Security & Chip Card ICs

SLE 4436/36E

Intelligent 221–Bit EEPROM Counter
for > 20000 Units with Security Logic
and High Security Authentication

Short Product Information 07.99

SLE 4436/36E Short Product Information		Ref.: SPI_SLE4436_0799.doc
Revision History:	**Current Version 07.99**	
Previous Releases:	01.96	
Page	Subjects (changes since last revision)	
	Layout change	

Important: Further information is confidential and on request. Please contact:
Infineon Technologies AG in Munich, Germany,
Security & Chip Card ICs,
Fax +49 89 234-28925
E-Mail: Security-and.Chipcard-ICs@infineon.com

Published by Infineon Technologies AG, CC Applications Group
St.-Martin-Strasse 53, D-81541 München

Attention please!

The information herein is given to describe certain components and shall not be considered as warranted characteristics.

Terms of delivery and rights to technical change reserved.

We hereby disclaim any and all warranties, including but not limited to warranties of non-infringement, regarding circuits, descriptions and charts stated herein.

Infineon Technologies is an approved CECC manufacturer.

Information

For further information on technology, delivery terms and conditions and prices please contact your nearest Infineon Technologies Office in Germany or our Infineon Technologies Representatives world-wide (see address list).

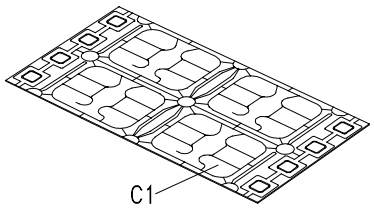
Warnings

Due to technical requirements components may contain dangerous substances. For information on the types in question please contact your nearest Infineon Technologies Office.

Infineon Technologies Components may only be used in life-support devices or systems with the express written approval of Infineon Technologies, if a failure of such components can reasonably be expected to cause the failure of that life-support device or system, or to affect the safety or effectiveness of that device or system. Life support devices or systems are intended to be implanted in the human body, or to support and/or maintain and sustain and/or protect human life. If they fail, it is reasonable to assume that the health of the user or other persons may be endangered.

Intelligent 221–Bit EEPROM Counter for > 20000 Units with Security Logic and High Security Authentication

Features



M3

- **221 bit EEPROM and 16 bit mask-programmable ROM**

  104 bit user memory fully compatible with SLE 4406/06E
  - 64 bit Identification Area consisting of
    - 16 bit Manufacturer code (mask-programmable ROM)
    - SLE 4436:
      8 bit Manufacturer data, card issuer dependent (ROM)
      40 bit for personalization data of card issuer (PROM)
    - SLE 4436E:
      48 bit for personalization data of card issuer (PROM)
  - 40 bit Counter Area including 1 bit for personalization (PROM/EEPROM)

  133 bit additional memory for advanced features
  - 4 bit Counter Backup (anti-tearing flags)
  - 1 bit initiation flag for Authentication Key 2
  - 16 bit Data Area 1 for free user access
  - 48 bit Authentication Key 1
  - either 48 bit Data Area 2 for user defined data or 48 bit Authentication Key 2
  - 16 bit Data Area 3 for free user access
- **Counter with up to 33352 count units fully compatible with SLE 4406/06E**
  - Five stage abacus counter
  - Due to testing purposes a maximum of 21064 count units is guaranteed
- **Counter tearing protection**
  - Backup feature activated at choice
- **High security authentication unit**
  - Random number as challenge
  - Individual secret Authentication Key 1
  - Optional individual secret Authentication Key 2
  - Calculation of up to 16 bit response
  - Calculation of a 16 bit response within 30 ms at a clock frequency of 100 kHz
- **Transport Code protection for delivery**
- **EEPROM security cells in sensitive areas**
- **Chip circuitry and chip layout optimised for high security against physical and electrical signal analysis**

Features (cont'd)

- **Ambient temperature –35 … +80°C**
- **Supply voltage 5 V ± 10 %**
- **Supply current < 5 mA**
- **EEPROM programming time 5 ms**
- **ESD protection typical 4000 V**
- **Endurance minimum 10^5 write/erase cycles / bit**[1)]
- **Data retention for minimum of 10 years**[1)]
- **Contact configuration and Answer-to-Reset (synchronous transmission) in accordance to standard ISO/IEC 7816**

Table 1 Ordering Information

Type	Package[2)]	Access of 3rd byte
SLE 4436 M3	M3	Data of 3rd byte are programmed by Infineon exclusively
SLE 4436 C	C	
SLE 4436E M3	M3	Data of 3rd byte are programmed by the card manufacturer at personalisation
SLE 4436E C	C	

1) Values are temperature dependent
2) Available as a wire-bonded module (M3) for embedding in plastic cards or as a die (C) for customer packaging

Pin Description

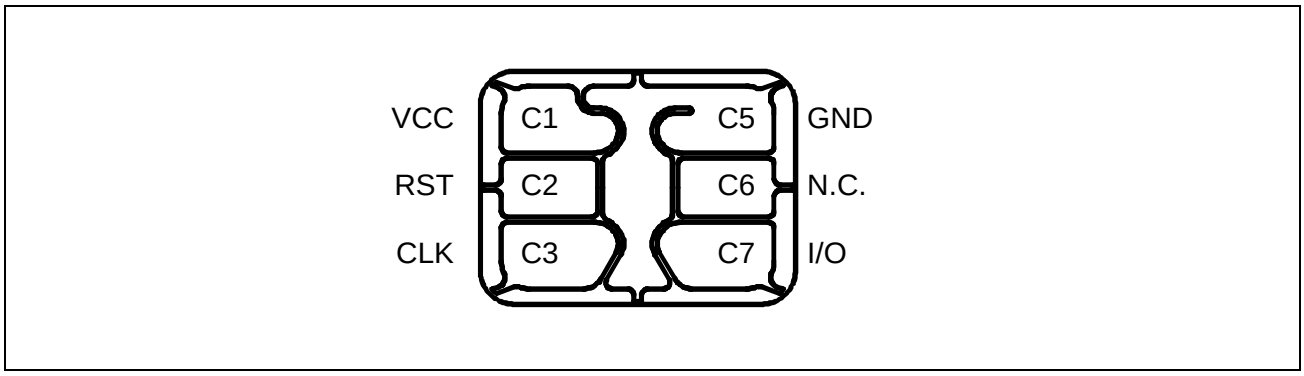


Figure 1 Pin Configuration Wire-bonded Module (top view)

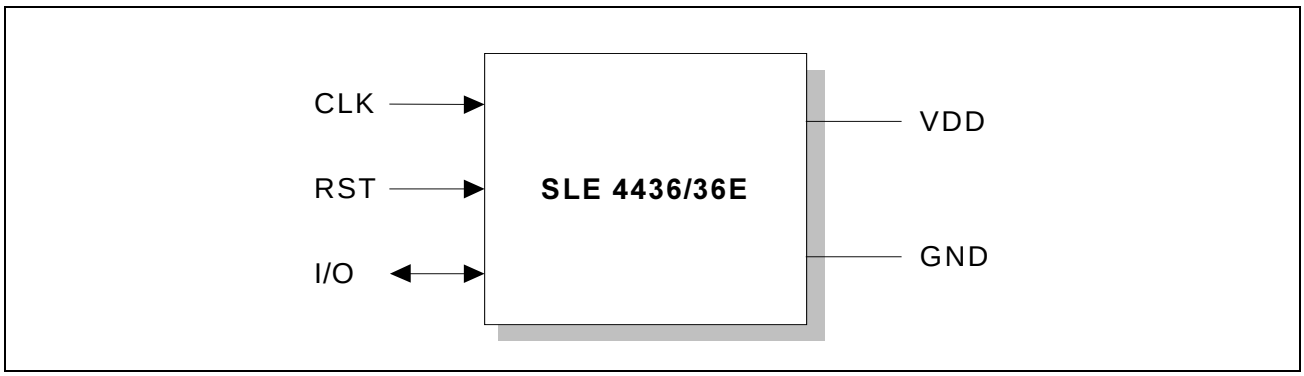


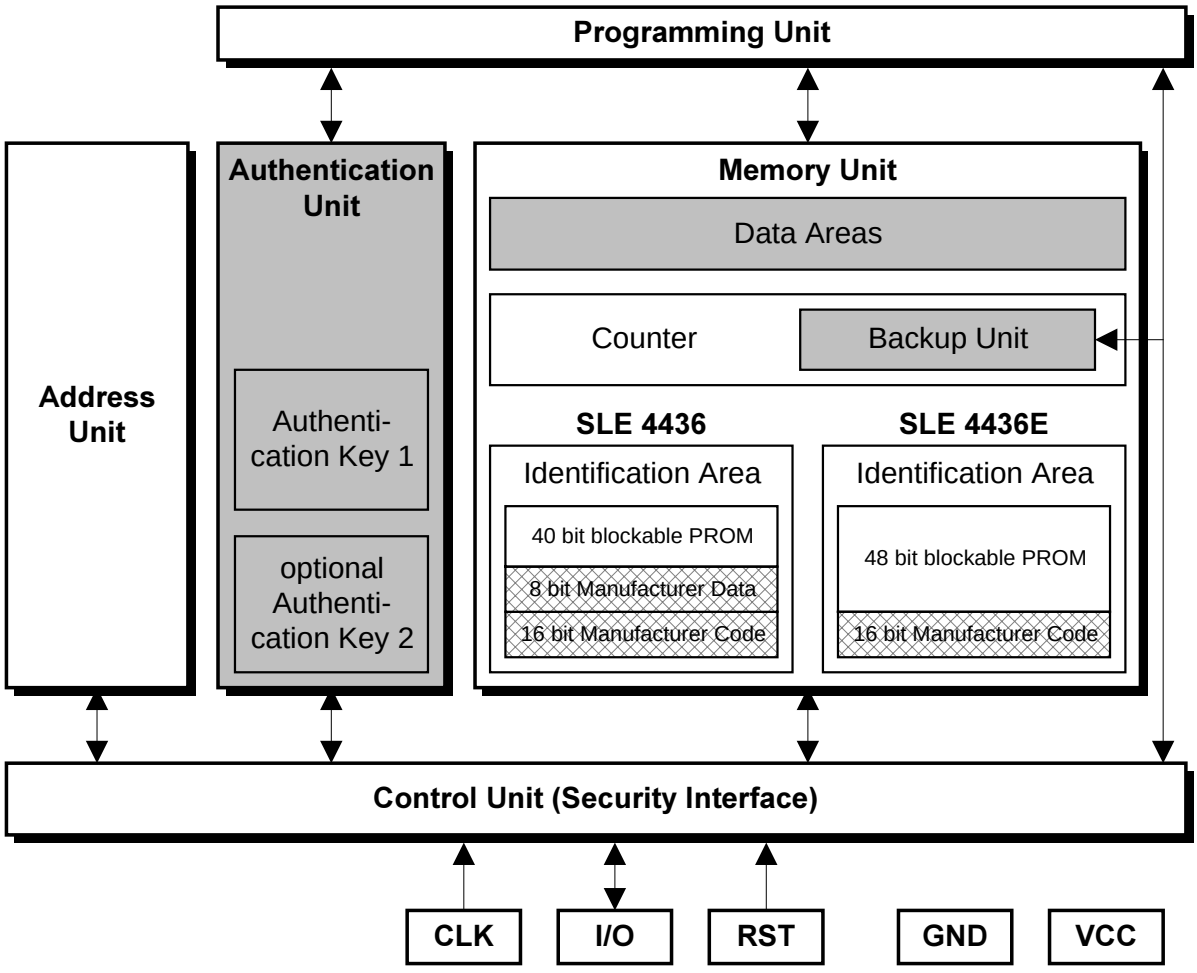
Figure 2 Pad Configuration Die

Table 2 Pin Definitions and Functions

Card Contact	Symbol	Function
C1	VCC	Supply voltage
C2	RST	Control input (Reset Signal)
C3	CLK	Clock input
C5	GND	Ground
C6	N.C.	Not connected
C7	I/O	Bi-directional data line (open drain)

General Description

SLE 4436/36E is designed for applications in prepaid telephone cards. The chip consists of an EEPROM memory of 221 bit, a ROM of 16 bits, a control/security unit and a special computing unit for chip authentication. The shaded blocks in the block diagram (Figure 3) contain the enhanced features of SLE 4436/36E compared to SLE 4406/06E.



Legend
Shaded blocks - Enhanced features of SLE 4436/36E compared to SLE 4406/06E
Blocks marked by cross hatch - Defined by chip manufacturer

Figure 3 Block Diagram

- **Memory Unit**
  Counter, Identification Data (e.g. serial number, expiry date) and Data Areas.
- **Address Unit**
  Setting of the address counter is synchronously with the CLK.
- **Programming Unit**
  The programming voltage for the EEPROM/PROM is generated internally.

- **Backup Unit**
  An associated backup bit indicates an interrupt caused by e.g. tearing a card out of a reader without mechanical locking device during a reloading cycle of a devaluated counter stage.
- **Authentication Unit**
  The secret algorithm offers a challenge & response procedure for individual card authentication; the optional activation of cipher block chaining allows the certification of a counter decreasing procedure.
- **Security Interface**
  Ensures a minimum and a maximum frequency and proper logical voltage levels.