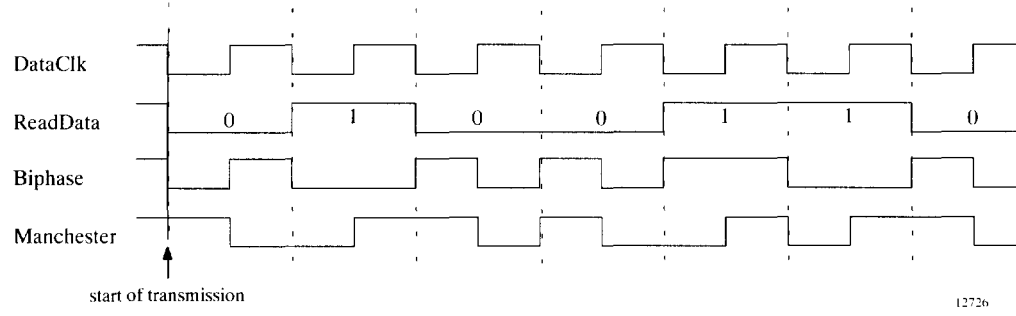


Figure 11. Types of modulation

4.5.3 Data Streams

Reading begins with block 1 (LSB first). Depending on the selected bitcount, block 1 is followed by block 2, 3 and 4 (128-bit bitcount) or just by block 4 (64-bit bitcount). The ID code is transmitted in loop or interrupted by the selected terminator, respectively. To avoid malfunction, the mode register is refreshed continuously with the content of EEPROM blocks 0 and 9 during reading of block 4. The data streams of the ID mode are shown in figure 13.

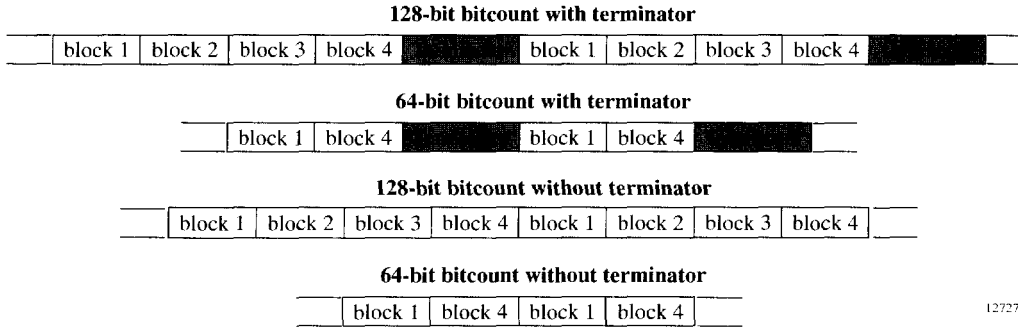


Figure 12. ID mode data streams

4.5.4 Terminators

Terminators are a special pattern to mark the beginning and end of the code. The terminators may be used to synchronize the base station. They can be detected reliably since they are a violation of the modulation scheme. After a terminator is sent, transmission of the first bit of the ID-code starts with damping on for a certain detection (if biphase modulation is used).

Note: Terminator 2 is only available in ID mode; all other modes make use of terminator 1.

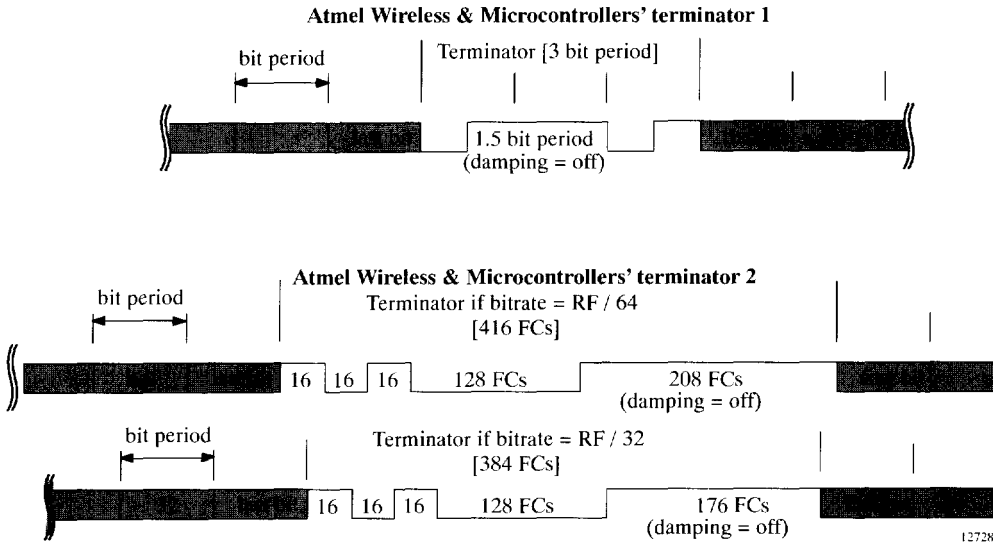


Figure 13. Terminators

4.6 Data Transmission to the e5561 (Write)

Data transmission from the base station to the e5561 is carried out by using the Atmel Wireless & Microcontrollers write method. It is based on interrupting the RF field with short gaps. The number of field clock cycles (FC) of two consecutive gaps encodes the '0/1' bit-information to be transmitted.

4.6.1 Start Gap

The first gap is the start gap which triggers writing. During writing the damping is permanently enabled which simplifies gap detection. The start gap has to be longer than the subsequent gaps in order to be reliably detected. By default, a start gap will be detected at any time after start-up intialization has been finished (field-on plus approx. 2 ms).

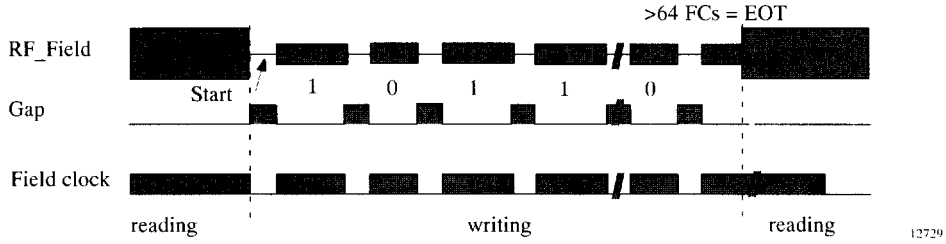


Figure 14. Signals to the transponder during writing

4.6.2 Bit Decoder

The duration of the gaps is usually 50µs - 150µs. The time between two gaps is nominally 24 field clocks for a '0' and 56 field clocks for a '1'. The bit will be interpreted as '0' if there are 16 to 32 field clocks since the last field gap; it will be interpreted as '1' if the number of field clock cycles is in a range of 48 to 64. When there is no gap for more than 64 field clocks, writing is carried out (EOT). If there is a wrong number of field clocks between two gaps- i.e., one or more data sent were not a valid '0' or '1' - the e5561 will detect an error (see 'Error handling').

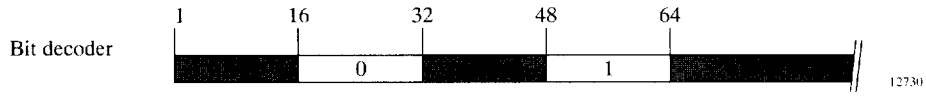


Figure 15. Bit decoding scheme (number of FCs between two consecutive gaps)

4.6.3 OP Codes

The OP code is defined as the first two bits of a writing sequence. It is used for changing the operational modes of the e5561. There are three valid OP codes: The programming mode and direct-access mode are entered with the '10' OP code, '01' is used to initiate the authentication of the e5561, and the OP code '00' disables modulation until a POR occurs.

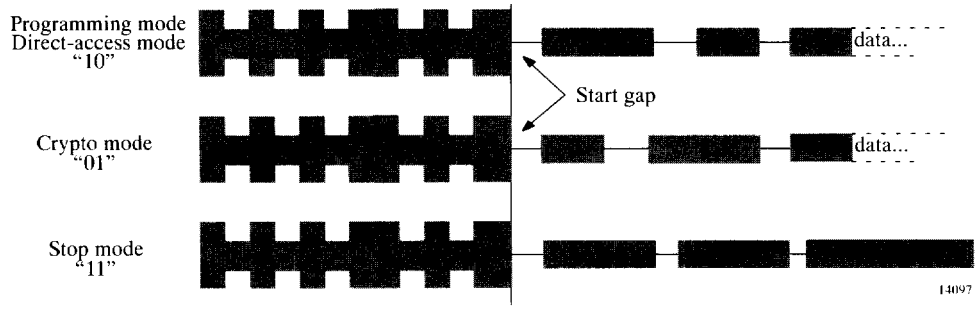


Figure 16. OP codes

4.6.4 Programming Mode

Programming the EEPROM of the e5561 is carried out blockwise, i.e., every single block has to be programmed separately. The programming-mode write sequence is shown in figure 18. After the OP code '10', the 32 data bits have to be sent followed by the four address bits specifiying the block to be programmed (each LSB first). The sequence is completed by sending an EOT (end of transmission), i.e., more than 64 field clocks without any gap.

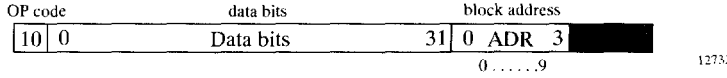


Figure 17. Programming mode write sequence

When the entire write sequence is written to the e5561, programming may proceed. There is a 64-clock delay between the end of writing and the start of programming. During this time, the EEPROM's programming voltage V_{PP} is measured and the lockbit for the block to be programmed is examined. Further, V_{PP} is continually monitored throughout the programming cycle. If Vpp is too low, the chip starts error handling. The programming time is 16 ms (including erase) with a field clock frequency of 125 kHz.

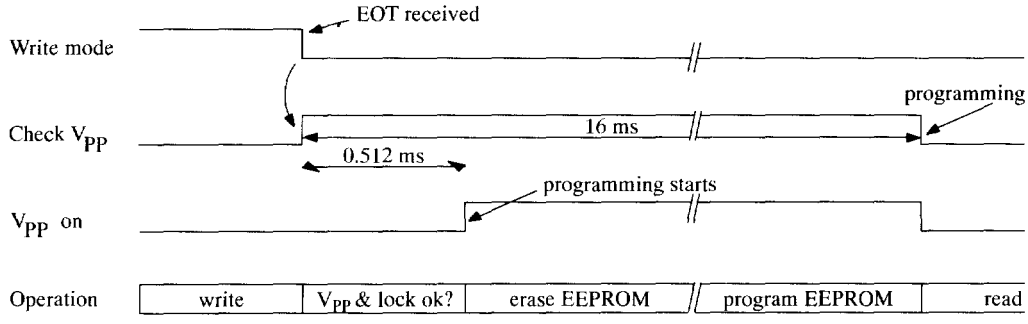


Figure 18. Programming

After programming is carried out, the e5561 sends an Fh preburst followed by the terminator 1. After that, the just programmed data is read out of the EEPROM and sent in loop with the terminator 1. This enables the base station to detect a malprogramming by comparing the data transmitted with the data read out after programming. This mode remains until a POR occurs or another gap is detected.

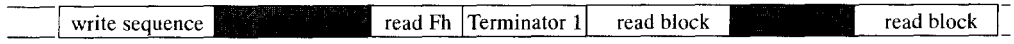


Figure 19. Programming mode datastream

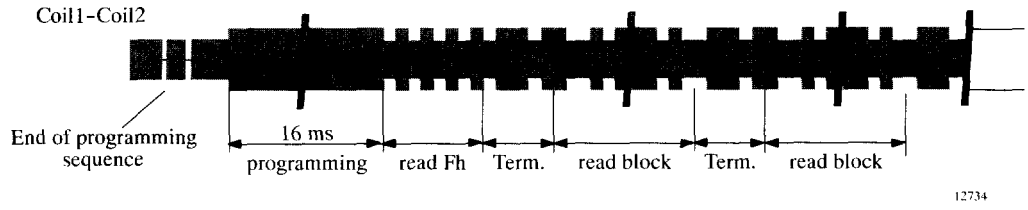


Figure 20. Coil voltage in programming mode

4.6.5 Direct-Access Mode

The direct-access mode is typically used to read out the content of a single block of the EEPROM. The write sequence is shown in figure 22. Following the OP code '10', the address of the block to be read has to be sent (LSB first).

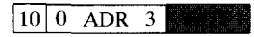


Figure 21. Direct-access mode write sequence

Reading the content of block 0 and the four blocks of the ID code is always possible. The blocks containing the crypto-key (blocks 5 to 8) can only be accessed when the corresponding lockbit in block 9 is not set. Therefore, there is no possibility for a non-authorized person to read out or modify the crypto key if it is locked. Figure 23 shows the direct-access-mode data stream. After the write sequence, an FFh preburst is sent followed by the terminator 1. After that, the addressed block and the terminator 1 are sent in loop.

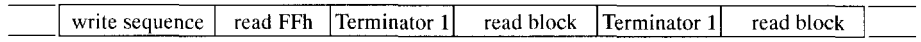


Figure 22. Direct-access mode datastream

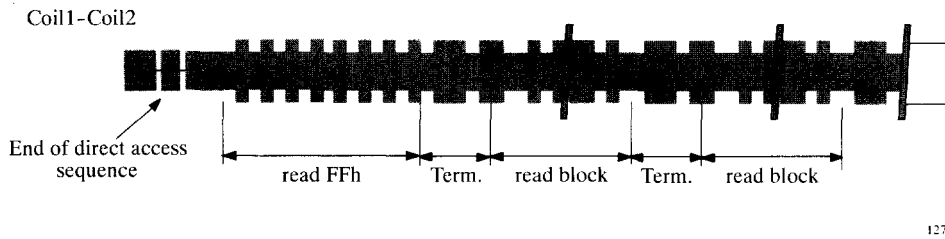


Figure 23. Coil voltage in direct-access mode

4.6.6 Software Reset

To set up the ICs in a defined state, a software reset command can be executed by sending a pseudo block address Fh. The write sequence is shown in figure 25. The Reset command is also accepted during stop mode.

Figure 24. Software reset

4.6.7 Crypto Mode

The crypto mode enables the high-security authentication of the e5561. For this purpose, a certified algorithm called AUT64 is used. The crypto-mode write sequence is shown in figure 26. After the OP code '01', the challenge is sent to the e5561 (LSB first).

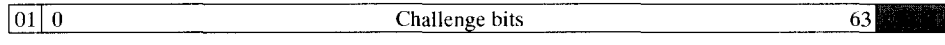


Figure 25. Crypto mode write sequence

After the write sequence, the AUT64-algorithm is started. The computation of the response takes about 30/10 ms (125 kHz). During this time, a checksum - the number of the challenge bits set to '1' - can be read by the base station. Once the response has been computed, the base station can read the response in loop with the terminator 1. This remains until a POR occurs or another gap is detected. The datastream of the crypto-mode is shown in figure 27.

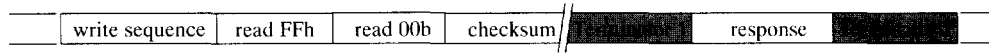


Figure 26. Crypto mode datastream

During the encryption calculation, the checksum is sent in loop with a special pattern (see figure 28). The bits of the checksum are sent with LSB first. If the base station detects an error by comparing the checksum, the calculation of the response can be interrupted by sending a new challenge. This will start the authentication procedure again.

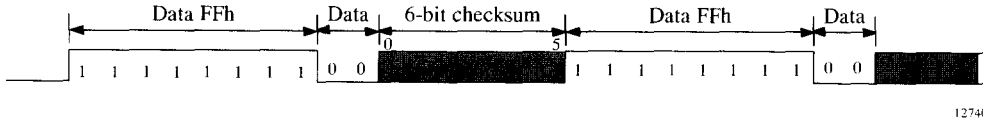


Figure 27. Checksum

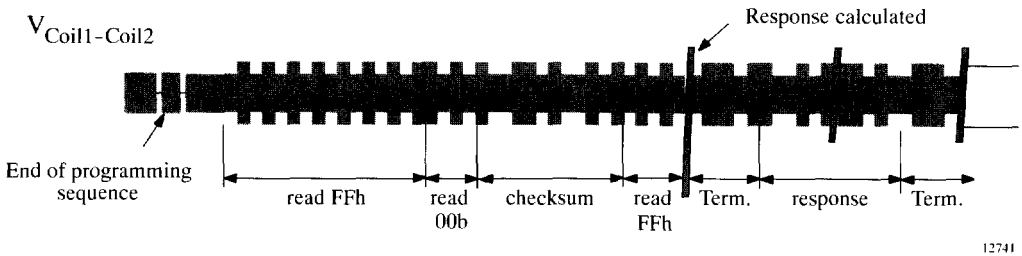


Figure 28. Coil voltage in crypto mode

The encryption time is programmable in two options: The entire algorithm AUT64 is executed 8 or 24 times. This feature can be set at block 0, bit 7.

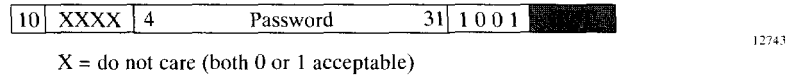
4.6.8 Stop Mode

If several transponders enter the RF field of the base station one after the other (e.g., in a manufactoring step), it might be useful to be able to set the transponder in a passive state. In this case, the transponder may be collected one by one and disabled after being read out. To avoid a communication conflict, the base station has to transmit a special data sequence to the active transponder(s) forcing them to enter the stop mode.

In the stop mode, the e5561 switches off the damping as long as the RF field is applied. After a power-on reset, the e5561 enters the start-up und the ID mode again.

An other possibility to leave the stop mode is to send the software reset (see figure 30). This command results in a new initialization of the IC.

Figure 29. Stop mode data sequence



X = do not care (both 0 or 1 acceptable)

Figure 30. Write sequence to disable password function

4.6.9 Password Function

The password function is a separate protection mechanism to avoid that a base station can read or manipulate the internal configuration and data blocks of the e5561 without knowing the password.

The password function may be used to prevent unauthorized programming or reading via direct-access mode. If the password bit in block 9 of the EEPROM is set, only certain operations are posible, i.e., reading the ID code in ID mode or authentication.

For programming or direct-access mode, the password function has to be disabled by receiving the password.

If this function is enabled, the customer configuration can only be changed by an authorized person using the correct password of the e5561.

During password mode, the e5561 monitors several fault and protection mechanism. If a fault or a protection violation is detected, the e5561 enters the ID mode.

4.7 Error Handling

Several error conditions can be detected to ensure that only valid operations have effect on the e5561.

4.7.1 Errors During Writing Data

There are four detectable errors possible during writing data to the e5561:

- Field gap was not detected
- Wrong number of field clocks between two gaps, e.g., 37 FCs
- The OP code is not valid ('11')
- The number of bits received is incorrect; valid bit counts are:

programming mode	38 bits
direct-access mode	6 bits
crypto mode	66 bits
stop mode	2 bits

If any of these four conditions is detected, the e5561 stops writing and enters ID mode. This can easily be analyzed using the damping which is usually on during writing. It changes according to the selected modulation scheme in ID mode.

4.7.2 Errors During Programming Mode

If the writing sequence has been transmitted successfully, there are three errors that may prevent the e5561 from programming the data to the EEPROM:

- The programming voltage V_{PP} is too low, i.e., the field strength is not high enough
- The lockbit of the adressed block is set
- The password function is enabled

In these cases, the procedure stops immediately after the error is detected and the IC reverts to ID mode.

4.7.3 Errors During Direct-Access Mode

In addition to the possible errors mentioned before, two errors may occur in direct-access mode:

- The lock bit of the addressed block 5 to 8 is set
- The password function is enabled

In these cases, the enters the ID mode after the end of the writing sequence.

4.7.4 Errors During Crypto Mode

In crypto mode, ONE error mechanism is active, that may prevent the e5561 from sending the correct response:

- Error during the crypto writing sequence

The e5561 will enter ID mode immediately if an error in the writing sequence is detected. If the password function is enabled, the e5561 enters ID mode after having completed the writing sequence.

4.7.5 Error Handling in Password Mode

If password function is enabled and the password transmitted does not match the programmed password, the full programming sequence is performed but without programming block 9. This makes it more difficult to find out the correct password by trial and error because in each case the result of the operation can only be recognized after the whole sequence has been processed. This increases the time needed to check a certain number of combinations.

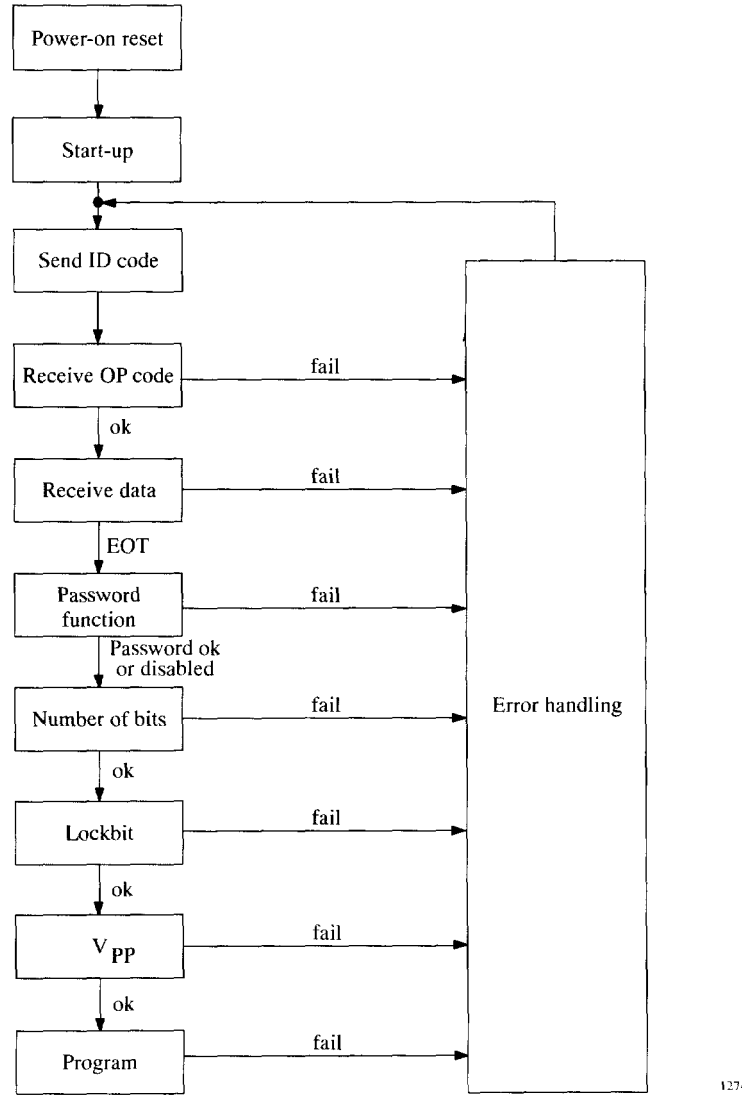


Figure 31. Simplified error handling of the e5561

4.8 Authentication

Especially for applications with high-security demands such as immobilizer systems, the e5561 contains an optimized authentication procedure with the following advantages:

- Secure and fast authentication (< 100 ms)
- Application-optimized high-security algorithm
- Customer-specific generation of unique keys

Therefore, a high-security data transmission and encryption as well as a short authentication time is achieved.

For further information, some additional documentation and programms are available:

- The encryption process of the e5561
- Key generating program
- Algorithm program

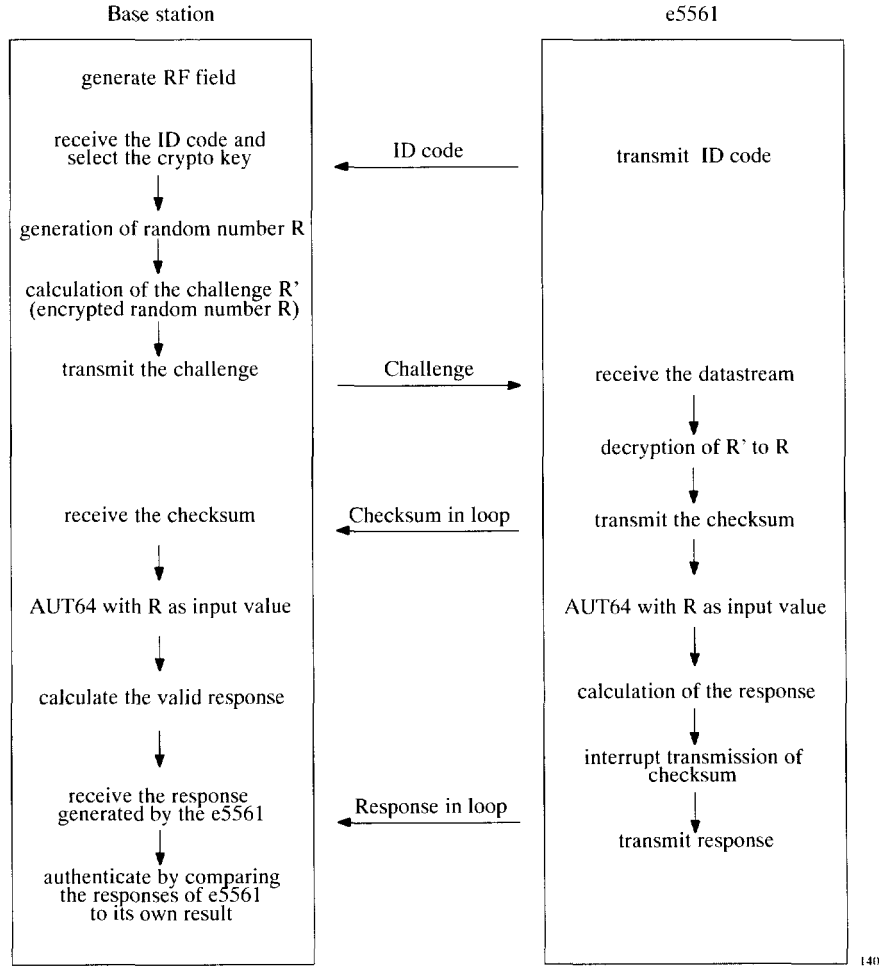


Figure 32. Authentication procedure

4.8.1 Initialization

Before using the e5561 in crypto mode it has to be initialized.

First, the crypto key to be used by the crypto algorithm has to be generated by the key-generating program. This program guarantees that each crypto key is unique, no other e5561 has the same key. This key has to be stored in the memory (block 5 - block 8) of the e5561 via the programming mode. Once the crypto key is locked, it can not be overwritten or read out anymore with direct-access mode.

For correct authentication it is necessary that base station and transponder both use the same key. Therefore, the base station needs to know which transponder is currently in the field. Only then the base station can select the key corresponding to this particular transponder. For this identification the e5561 sends a string of data after it is powered up. This ID code also has to be stored in the e5561.

4.8.2 Starting the Authentication

After power-up the various modes (bitrate, encoding) are read out of block 0. Then, the e5561 transmits the ID code to identify itself. Thereby, the base station can identify the transponder and knows which crypto key to use. The base station forces the e5561 in crypto mode by sending the OP code '01' followed by a 64-bit string, the challenge.

4.8.3 Challenge

The base station generates a 64-bit random number R. This number is the starting value of the actual encryption algorithm. To improve security, this random number is not sent directly to the transponder, but is encrypted by means of a part of the crypto key. The encoded result R' is then transmitted as challenge to the transponder. Once the transponder has received the encoded random number R', it recovers the random number R originally generated by the base station. Both devices, the base station as well as the transponder, then start with the encryption of this number. If the number of received bits is incorrect, the e5561 leaves the crypto mode and enters read mode immediatly, transmitting the ID code.

4.8.4 Checksum

For verification of the received challenge, the e5561 sends a checksum (representing the number of '1' of the challenge) with a special pattern in loop until the encryption is finished (less than 10 ms - optionally 30 ms).

4.8.5 Encryption

For encryption, the optimized high-security algorithm AUT64 is used. The elementary parts of this 64-bit block cipher are transposition and substitution (figure 34). For more detailed information on this algorithm additional documentation is provided. The entire algorithm AUT64 is executed 24 times. At each of these 8/24 times, another key is generated out of the crypto key. Therefore, the algorithm keeps changing and a high-security level is achieved. This is confirmed by statistical analysis.

For more detailed information, the description 'The Encryption Process of the e5561' can be provided.

4.8.6 Response

The 64-bit result of the algorithm is reduced to 32 bits using logical operations. This 32-bit response is sent back to the base station for comparison. If the correct keys were used, the result generated inside the base station is identical to the result sent by the e5561. The response is transmitted in loop including the terminator until the IC is powered by the RF field. This gives the base station enough time for checking the validation of the response.

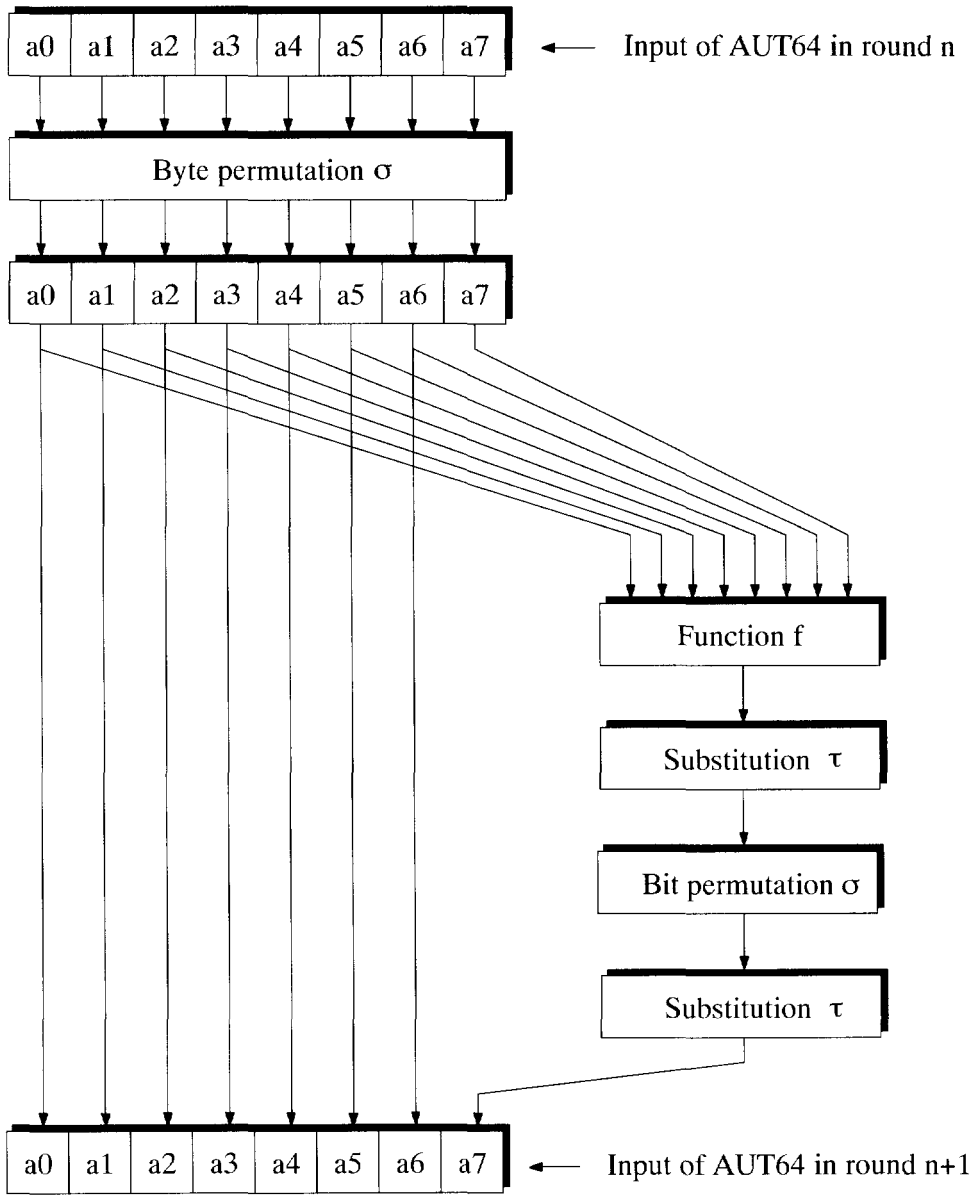


Figure 33. Atmel Wireless & Microcontrollers' crypto algorithm AUT64

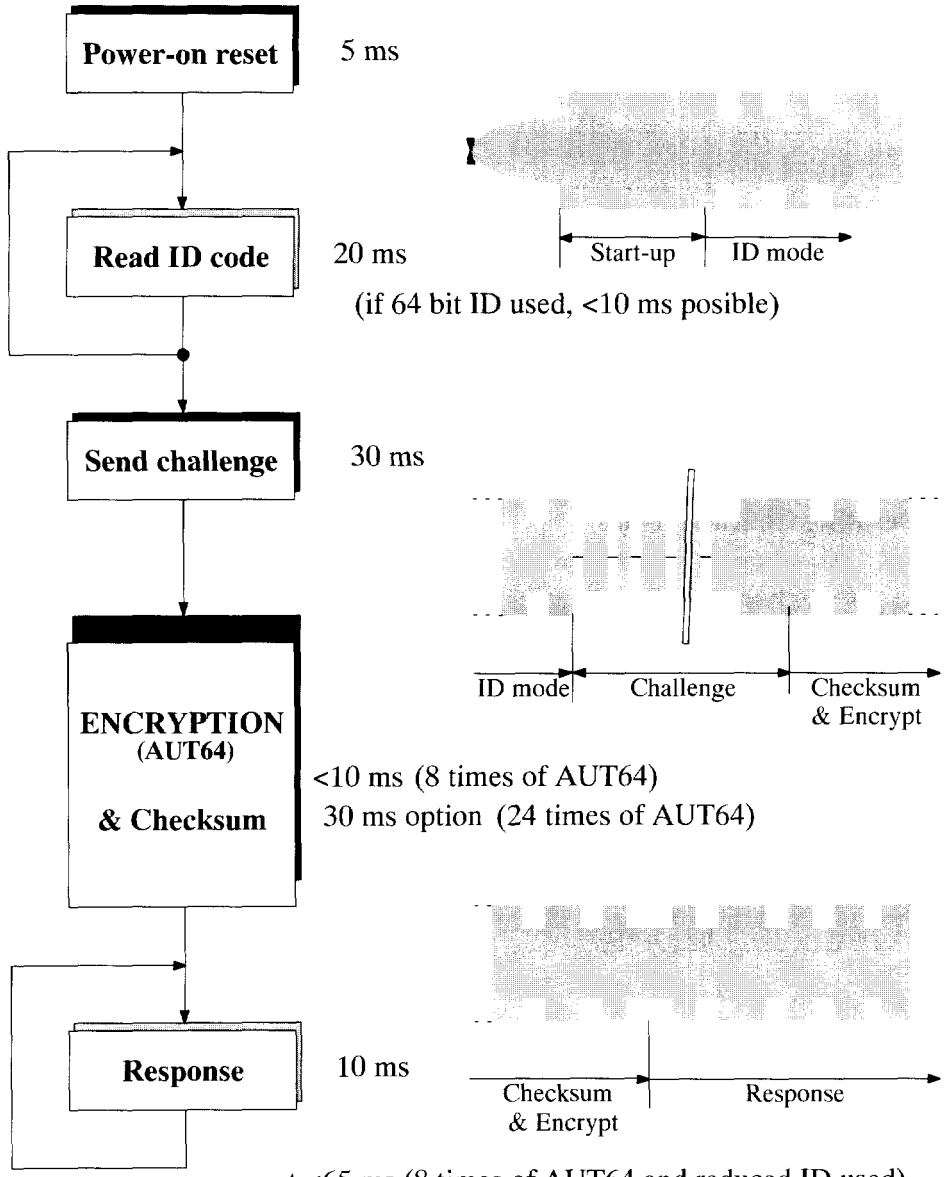


Figure 34. Authentication example

5 Technical Data

5.1 Absolute Maximum Ratings

All voltage are given corresponding to V_{SS}.

Parameters	Symbol	Value	Unit
Supply voltage	V_{DD}	-0.3 to +7.0	V
Input voltage	V_{IN}	V_{SS} -0.3 ≤ V_{IN} ≤ V_{DD} +0.3	V
Current into Coil1/Coil2	$I_{C1/C2}$	10	mA
Power dissipation (dice) (1)	P_{tot}	100	mW
Operating temperature range	T_{amb}	-40 to +85	°C
Storage temperature range (2)	T_{stg}	-40 to +125	°C
Assembly temperature (t ≤ 5 min)	T_{ass}	170	°C

Notes:

(1) Free-air condition. Time of application: 1s
(2) Data retention reduced

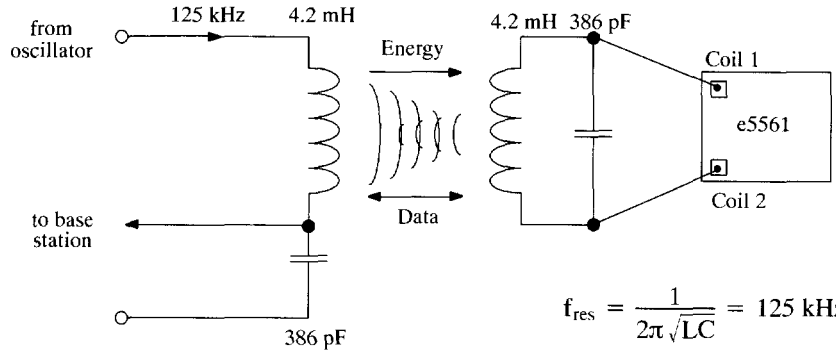
Stresses above those listed under "Absolute Maximum Ratings" may cause permanent damage to the device.

5.2 Operating Characteristics

$T_{ambient}$ = 25°C; reference terminal is V_{SS}; DC operating voltage V_{DD} - V_{SS} = 2 V (unless otherwise noted)

Parameter	Test Conditions	Symbol	Min	Typ	Max	Unit
RF frequency range		f_{RF}	100	125	150	kHz
Supply current	f_{RF} = 125 kHz, read & write	I_{DD}		15		µA
	f_{RF} = 125 kHz, programming	I_{DD}		100		µA
	No clock	I_{DD}	100	250	500	nA
Clamp voltage	Current into Coil1/2 = 5 mA	V_{cl}	7.5	9.0	10.2	V
Equivalent coil input capacitance (without self-adapt)		$C_{1,2}$		30		pF
Programming voltage		V_{PP}	15	16	19	V
Programming time	f_{RF} = 125 kHz	t_{PP}		16		ms
Data retention		$t_{retention}$	10			years
Programming cycles		n_{cycle}	100 000			-
Lowest operating voltage for programming		V_{mfs}	1.8			V

6 Application Example



$$f_{res} = \frac{1}{2\pi\sqrt{LC}} = 125\ \text{kHz}$$