UHF RFID tag IC with cryptographic authentication

SPECIFICATION

1 FEATURES

- SMIC EEPROM CMOS 180 nm
- Operating temperature range -40…+65 °C
- Passive operation – no battery needed
- Operating frequency 860 - 960 MHz
- EPC Class 1 Generation 2 compliant
- 352 bit memory organized in 3 banks: EPC, TID and RESERVED
- Hidden 128 bit bank for secret key storing
- Secret-key authentication using GOST 28147-89 crypto algorithm
- Support of ClearKey, WriteKey and Authenticate custom commands for secret key management and authentication procedure
- Two pads with combined on-wafer testing and RF operation functionality
- Small area (0.242 mm^2)

2 APPLICATIONS

- Protection of goods against counterfeiting
- Supply chain management and logistics
- Airline baggage handling
- Mail and parcel delivery
- Automobile billing systems
- Asset tagging

3 FUNCTIONAL DESCRIPTION

The chip is intended for use in passive UHF transponder applications. IC derives its operating power from an RF electromagnetic field generated by a reader, which is received and rectified by the chip. The chip sends the answer back to the reader using a backscatter modulation technique. Chip can be connected to external dipole-like antenna. NT1025D provides a fast and flexible anti-collision protocol based on internal random number generator according to EPC standard. NT1025D supports all EPC C1G2 mandatory command as well as optional Access command and custom ClearKey, WriteKey and Authenticate commands.
NT1025D has a 480 bit EEPROM organized in 4 banks as shown in Table 1.

Table 1: NT1025D EEPROM map.

Bank address	Bank name	Bank size
“01”	EPC	224 bit
“10”	TID	64 bit
“00”	RESERVED	64 bit
-*	GOST_KEY	128 bit

* - achievable only with ClearKey and WriteKey commands; used while executing Authentication command

Short-time memory block provides 4-bit storage for inventoried flags with persistence values according to EPC C1G2 standard.

NT1025D provides an authentication procedure based on the GOST 28147-89 cryptographic algorithm. The procedure represents a verification of a tag's secret key and executes as follows:

1. Interrogator generates 64-bit random number and sends it to NT1025D-based tag
2. Interrogator encrypts number generated in p.1 with a "true" key and stores the result
3. Tag encrypts number received from interrogator with a key stored in its hidden bank
4. Tag sends the encryption result back to the interrogator
5. Interrogator compares "true" result stored in p.2 with the result acquired from tag in p.4. If two numbers are equal, then the tag's key is authentic

Secret key cannot be read out directly even in test mode; it can be verified only using the authentication procedure. Secret key or its parts can be rewritten only after complete hidden bank erasing. No key information is sent over air during authentication procedure. Authentication procedure execution takes about 20 ms. Commands used for secret key management and authentication are Custom commands compliant to EPC Class 1 Gen 2.
IC is designed on SMIC EEPROM CMOS 180 nm technology.

4 STRUCTURE

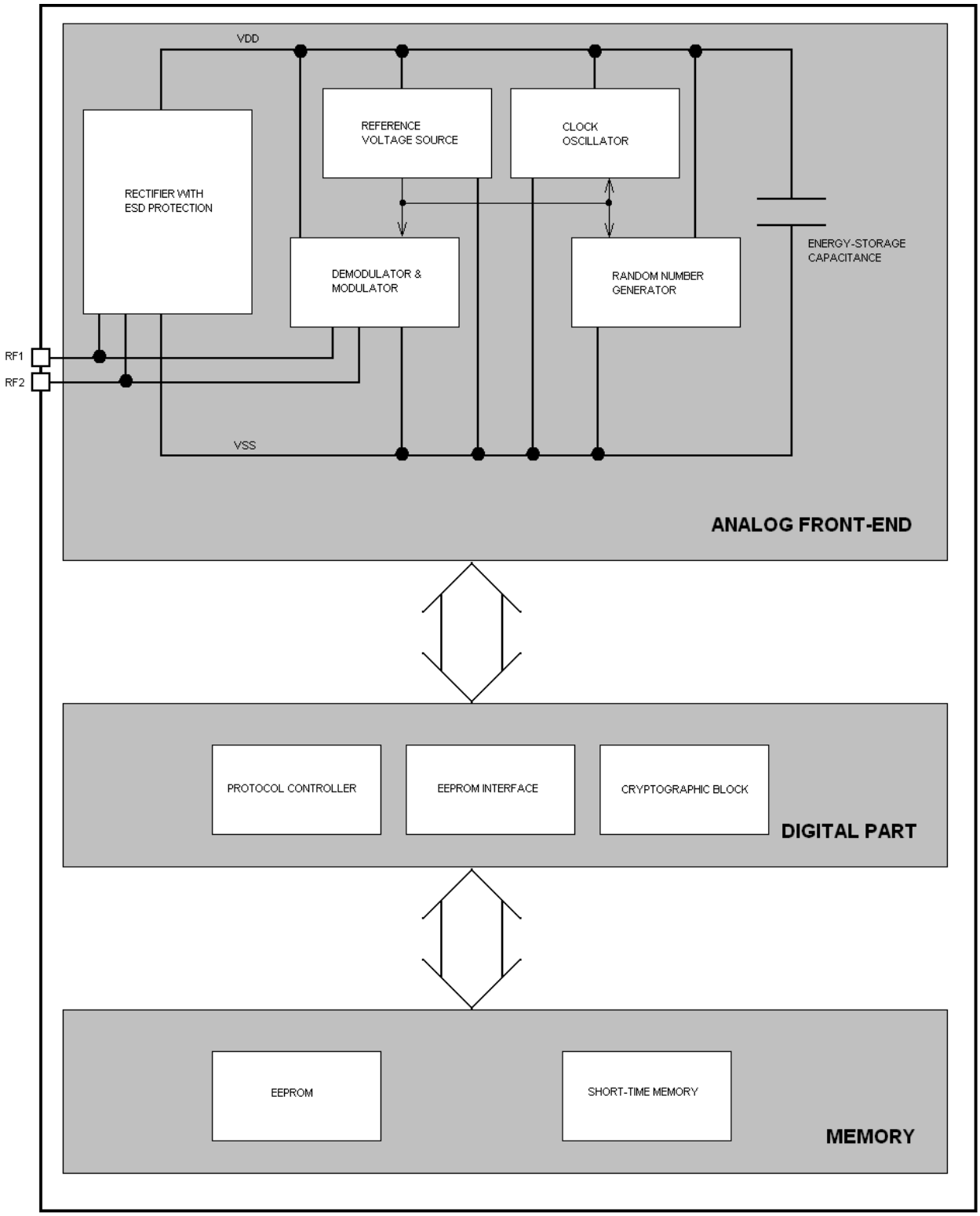

Figure 1: UHF RFID tag IC with cryptographic authentication structure.

5 PIN DESCRIPTION

Name	Direction	Description
RF1	IO	Test pad 1 / antenna port 1
RF2	IO	Test pad 2 / antenna port 2

6 LAYOUT DESCRIPTION

The IC dimensions are given in the table 2.

Table 2: IC dimensions.

Dimension	Value	Unit
Height	420	µm
Width	575	µm

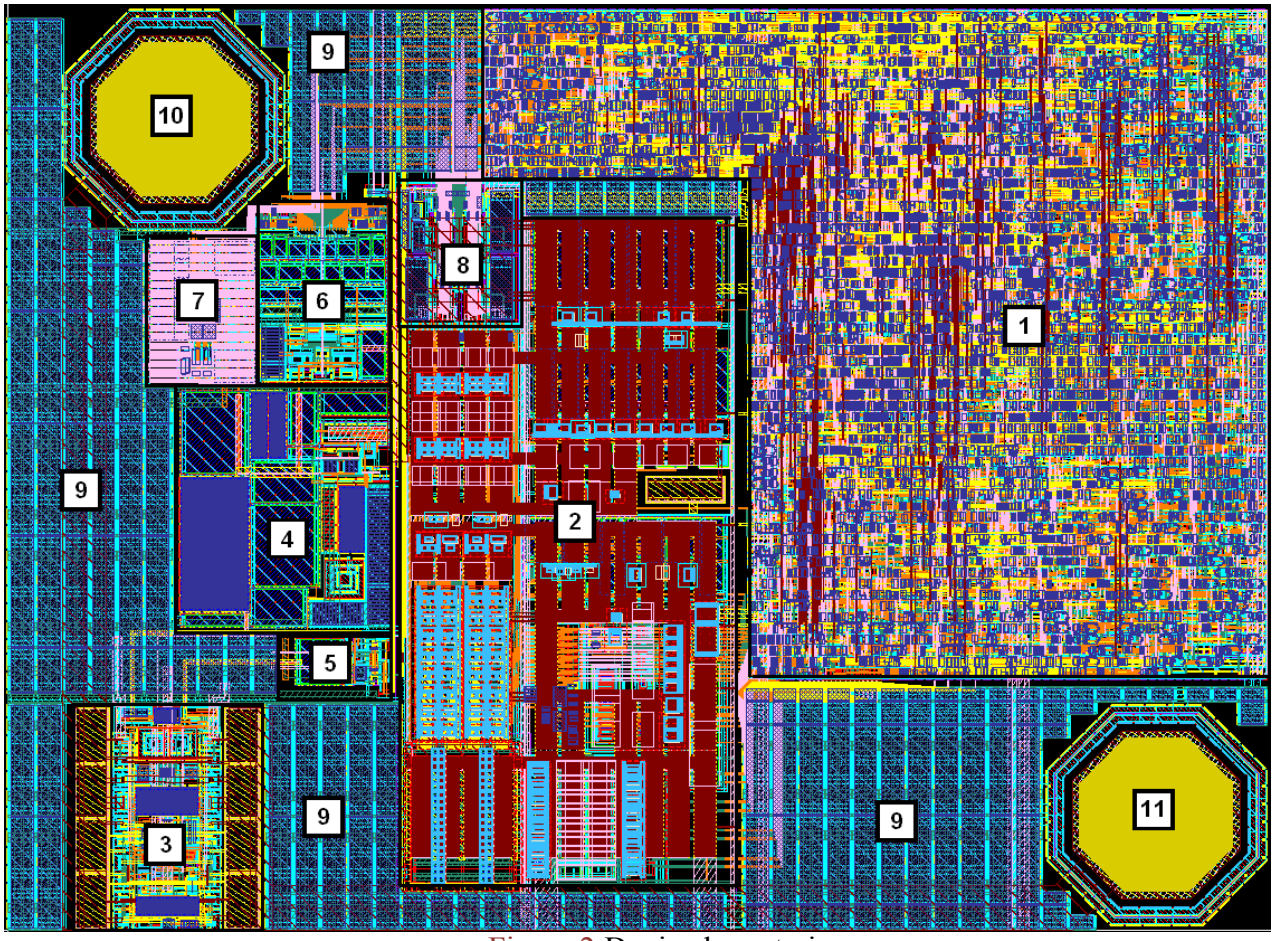

Figure 2:Device layout view.

1. Digital part
2. EEPROM
3. Rectifier
4. Reference voltage source
5. Demodulator
6. Clock oscillator
7. Random number generator
8. Short-time memory
9. Energy-storage capacitance
10. Pad RF1
11. Pad RF2

7 OPERATION CHARACTERISTICS

7.1 TECHNICAL CHARACTERISTICS

Technology SMIC EEPROM CMOS 180 nm
Status silicon proven
Area 0.242 mm^2

7.2 ELECTRICAL CHARACTERISTICS

Parameter	Symbol	Conditions	Value			Unit
			min	typ	max	
Operating temperature	T_A		-40	25	+65	°C
Operating carrier frequency	F_c		860	-	960	MHz
Read sensitivity	P_{rd_min}	T_A = 25 °C	-	30	-	µW
Authenticate sensitivity	P_{auth_min}	T_A = 25 °C	-	30	-	µW
Write sensitivity	P_{wr_min}	T_A = 25 °C	-	50	-	µW
Impedance[1]	Z	F_c = 867 MHz	-	16-j350	-	Ω

Note: 1 Measured for QFN32 package.

8 DELIVERABLES

IP contents:

- Datasheet
- Layout View (GDSII)
- Evaluation kit based on packaged IC
- Characterization Report
- Behavioral Model
- SPICE netlist (.cdl)
- Integration Support