Crypto Contactless Identification Device

Features

- On Chip Crypto-Algorithm
- Two Way Authentication protocol
- 96 bits of Secret-Key in EEPROM (unreadable)
- 32 bits of fix Device Identification
- 30 bits of USER_MEMORY (UM) with read access (OTP)
- Secret-Key programmable via CID-Interface
- Lock-Bits to inhibit programming
- Data Transmission performed by Amplitude Modulation
- Bit Period = 32 periods of carrier frequency
- 200 pF on chip Resonant Capacitor (untrimmed)
- -40 to +85°C Temperature range
- 115 kHz TO 135 kHz Field Frequency
- On chip Rectifier and Voltage Limiter
- No external supply buffer capacitance needed due to low power consumption

Typical Operating Configuration

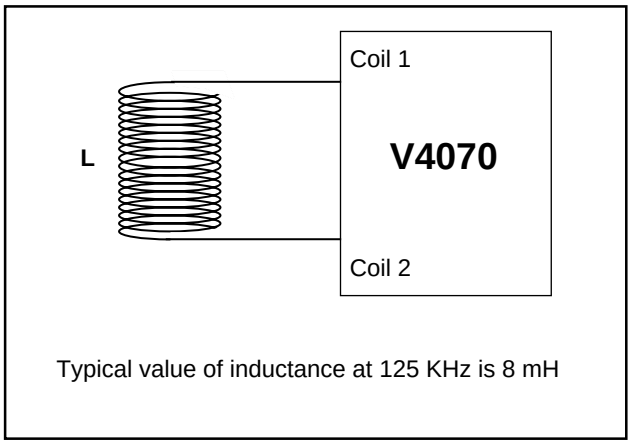

Figure 1

Description

The V4070 is a CMOS integrated circuit intended for use in electronic Read/Write RF Transponders. The chip contains an implementation of a crypto-algorithm with 96 Bits of user configurable secret-key contained in EEPROM. It also provides a unique Device Identification of 32 Bits that can never be modified as well as 30 Bits of freely programmable USER-MEMORY. Bits 15 and 14 of word 1 are used as Lock-Bits. The memory can only be accessed for writing or erasing if these two bits have the contents «10» as when they are delivered.

The V4070 transmits data to the transceiver by modulating the amplitude of the electromagnetic field, and receives data and commands in a similar way.

The coil of the tuned circuit is the only external component required, all remaining functions are integrated in the chip.

Pin Assignment

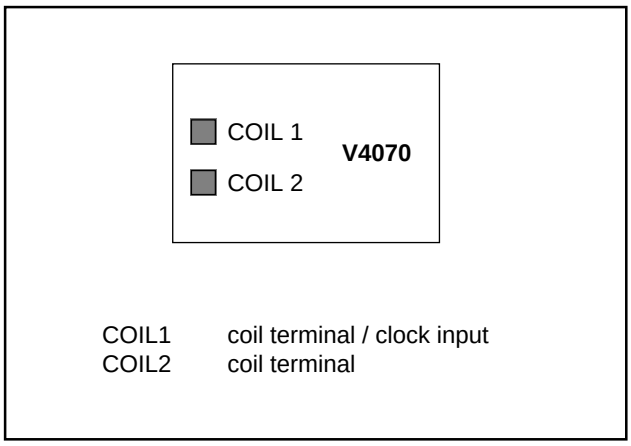

Figure 2

Applications

- High security automotive immobilizer
- High security hands-free access control

A COMPANY OF THE SWATCH GROUP

Absolute Maximum Ratings

Parameter	Symb.	Min.	Max.	Unit
Supply voltage	V_{DD}	-0.3	9.5	V
Voltage at remaining pins	V_{pin}	V_{SS} - 0.3	V_{DD} + 0.3	V
Storage temp.	T_{store}	-55	125	°C
Operating temp.	T_{op}	-40	85	°C
Maximum AC peak Current induced on COIL1 and COIL2	I_{COIL}	-30	30	mA

Table 1

Stresses above these listed maximum ratings may cause permanent damage to the device. Exposure beyond specified electrical characteristics may affect device reliability or cause malfunction.

Handling Procedures

This device has built-in protection against high static voltages or electric fields; however, anti-static precautions should be taken as for any other CMOS component. Unless otherwise specified, proper operation can only occur when all terminal voltages are kept within the supply voltage range.

System Principle

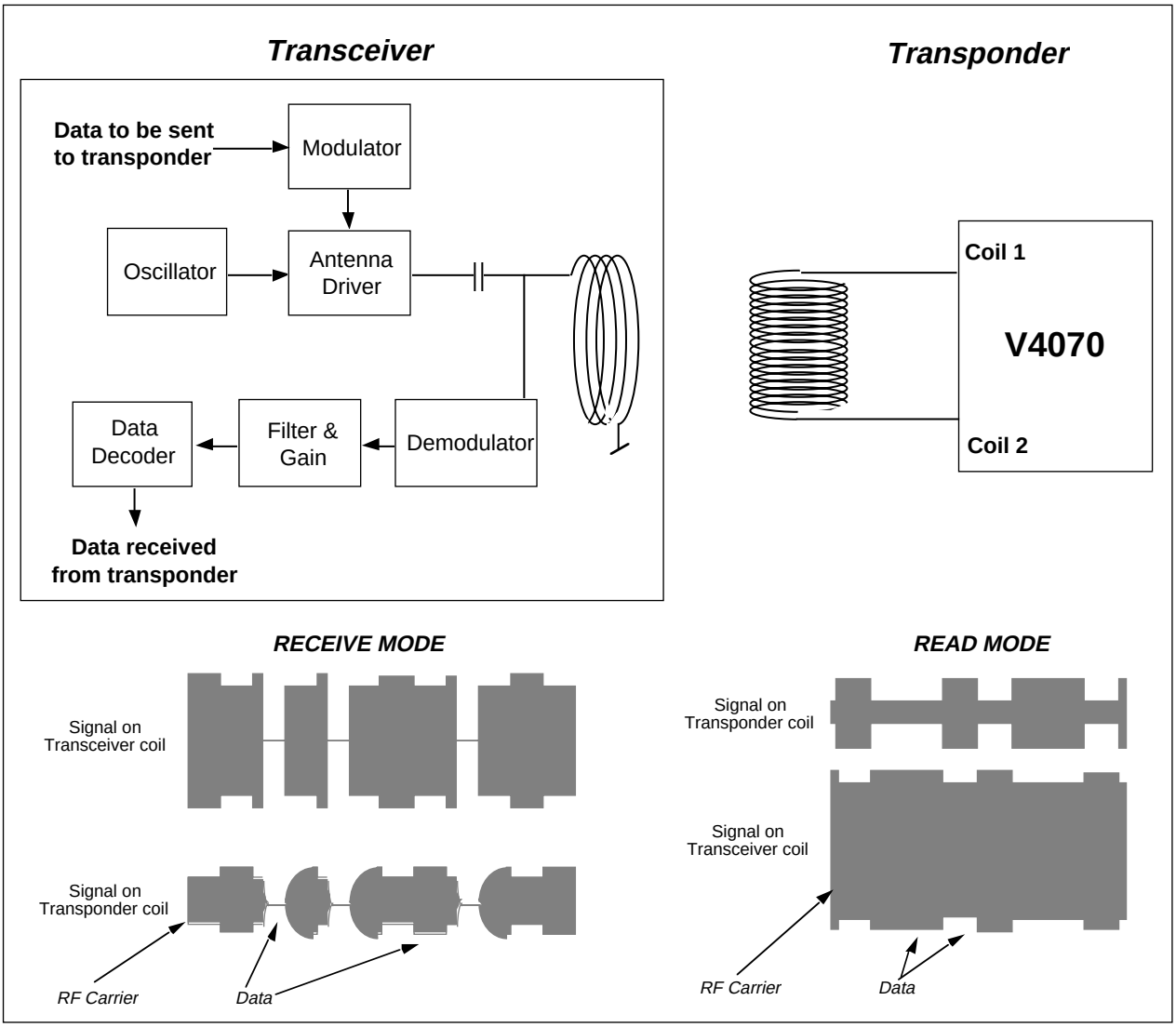

Figure 3

Electrical Characteristics

Operating Conditions

V_{DD} = 2.5V V_{SS} = 0V f_{coil} = 125 kHz Sine wave V_{coil} = 1Vpp T_{op} = 25°C

Parameter	Symbol	Conditions	Min.	Typ.	Max.	Unit
Supply voltage	V_{DD}	Read Mode	2		1)	V
EEPROM write voltage	V_{EE}		3			V
Supply current/read	I_{rd}	Read Mode V_{DD}=2.0V			5	µA
Supply current/read/H	I_{rdH}	Read Mode V_{DD}=5.0V			10	µA
Supply current/write	I_{wr}	Write Mode V_{DD}=3.0V -40°C<T<85°C			50	µA
Supply current/write/H	I_{wrH}	Write Mode V_{DD}=5.0V			80	µA
Modulator voltage drop	V_{ON}	$V_{(Coil1-VSS)}$ & $V_{(Coil2-VSS)}$ Icoil = 100µA			0.5	V
		$V_{(Coil1-VSS)}$ & $V_{(Coil2-VSS)}$ Icoil = 5mA			2.5	V
Resonance capacitor	C_r		170	200	230	pF
Capacitor temp. coeff	TK_{Cr}	-40°C to 85°C	-75		75	ppm/K
Capacitor tolerance/wafer	TOL_{Cr}		-2		2	%
POR level high	V_{prh}	Rising supply		2.2	2.8	V
Clock extractor input min.	V_{clkmin}	Min for clock extraction	1			Vpp
Clock extractor input max.	V_{clkmax}	Max for clock extraction			50	mVpp
MONOFLOP delay	T_{mono}		40		80	µs
EEPROM data endurance	N_{cy}	Erase all / Write all	1000			cycles
EEPROM retention	T_{ret}	T_{op} = 55°C after 1000 cycles	10			years

1) Maximum voltage is defined by forcing 10mA on Coil1-Coil2

Table 2

Timing Characteristics

Parameter	Symbol	Conditions	Value	Unit
Power on Reset Time	t_{por}		600	µs
Read Bit Period	t_{rdb}	RF periods	32	periods
LIW/ACK/NACK pattern Duration	t_{patt}	RF periods	160	periods
Duration of ID	t_{rID}	RF periods	1024	periods
Divergence-Time	T_{div}	RF periods	224	periods
Authentication-Time	t_{auth}	RF periods	3744	periods
WRITE Access Time	t_{wa}	RF periods	128	periods
EEPROM write Time	t_{wee}	RF periods, V_{DD} = 3V	3072	periods

Table 3

RF periods respresent periods of the carrier frequency emitted by the transceiver unit. For example, if 125 kHz is used, the Read bit period would be: 1/125'000*32 = 256µs.

A COMPANY OF THE SWATCH GROUP

Block Diagram

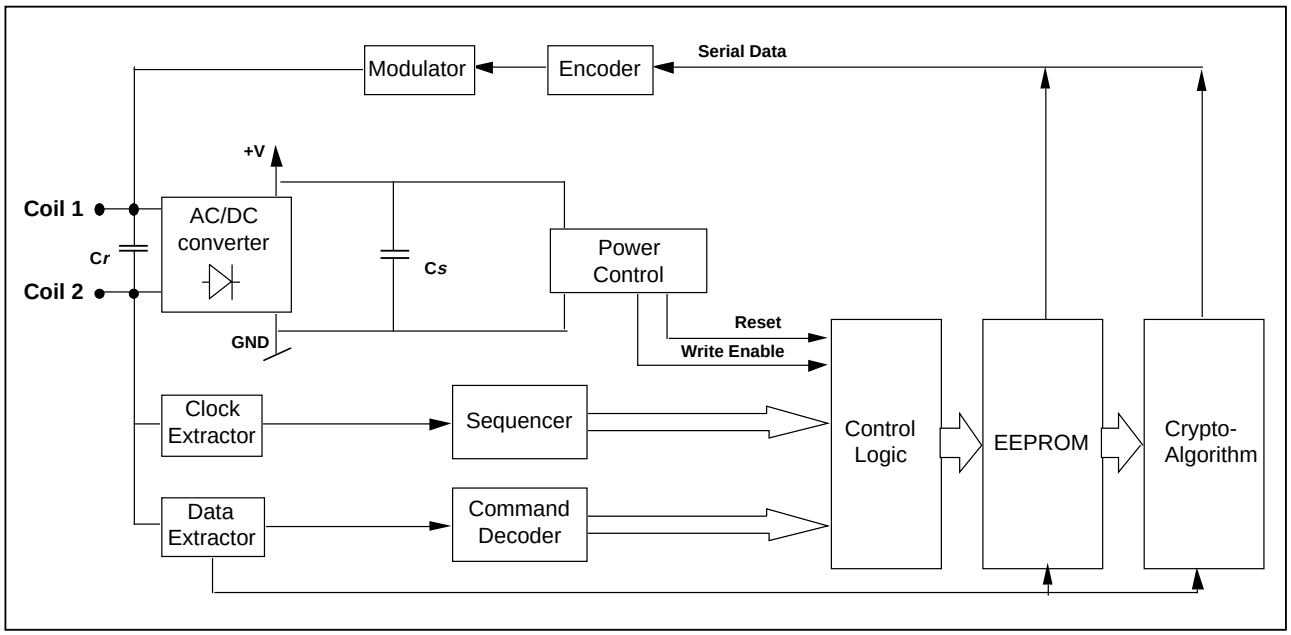

Figure 4

Pad Description

Pad	Name	Description
1	COIL2	Coil Terminal 2
3	VSS	Negative DC Supply
4	TST1	Test 1 connection
5	TST2	Test 2 connection
6	TST3	Test 3 connection
7	VDD	Positive DC Supply
8	COIL1	Coil Terminal 1

Functional Description

General

The V4070 is supplied by means of an electromagnetic field induced on the attached coil. The AC voltage is rectified in order to provide a DC internal supply voltage. When the DC voltage crosses the Power-On level, the chip will enter the Standby Mode and expect commands. In Standby Mode a continuous sequence of Listen Windows (LIW) is generated. During this time, the crypto-Chip will turn to the Receive Mode (RM) if it receives a valid RM pattern. The chip then expects a command to enter the desired mode of operation.

Memory Organisation

The 160 bits EEPROM are organised in 10 words of 16 bits. Words 0 and 1 contain the USER_MEMORY and the Lock-Bits LB1 and LB0. Write-Mode can only be entered if LB1='1' and LB0='0'. Words 2 and 3 contain the ID that can never be modified. Words 4 through 9 contain the 96 bits of secret key. These bits influence the crypto-algorithm but cannot be read directly.

A COMPANY OF THE SWATCH GROUP

Memory Map

	Bit15	Bit0
word 9	Crypt Key 95	Crypt Key 80
8	Crypt Key 79	Crypt Key 64
7	Crypt Key 63	Crypt Key 48
6	Crypt Key 47	Crypt Key 32
5	Crypt Key 31	Crypt Key 16
4	Crypt Key 15	Crypt Key 0
3	ID 31	ID 16
2	ID 15	ID 0
1	LB1,LB0,UM 29	UM 16
0	UM 15	UM 0

Figure 5

Standby Mode

After a Power-On Reset and upon completion of a command, the chip will execute the Standby Mode, in which it will continuously send LIWs to allow the reader to issue commands. As every LIW has a duration of 160 periods of the RF field the reader can turn to Receive mode every 1.3ms at 125kHz.

Receive Mode

To change from Standby Mode to another operation the chip has to be brought into Receive Mode. To do this the Transceiver sends to the chip the RM pattern during the 32 clocks of modulated phase in a Listen Window (LIW). The V4070 will stop sending data upon reception of a valid RM. The RM pattern consists of 2 bits “0” sent by the transceiver. The first “0” is to be detected during the 32 periods when the modulation is “ON” in the LIW.
Next the V4070 expects a command to specify the operation to be executed.

Commands

The commands are composed of 4 bits, divided into 3 data bits and 1 even parity bit (total amount of “1’s” is even including the parity bit). There exist 4 different commands. Upon reception of an unknown command or a command with wrong parity the chip will immediately return into Standby Mode.

Commands

COMMAND BITS	*FUNCTION*
0 0 1 1	ID-MODE
0 1 0 1	UM-MODE
0 1 1 0	AUTHENTICATION
1 0 1 0	WRITE WORD

First bit Recieved — Parity bit

Figure 6

ID Mode

After reception of the command including the parity the chip sends a header consisting of 12 manchester coded ‘1’s followed by 4 manchester coded ‘0’s. Then the chip sends the 32 Bits of ID contained in words 3 and 2 of the EEPROM once, without parity, starting with the MSB of word 3. After completion the chip returns to Standby-Mode.

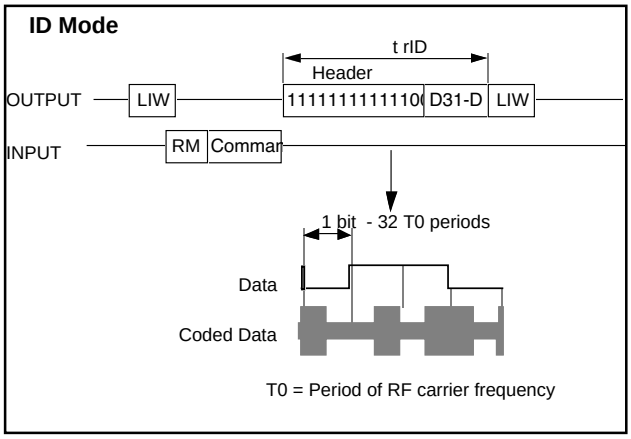

Figure 7

UM-MODE

In UM-MODE the chip sends LB1 and LB0 followed by the 30 Bits of UM starting with the MSB following the same procedure as in ID-MODE. After completion the chip returns to Standby Mode.

A COMPANY OF THE SWATCH GROUP

Authentication

In this mode the chip first receives the 56 bits of random number followed by seven bits of divergency bits that the reader should send as “0” followed by 28 Bits of cipher_1 (f(RN)) as authentication of the lock. The chip decides if the authentication is accepted. In this case the V4070 sends a header (12 manchester coded ‘1’s followed by 4 manchester coded ‘0’s). Next 20 Bits of cipher_2 (g(RN)) are sent. Else it sends a single NAK.

Upon completion of this command the V4070 returns to Standby Mode.

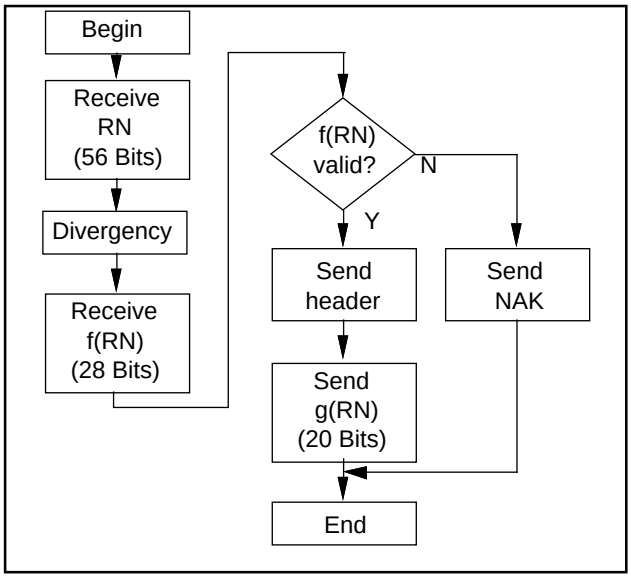

Figure 8

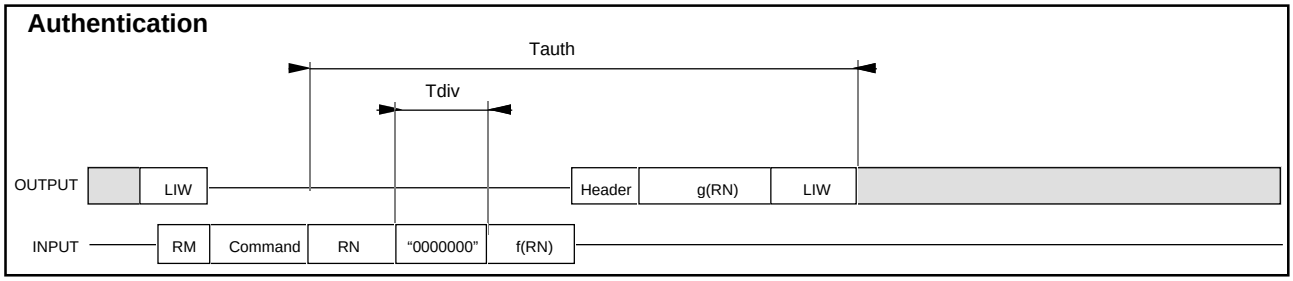

Figure 9

Write Word

The Write Word command is followed by the address and data. The address consists of a 5 bit block containing 4 data bits and 1 even parity. The data consists of 4 times 5 bit blocks, each block consisting of 4 data bits and 1 associated even parity bit. One additional block consists of 4 column parity bits and a trailing zero (refer to fig 10).

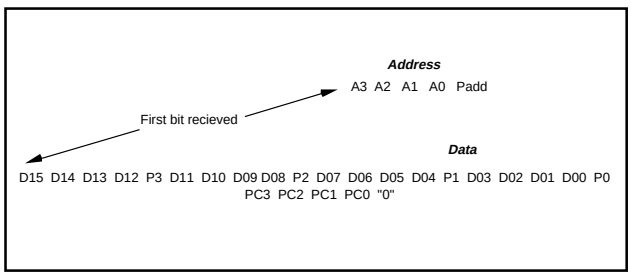

Figure 10

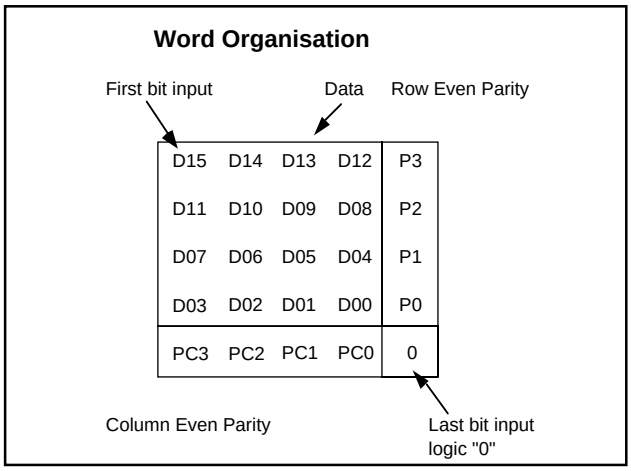

Figure 11

After reception of the write command, the address and the data, the V4070 will check the parity and the Lock-Bits. If all the conditions are fullfilled, an Acknowledge pattern (ACK) will be issued, and the EEPROM writing process will start. At the end of programming the chip will send an Acknowledge pattern (ACK). If at least one of the checks fails, the chip will issue a No Acknowledge pattern (NAK) instead of ACK and return to the Standby Mode.

The V4070 might also return to the Standby Mode without sending back a NAK if the incomming data is corrupted and/or inconsistent.

A COMPANY OF THE SWATCH GROUP

Write Word

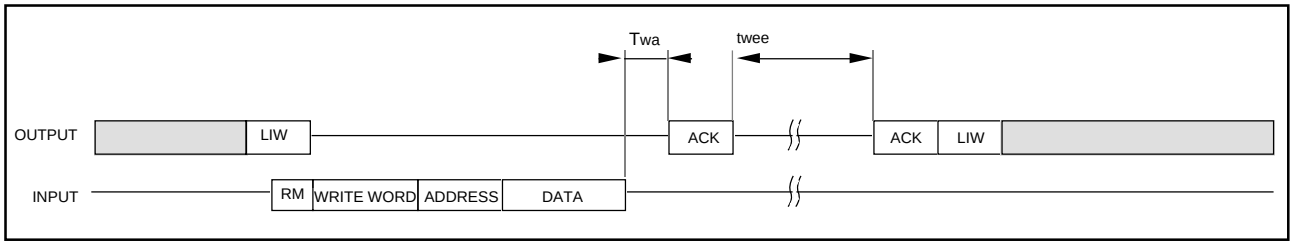

Figure 12

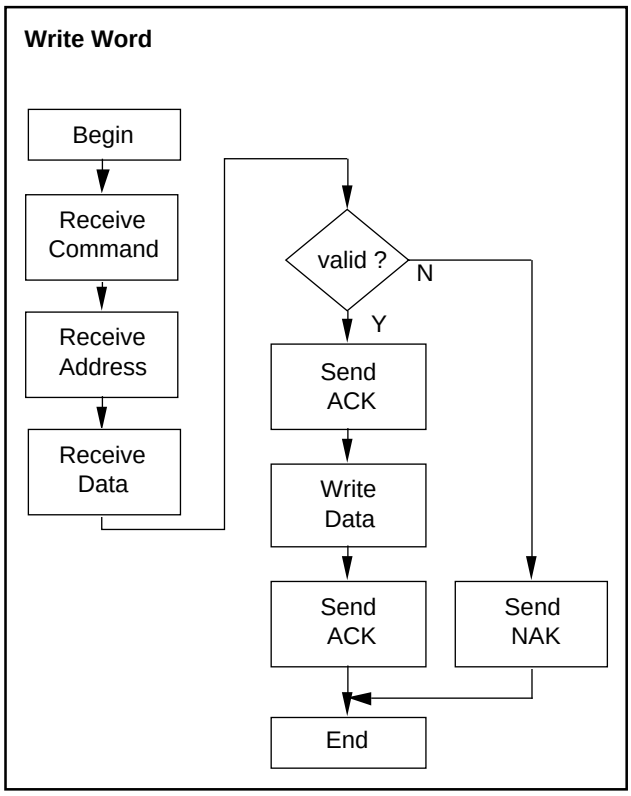

Figure 13

Power On Reset

When the V4070 with its attached coil will enter an electromagnetic field, the built in AC/DC converter will supply the chip. The DC voltage is monitored and a Reset signal is generated to initialise the logic. The power On Reset is also provided in order to make sure that the chip will start issuing LIWs and be ready to accept commands with a sufficient DC power level. A hysteresis is provided to avoid improper operation at limit level.

AC/DC Converter and Voltage Limiter

The AC/DC converter is fully integrated on chip and will extract the power from the incident RF field. The internal DC voltage will be clamped to avoid high internal DC voltage in strong RF fields.

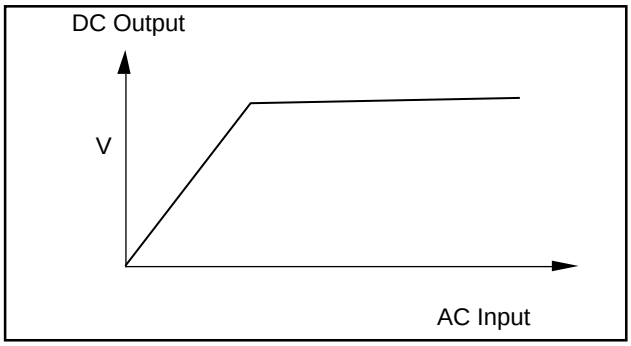

Figure 14

Clock Extractor

The Clock extractor will generate a system clock with a frequency corresponding to the frequency of the RF field. The system clock is fed into a sequencer to generate all internal timings.

The clock extractor is optimized for power-consumption, sensitivity and noise-suppression. As the input signal is subject to a large dynamic range due to the amplitude modulation, the clock-extractor may miss clocks or add spurious clocks close to the edges of the RF-envelope. This desynchronisation will not be larger than ± 1 clocks per Bit and must be taken into account when developping reader software.

Data Extractor

The transceiver generated field will be amplitude modulated to transmit data to the V4070. The Data extractor demodulates the incomming signal to generate logic levels, and decodes the incomming data.

Modulator

The Data Modulator is driven by the serial data outputted from the memory or the Crypto-Logic which is Manchester encoded. The modulator will draw a large current from both coil terminals, thus amplitude modulating the RF field according to the memory data.

A COMPANY OF THE SWATCH GROUP

Communication from Transponder to the Transceiver (READ MODE)

The V4070 modulates the amplitude of the RF field to transmit data to the transceiver. The data is output serially from the EEPROM and manchester encoded.

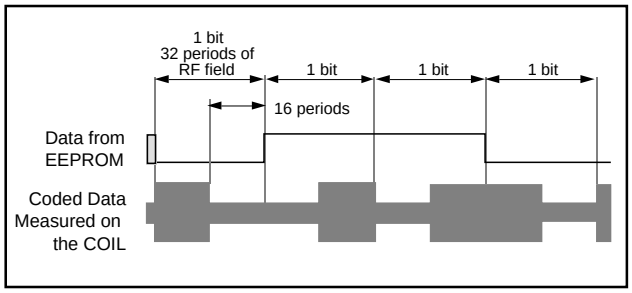

Figure 15

The V4070 uses different patterns to send status information to the transceiver. Their structure cannot be confused with a bit pattern sequence. These patterns are the Listen Window (LIW) to inform the transceiver that data can be accepted, the Acknowledge (ACK) indicating proper communication and end of EEPROM write, and the No Acknowledge (NAK) when something is wrong.

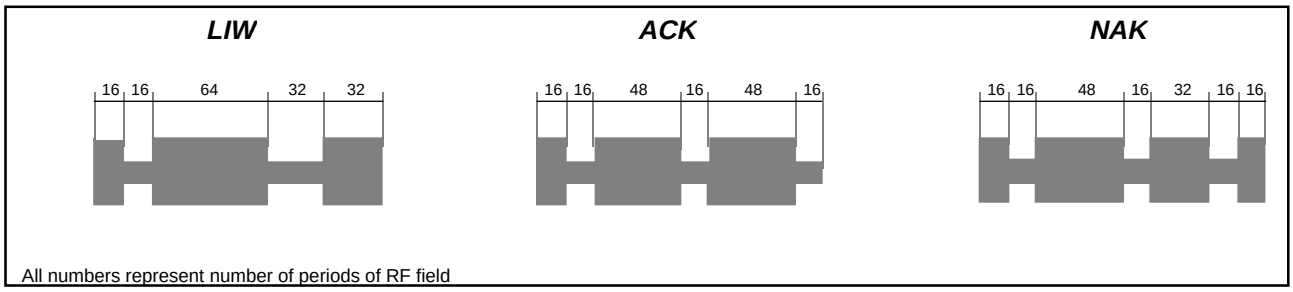

Figure 16

Communication from the Transceiver to the Transponder (RECEIVE MODE)

The V4070 can be switched to the Receive Mode ONLY DURING A LISTEN WINDOW. The Transceiver is synchronized with the incomming data from the transponder. During the phase when the chip has its modulator “ON” (32 periods of RF), the transceiver has to send a bit “0”. At reception of the first “0”, the chip stops immidiately the LIW sequence and expects then another bit “0” to switch to receive mode. The transceiver and the chip are now synchronized and further data is sent with a bit rate of 32 periods of the RF field. The V4070 turns “ON” its modulator at the beginning of each frame of 32 clock periods corresponding to one bit. To send a logic “1” bit, the transceiver continues to send clocks without modulation. After 16 clocks, the modulation device of the V4070 is turned “OFF” allowing recharge of the internal supply capacitor. To send a logic “0” bit, the transceiver stops sending clocks (100% modulation) during the first half of a bit period (first 16 periods). The transceiver must not turn “OFF” the field earlier than clock 1 of a bit period. It is recommended to turn “OFF” the field after 4 clocks of the bit period. The field is stopped from clock 5 to 16 of the bit period, and then turned “ON” again for the remaining 16 periods.

To ensure synchronisation between the transceiver and the transponder, a logic bit set to “0” has to be transmitted at regular intervals. The RM pattern consists of two bits set to “0” thus allowing initial synchronisation. While the transceiver is sending data to the transponder, two different modulations will be observed on both coils. During the first 16 clocks of a bit period, the V4070 is switching “ON” its modulation device causing a modulation of the RF field. This modulation can also be observed on the transceiver’s coil. The transceiver to send a bit “0” will switch “OFF” the field, and this 100% modulation will be observed on the transponder coil.

A COMPANY OF THE SWATCH GROUP

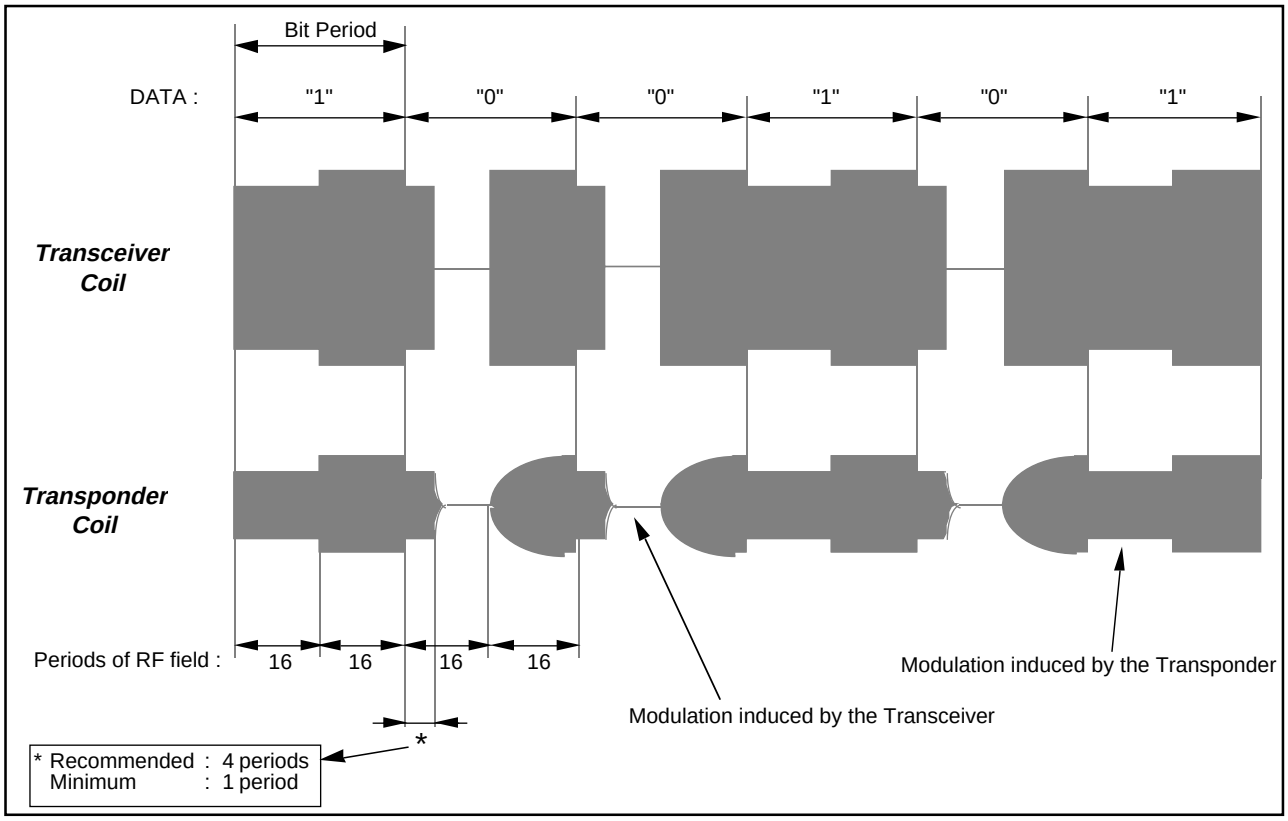

Figure 17

Package and Ordering Information

Dimensions of PCB Version

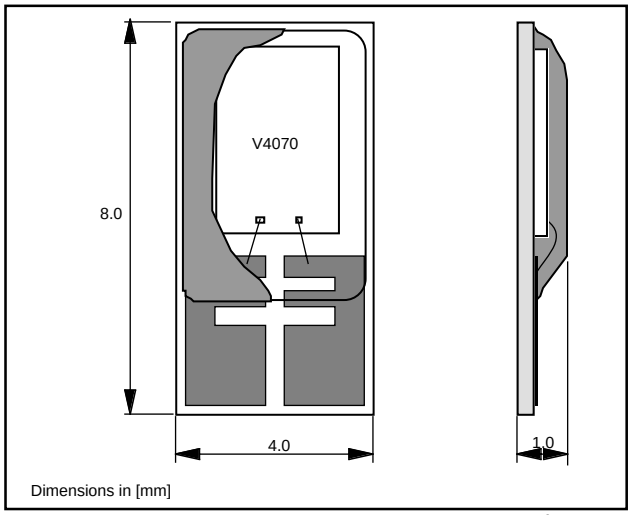

Figure 18

Chip Dimensions

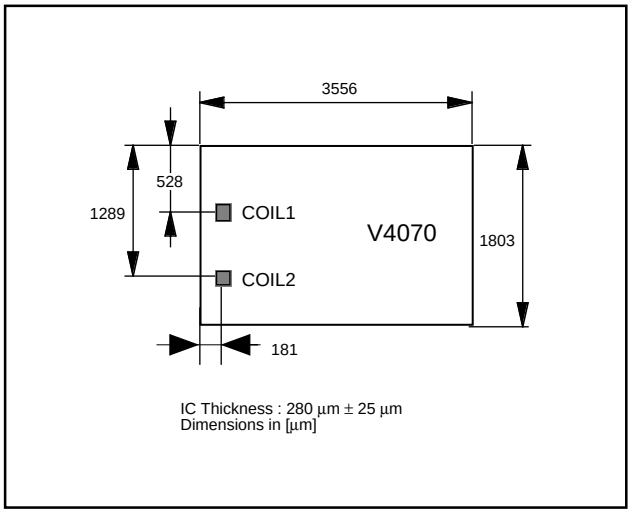

Figure 19

Ordering Information

The V4070 is available in chip form:	without Bumps	V4070 IC
For sampling, the following version is available:	PCB	V4070 - PCB

Other packages available on request.

EM Microelectronic-Marin SA cannot assume responsibility for use of any circuitry described other than circuitry entirely embodied in an EM Microelectronic-Marin SA product. EM Microelectronic-Marin SA reserves the right to change the circuitry and specifications without notice at any time. You are strongly urged to ensure that the information given has not been superseded by a more up to date version.

© 1997 EM Microelectronic-Marin SA, 10/97 Rev. A/188