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 Typically 16 ms**
- **Main Options Set by EEPROM:**
  - **Bit Rate [Bit/s]: RF/32, RF/64**
  - **Encoding: Manchester, Bi-phase**

Description

The e5561 is a member of Atmel's IDentification 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 bi-directional data communication (Read/Write) to a base station. Atmel offers an LC circuit and a chip assembled in the 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 cannot be read out.

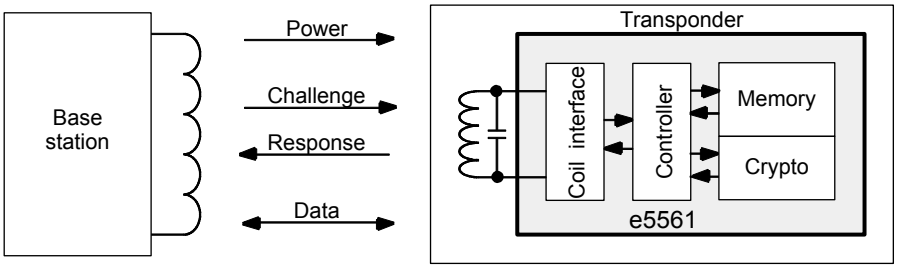
125 kHz is the typical operational frequency of a system using the e5561. Two read data rates are programmable. Reading occurs through damping the incoming RF field with an on-chip load. This damping is detected by the field-generating base station. Data transmission starts after power-up with the transmission of the ID code and continues as long as the e5561 is powered. Writing is carried out with Atmel's 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.

Standard Read/Write Crypto Identification IC

e5561

Rev. 4699A–RFID–04/03

Figure 1. Transponder System Example Using e5561



Internal Modes

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".

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.

ID Mode

During ID mode, the e5561 transmits an identification data stream (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 data stream and the type of modulation depend on the configuration loaded during start-up. The following options are available during ID mode:

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

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 EEPROM blocks. Programming is carried out by sending the programming data sequence to the e5561. When the base station sends data to the transponder, this direction of data transmission will be designated as 'write'.

When 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 data stream 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 switches to ID mode.

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

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 a challenge. Receiving this data sequence causes the e5561 to switch to crypto mode.

This initiates the following actions:

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

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 to 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 switch to stop mode.

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

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

The stop command can be disabled.

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

Password Function

The password function is a separate protection mechanism to prevent a base station from reading or manipulating the internal configuration and data blocks of the e5561 without knowing the password. Only a transition to the crypto mode is possible. If the password function is active, the base station must first send the password to enable any other operations.

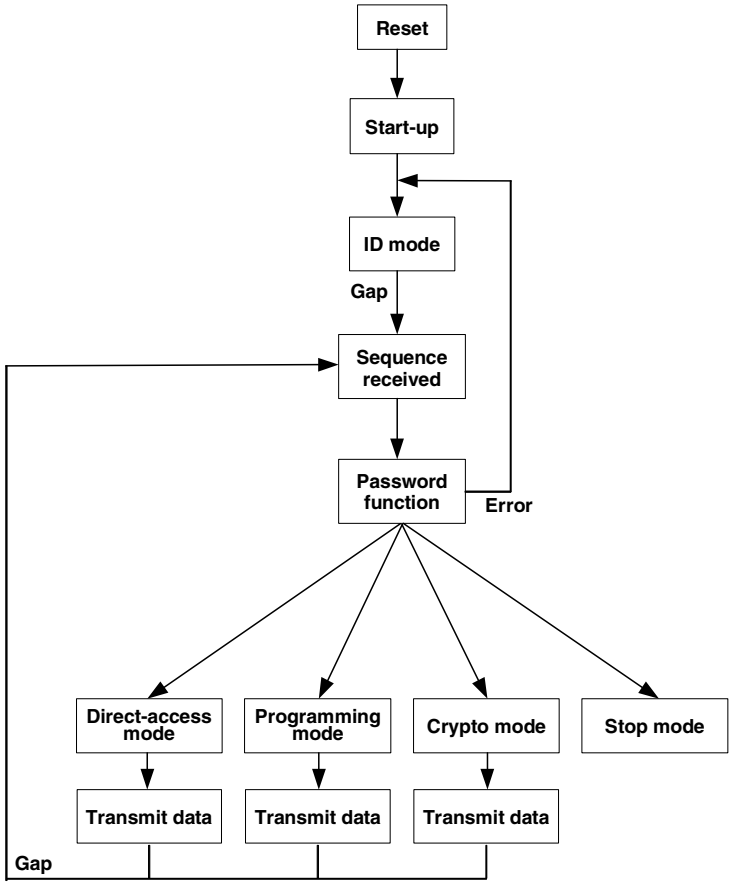
During password mode, the e5561 monitors several fault and protection mechanism. If a fault or a protection violation is detected, the e5561 enters ID mode.

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, switching to another mode is only possible by sending an uncorrect data sequence to the transponder.

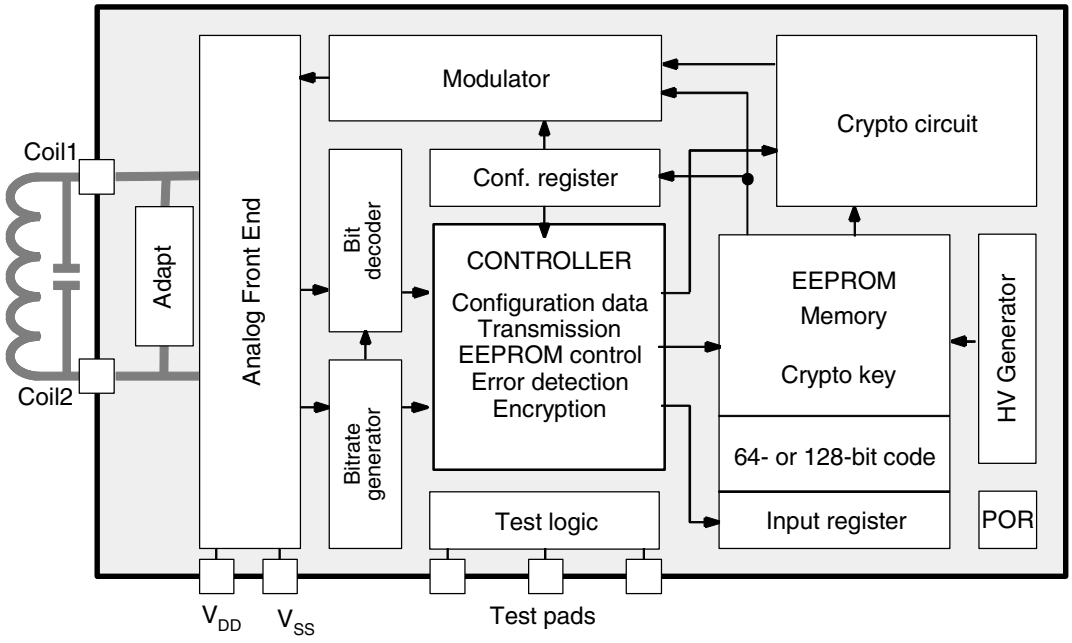
Figure 2. State Diagram of the e5561 (Overview)



Note: This diagram provides only an overview. In reality, more transitions are possible.

Building Blocks

Figure 3. Block Diagram



Analog Front End (AFE)

The AFE includes all circuits directly connected to the coil. It generates the IC's power supply and handles the bi-directional 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)

Controller

The controller has the following functions:

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

Power-On Reset (POR)

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

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).

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 the adaptation function is carried out automatically every time the e5561 enters the RF field or when the EEPROM is read out. This depends on a control bit. The automatic adaptation stops when the optimized adaptation has been reached. This 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 the start-up phase by the IC itself, it is possible to set the adapt bits in the EEPROM manually.

Before carrying out the manual setting of the adapt bits, bit A in block 0 must be set to 1 (see Figure 8).

The content of these 3 bits, that need to be defined, determines the transponder's response frequenzy in a limited range.

Bits are set by programming block 0 in the microcontroller.

Bit-rate Generator

The bit-rate generator can deliver bit rates of RF/32 and RF/64 for data transmission from the e5561 to the base station.

Bit Decoder

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

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
- Bi-phase
  - Every bit creates a change, a data 0 creates an additional mid-bit change

  By using Bi-phase modulation, data transmission always starts with damping on.

HV Generator

The HV generator is a voltage pump which generates about 18 V for programming the EEPROM.

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.

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

- Type of modulation and bit rate
- Length of ID code
- Several lock-bits
- Terminator set

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

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

Figure 4. Types of Modulation

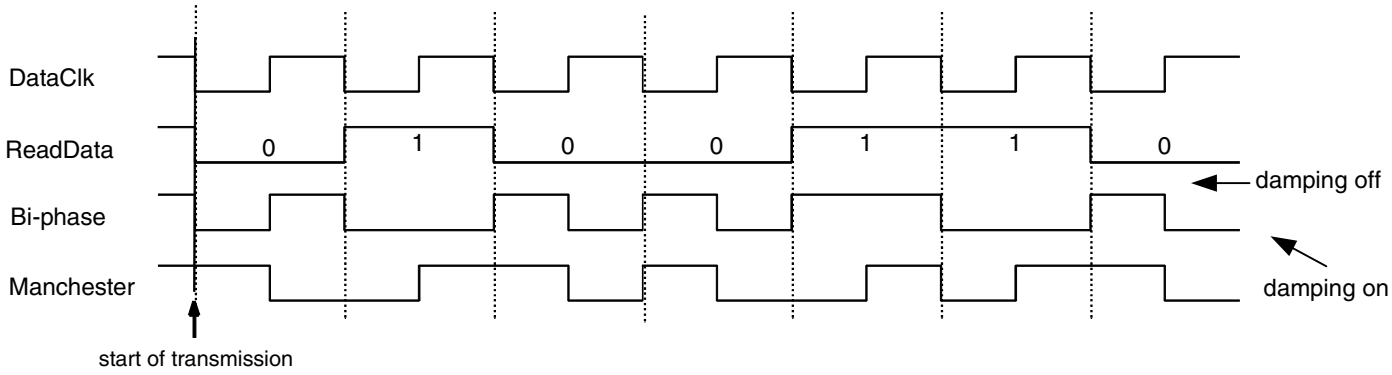
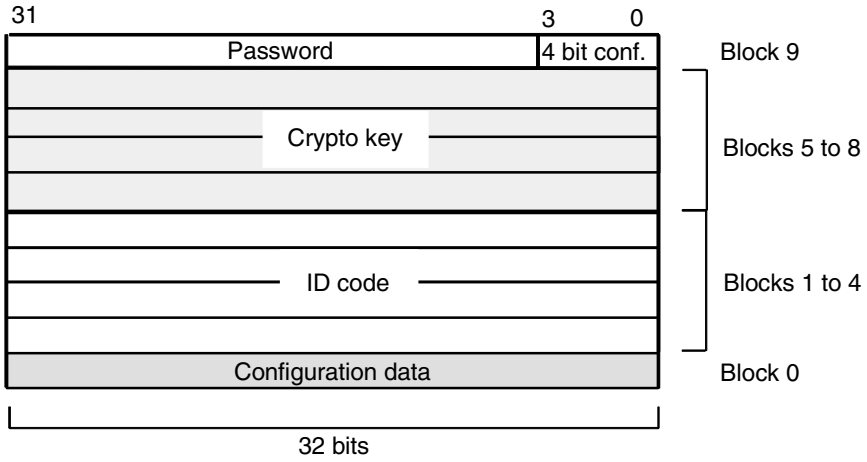


Figure 5. Memory Map



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 out 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 blocks 5 to 8 of the EEPROM and can be locked by the user to avoid read out or changes.

Protection Mechanisms

Several protection mechanisms are implemented into the e5561. These are mainly:

- 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.

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.

Lock-bit Protection

A lock-bit is a physical part of the EEPROM's content and is under user control. The lock-bit 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 the direct-access mode

If the base station tries to read out the crypto key and the corresponding lock-bit is set, the e5561 will enter ID mode immediately. Once the crypto key lock-bit is set, the crypto key can not be modified or read out any more.

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

- Lock-bits to inhibit programming of the specified blocks of the EEPROM
- Lock-bits 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 lock-bit will cause an error handling procedure (i.e., the e5561 enters ID mode)

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.

Operating the e5561

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 the 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 blocks 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.

Supply

The e5561 is supplied via a tuned LC circuit which is connected to 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.

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. When the adaptation has been carried out, the e5561 enters ID mode immediately if terminator 2 is selected, otherwise, a data value of Fh in the selected configuration (modulation, bit rate) is sent followed by the optionally specified terminator 1 (see Figure 8).

Figure 6. Application Circuit

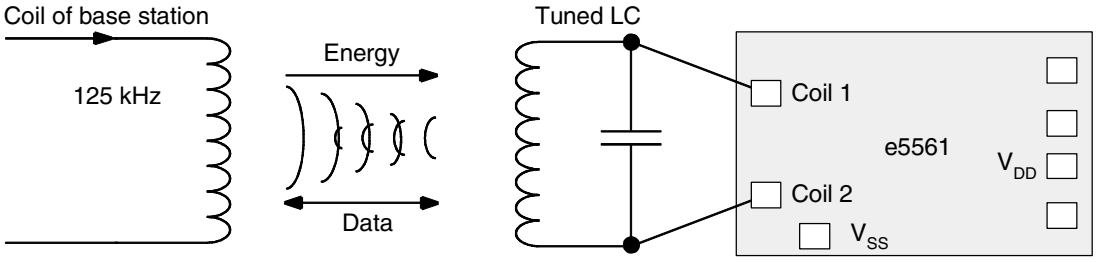
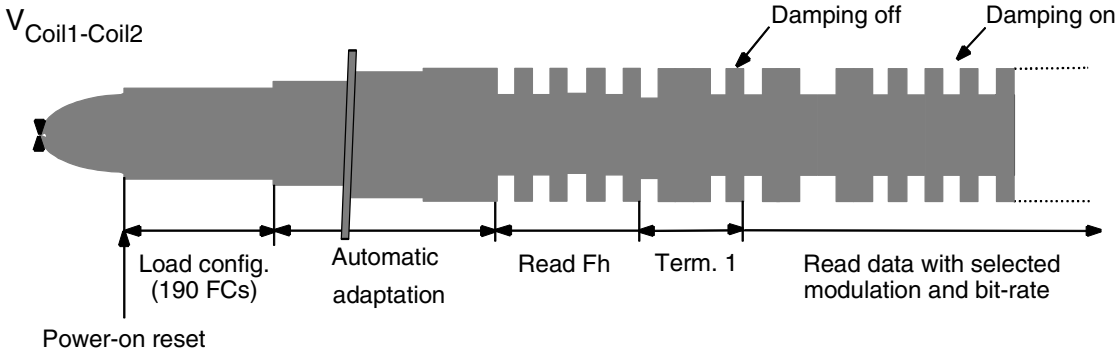


Figure 7. Voltage at Coil1/Coil2 after Start-up (e.g., RF/32, Manchester, Terminator 1)



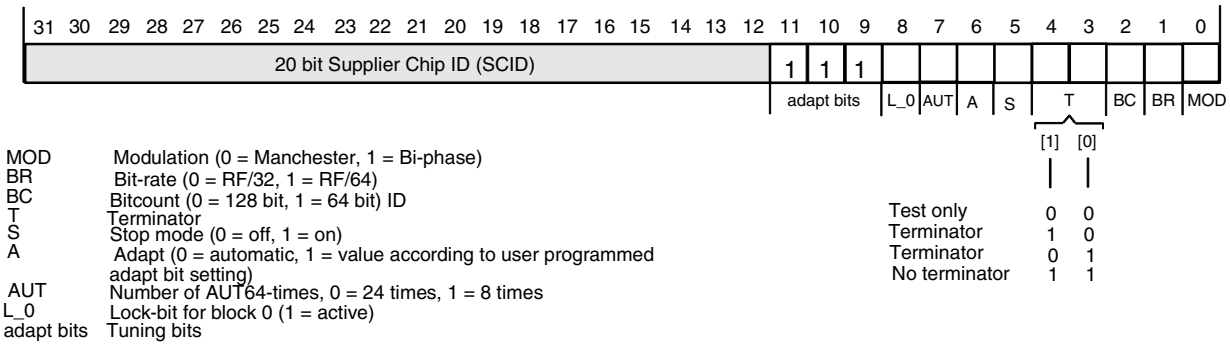
Configuration

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 bit rate
- ID code length
- Several lock-bits
- 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 lock-bit L_0 in block 0 has not been set.

Figure 8. Configuration Data in Block 0

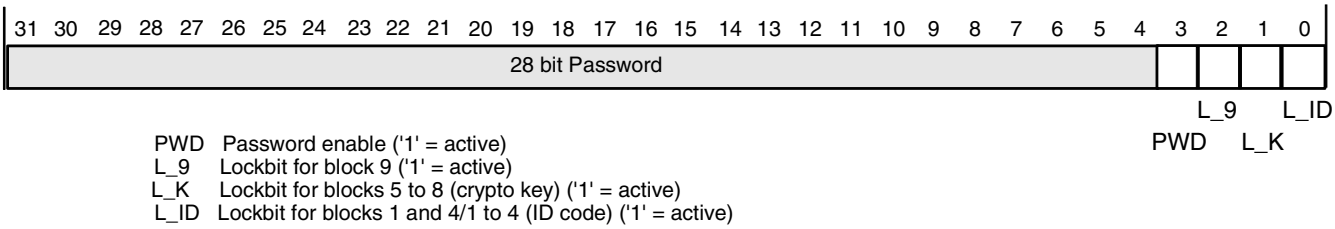


Block 9 contains the customer configuration and the password (if password function is enabled). The customer-configuration data in block 9 includes (see Figure 10):

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

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

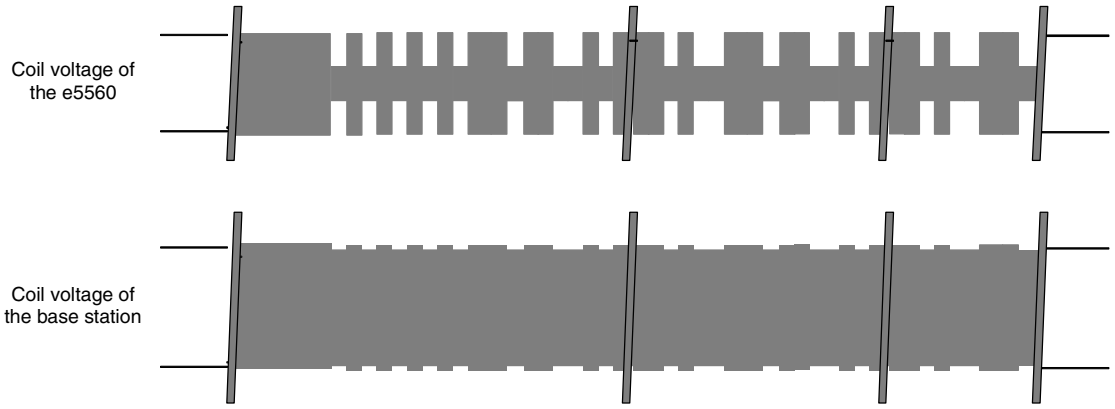
Figure 9. Customer Configuration Data in Block 9



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



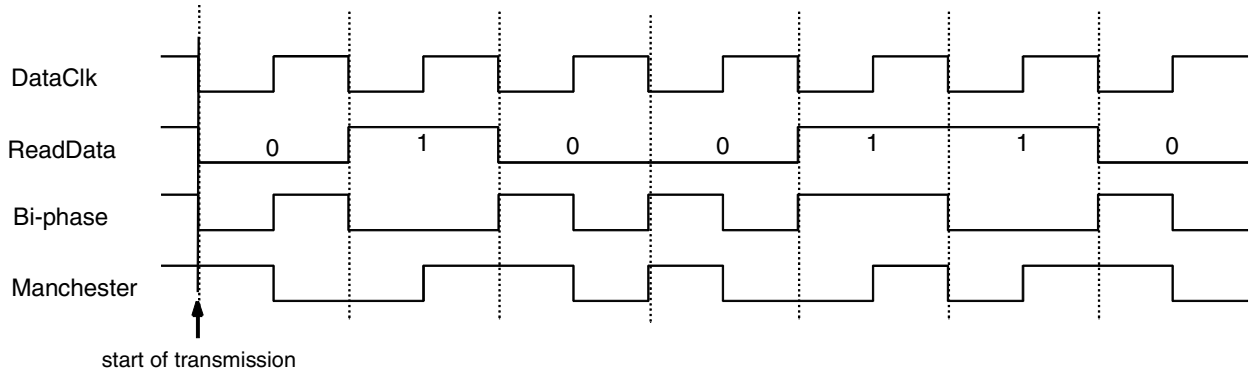
ID Mode

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

Modulation and Bit Rate

The different bit rates and modulations of the e5561 can be selected using the appropriate bit in block 0. Available bit rates are RF/32 and RF/64; the e5561 provides Bi-phase and Manchester modulation.

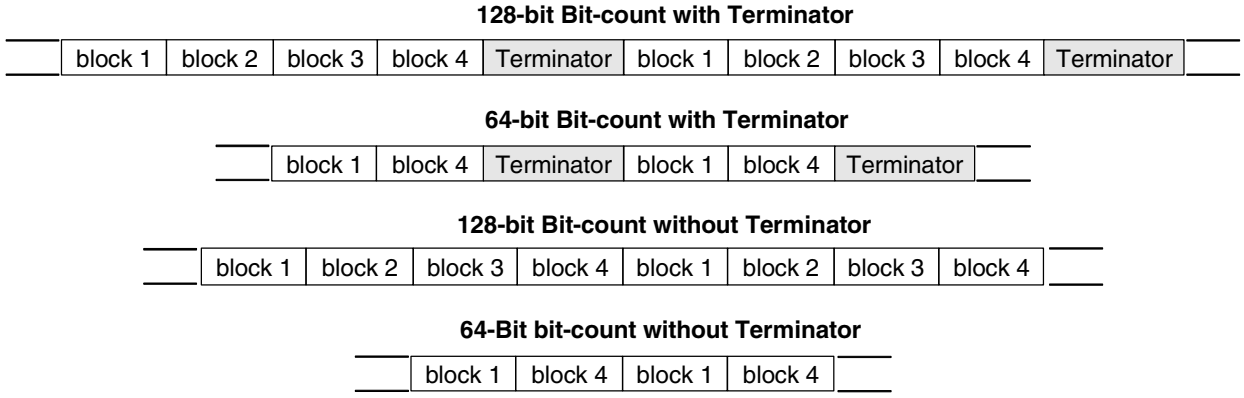
Figure 11. Types of Modulation



Data Streams

Reading begins with block 1 (LSB first). Depending on the selected bit count, block 1 is followed by block 2, 3 and 4 (128-bit bit count) or just by block 4 (64-bit bit count). 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 12.

Figure 12. ID Mode Data Streams

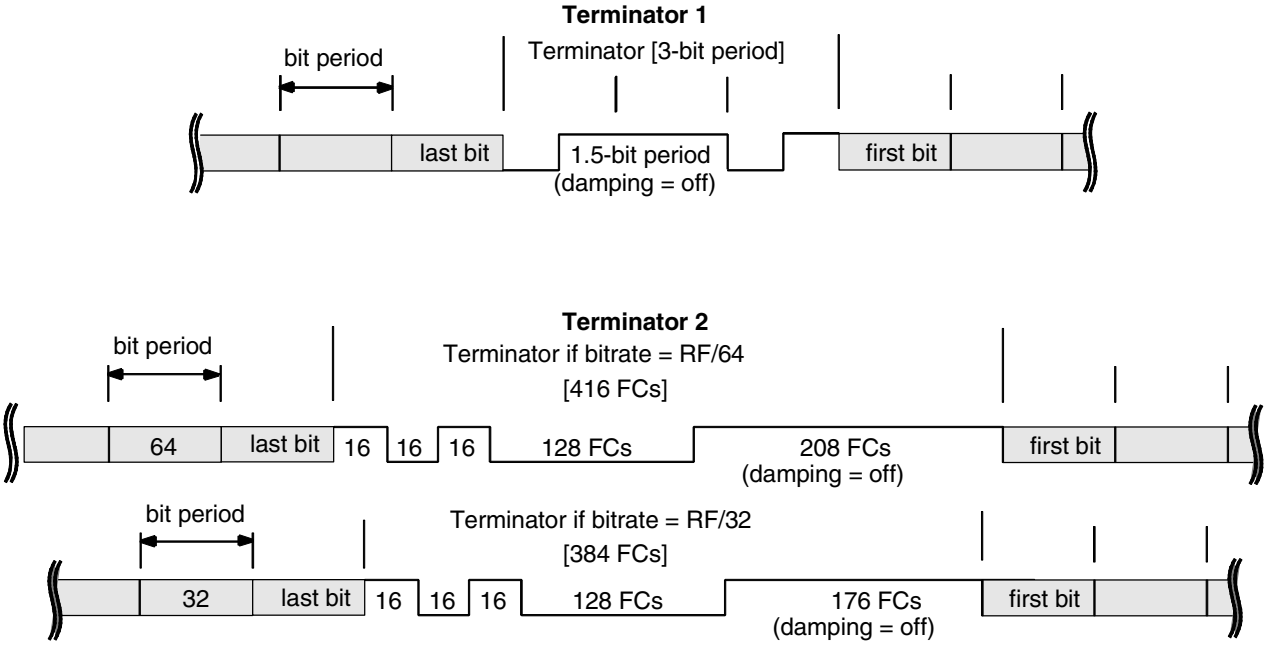


Terminators

Terminators are a special pattern to mark the beginning and the end of a 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 Bi-phase modulation is used).

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

Figure 13. Terminators



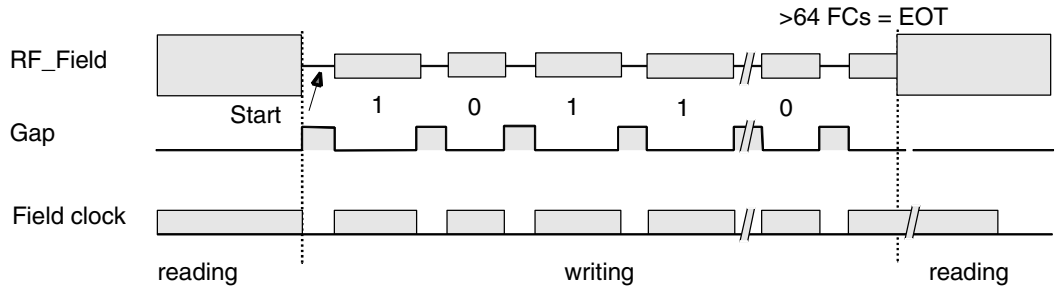
Data Transmission to the e5561 (Write)

Data transmission from the base station to the e5561 is carried out by using Atmel's 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.

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 approximately 2 ms).

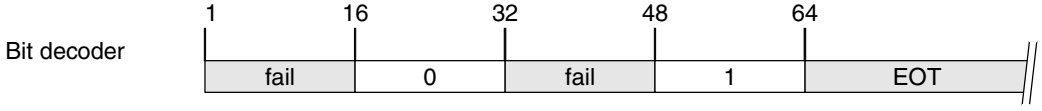
Figure 14. Signals to the Transponder During Writing



Bit Decoder

The duration of the gaps is usually 50 µs to 150 µs. 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 section "Error handling").

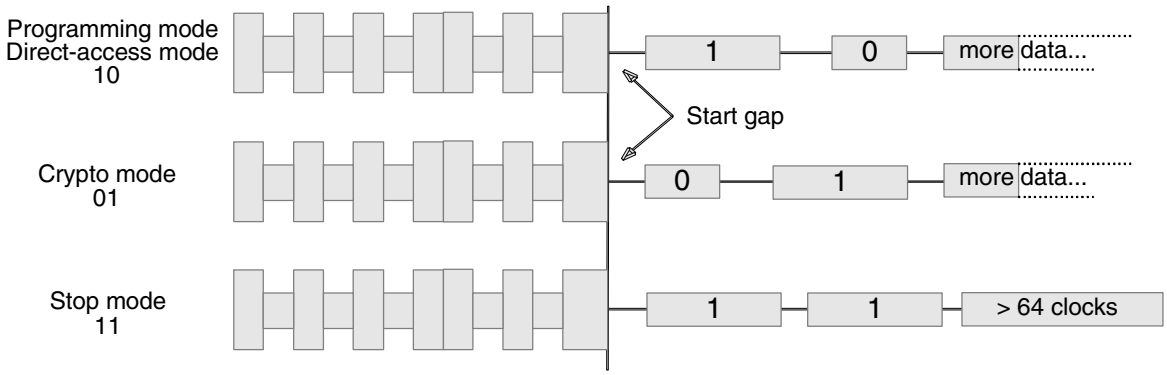
Figure 15. Bit Decoding Scheme (Number of FCs Between Two Consecutive Gaps)



OPcodes

The OPcode 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 OPcodes: 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 OPcode '00' disables modulation until a POR occurs.

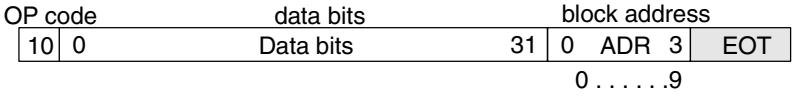
Figure 16. OP Codes



Programming Mode

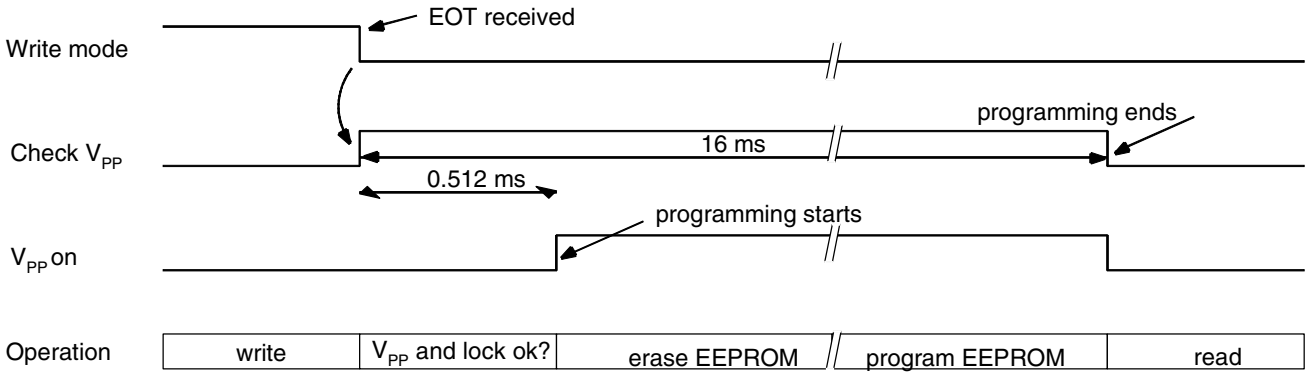
Programming the EEPROM of the e5561 is carried out blockwise, i.e., every single block has to be programmed separately. The programming-mode write sequence is shown in Figure 17. After OPcode 10, the 32 data bits have to be sent followed by the four address bits specifiying the block to be programmed (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 has been 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 lock-bit for the block to be programmed is examined. Further, V_{PP} is continually monitored throughout the programming cycle. If V_{PP} 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

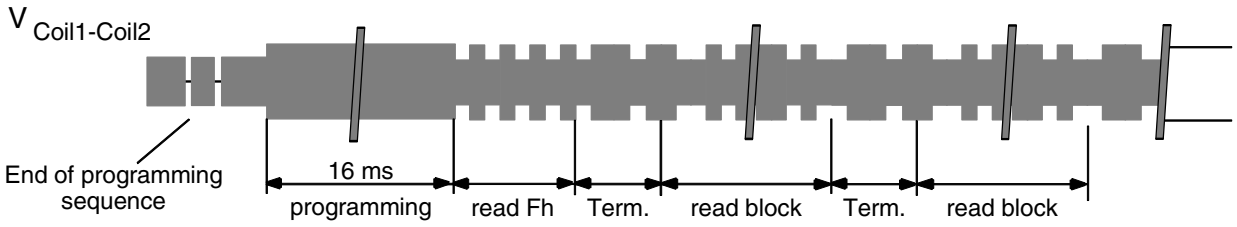


After programming has been carried out, the e5561 sends an Fh preburst followed by terminator 1. After that, the data just programmed is read out of the EEPROM and sent in loop with terminator 1. This enables the base station to detect a malprogramming by comparing the data transmitted with the data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

Figure 19. Programming Mode Data Stream



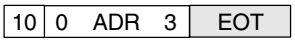
Figure 20. Coil Voltage in Programming Mode



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 21. Following the OPcode 10, the address of the block to be read has to be sent (LSB first).

Figure 21. Direct-access Mode Write Sequence



It is always possible to read the content of block 0 and the four blocks of the ID code. The blocks containing the crypto-key (blocks 5 to 8) can only be accessed when the corresponding lock-bit 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 terminator 1. After that, the addressed block and terminator 1 are sent in loop.

Figure 22. Direct-access Mode Data stream

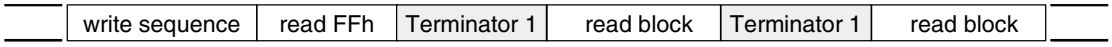
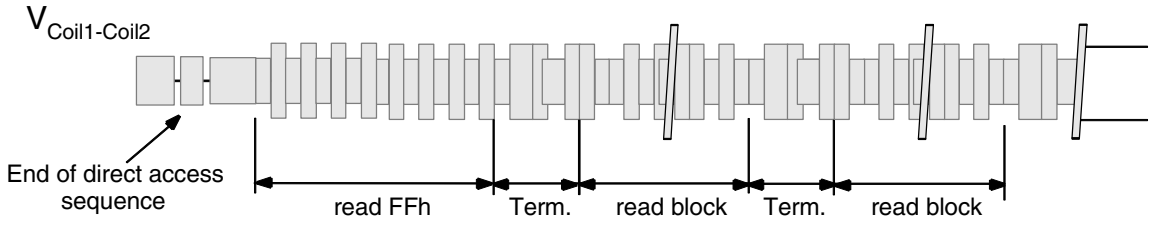


Figure 23. Coil Voltage in Direct-access Mode



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

10	1	1	1	1	EOT

Crypto Mode

The crypto mode enables a 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 25. After the OPcode 01, the challenge is sent to the e5561 (LSB first).

Figure 25. Crypto Mode Write Sequence

01	0	Challenge bits	63	EOT

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 data stream of the crypto mode is shown in Figure 26.

Figure 26. Crypto Mode Datastream

	write sequence	read FFh	read 00b	checksum	Terminator 1	response	Terminator 1

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

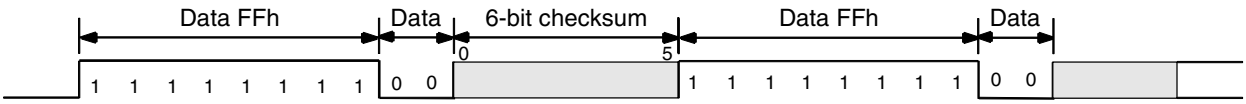
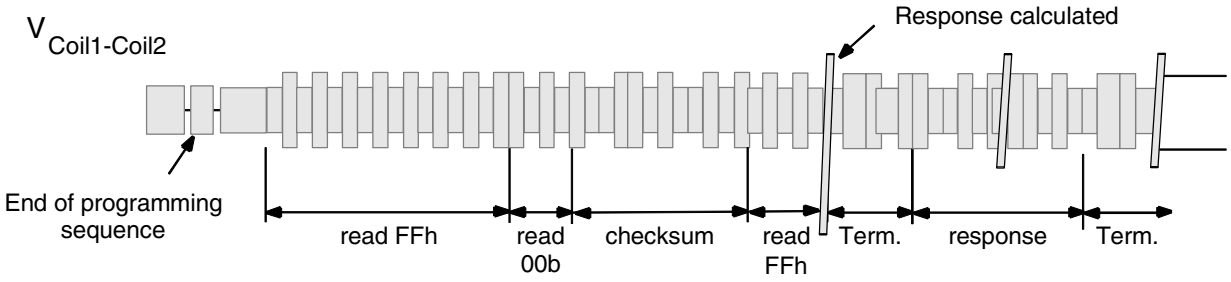


Figure 28. Coil Voltage in Crypto Mode



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.

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.

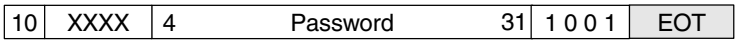
During stop mode, the e5561 switches off the damping as long as the RF field is applied. After a power-on reset, the e5561 enters the start-up and the ID mode again.

An other possibility to exit 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



Figure 30. Write Sequence to Disable Password Function



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

Password Function

The password function is a separate protection mechanism to prevent that a base station from reading or manipulating 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 ID mode.

Error Handling

Several error conditions can be detected to ensure that only valid operations affect the e5561.

Errors while 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 OPcode 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.

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 lock-bit of the adressed block is set
- The password function is enabled

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

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 IC enters ID mode after the end of the writing sequence.

Errors During Crypto Mode

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

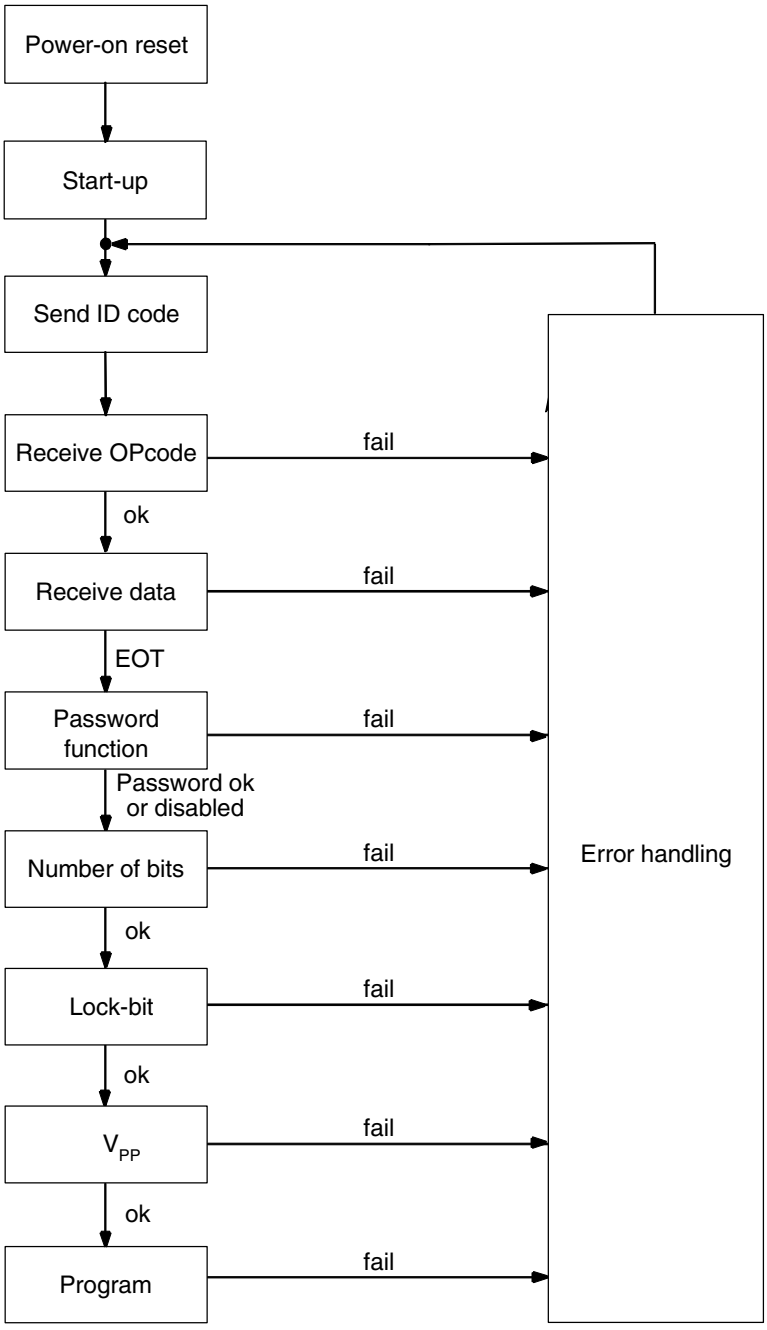
- Error during the crypto writing sequence

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.

Error Handling During 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



Authentication

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

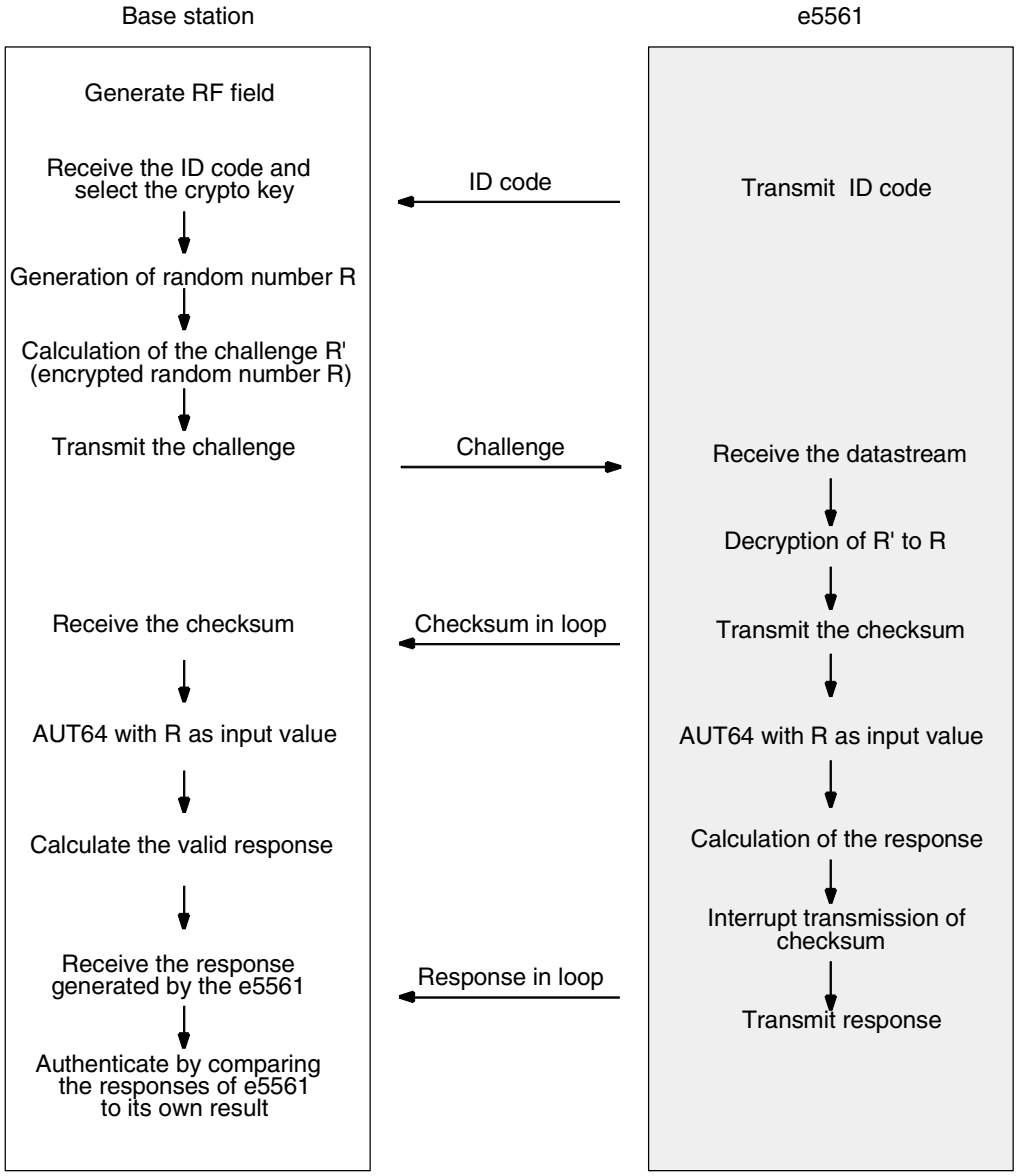
- Secure and fast authentication (< 100 ms)
- Application-optimized high-security algorithm
- Customer-specific generation of unique keys

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

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

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

Figure 32. Authentication Procedure



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 over-written 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 has been powered up. This ID code must also be stored in the e5561.

Starting the Authentication

After power-up the various modes (bit rate, 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 into crypto mode by sending the OPcode 01 followed by a 64-bit string, the challenge.

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.

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).

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.

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 to check the validation of the response.

Figure 33. Atmels' Crypto Algorithm AUT64

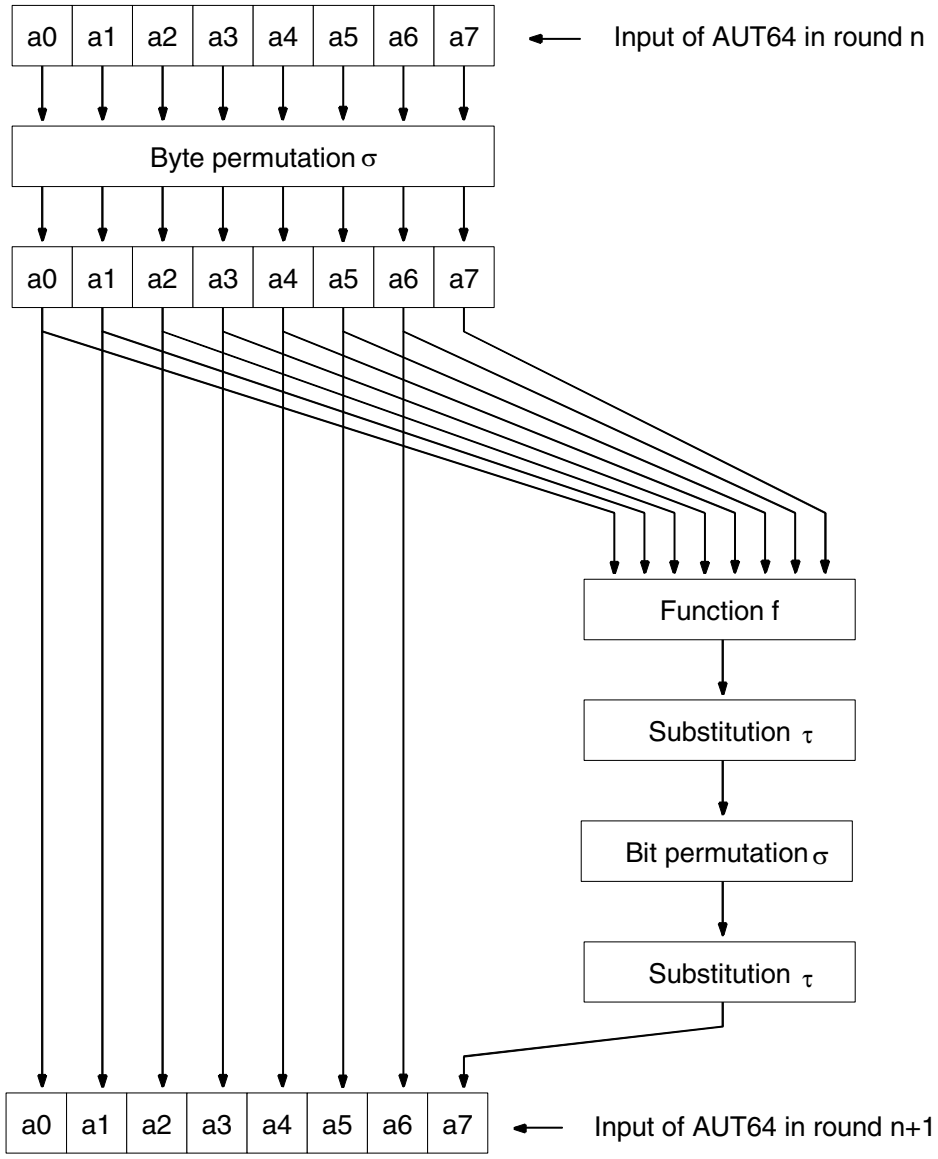
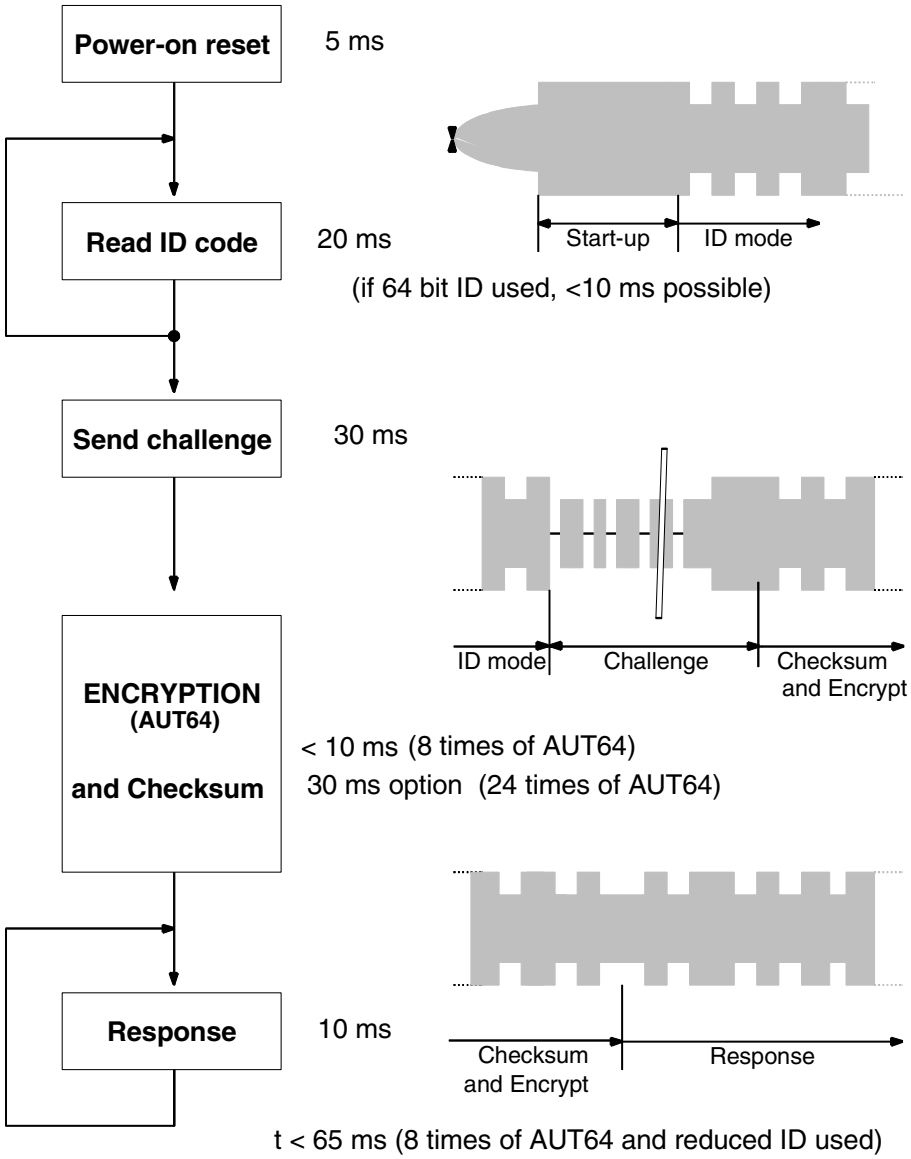


Figure 34. Authentication Example



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: 1 s.
2. Data retention reduced.

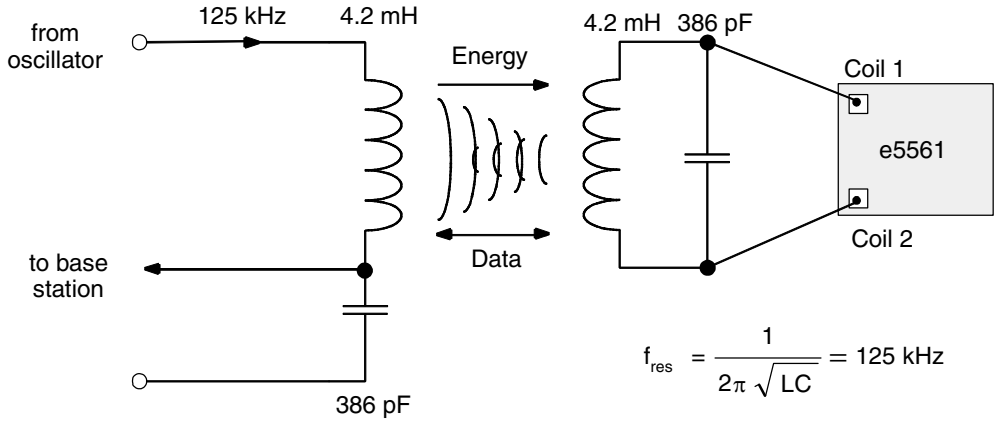
Stresses above those listed under "Absolute Maximum Ratings" may cause permanent damage to the device.

Operating Range

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

Parameters	Test Conditions	Symbol	Min.	Typ.	Max.	Unit
RF frequency range		f_{RF}	100	125	150	kHz
Supply current	f_{RF} = 125 kHz, read and 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/Coil2 = 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

Figure 35. Application Example



Ordering Information

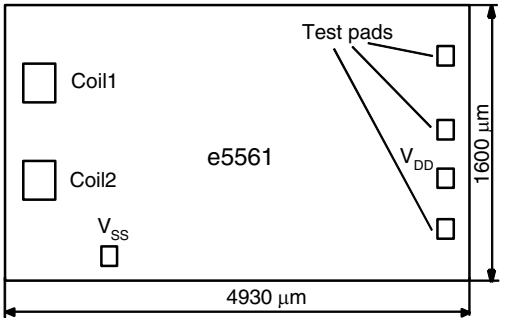
Extended Type Number	Package	Remarks
e5561A-DOW	DOW	–

Pads

Name	Pad Window	Function
Coil1	136 × 136 m^2	1st coil pad
Coil2	136 × 136 m^2	2nd coil pad
V_{DD}	78 × 78 m^2	Positive supply voltage
V_{SS}	82 × 82 m^2	Negative supply voltage (GND)

Note: For normal (coil-driven) operation, the e5561 needs only Coil1 and Coil2.

Chip Dimensions



Atmel Headquarters

Corporate Headquarters
2325 Orchard Parkway
San Jose, CA 95131
TEL 1(408) 441-0311
FAX 1(408) 487-2600

Europe
Atmel Sarl
Route des Arsenaux 41
Case Postale 80
CH-1705 Fribourg
Switzerland
TEL (41) 26-426-5555
FAX (41) 26-426-5500

Asia
Room 1219
Chinachem Golden Plaza
77 Mody Road Tsimhatsui
East Kowloon
Hong Kong
TEL (852) 2721-9778
FAX (852) 2722-1369

Japan
9F, Tonetsu Shinkawa Bldg.
1-24-8 Shinkawa
Chuo-ku, Tokyo 104-0033
Japan
TEL (81) 3-3523-3551
FAX (81) 3-3523-7581

Atmel Operations

Memory
2325 Orchard Parkway
San Jose, CA 95131
TEL 1(408) 441-0311
FAX 1(408) 436-4314

Microcontrollers
2325 Orchard Parkway
San Jose, CA 95131
TEL 1(408) 441-0311
FAX 1(408) 436-4314

La Chantrerie
BP 70602
44306 Nantes Cedex 3, France
TEL (33) 2-40-18-18-18
FAX (33) 2-40-18-19-60

ASIC/ASSP/Smart Cards
Zone Industrielle
13106 Rousset Cedex, France
TEL (33) 4-42-53-60-00
FAX (33) 4-42-53-60-01

1150 East Cheyenne Mtn. Blvd.
Colorado Springs, CO 80906
TEL 1(719) 576-3300
FAX 1(719) 540-1759

Scottish Enterprise Technology Park
Maxwell Building
East Kilbride G75 0QR, Scotland
TEL (44) 1355-803-000
FAX (44) 1355-242-743

RF/Automotive
Theresienstrasse 2
Postfach 3535
74025 Heilbronn, Germany
TEL (49) 71-31-67-0
FAX (49) 71-31-67-2340

1150 East Cheyenne Mtn. Blvd.
Colorado Springs, CO 80906
TEL 1(719) 576-3300
FAX 1(719) 540-1759

Biometrics/Imaging/Hi-Rel MPU/
High Speed Converters/RF Datacom
Avenue de Rochepleine
BP 123
38521 Saint-Egreve Cedex, France
TEL (33) 4-76-58-30-00
FAX (33) 4-76-58-34-80

---

e-mail
literature@atmel.com

Web Site
http://www.atmel.com

© Atmel Corporation 2003.
Atmel Corporation makes no warranty for the use of its products, other than those expressly contained in the Company's standard warranty which is detailed in Atmel's Terms and Conditions located on the Company's web site. The Company assumes no responsibility for any errors which may appear in this document, reserves the right to change devices or specifications detailed herein at any time without notice, and does not make any commitment to update the information contained herein. No licenses to patents or other intellectual property of Atmel are granted by the Company in connection with the sale of Atmel products, expressly or by implication. Atmel's products are not authorized for use as critical components in life support devices or systems.

Atmel® is the registered trademark of Atmel.

IDIC® stands for IDentification Integrated Circuit and is a registered trademark of Atmel Germany GmbH.

Other terms and product names may be the trademarks of others.

Printed on recycled paper.

4699A–RFID–04/03 xM