Security & Chip Card ICs

SLE 4466

Intelligent 515–Bit Memory Chip
with Counter for > 130.000 Units,
Security Logic and High Security Authentication

Short Product Information 07.99

SLE 4466 Short Product Info	Ref.: SPI_SLE4466_0799.doc
Revision History: Current Version 07.99	
Previous Releases: 10.98	
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).

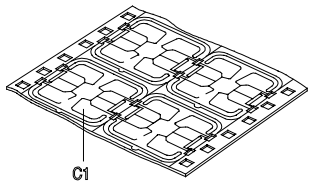
Warnings

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 515–Bit Memory Chip with Counter for > 130.000 Units, Security Logic and High Security Authentication

Features



M2

- **496 bit EEPROM and 16 bit mask-programmable ROM**
  128 bit Identification Area consisting of
  – 16 bit Manufacturer code (mask-programmable ROM)
  – 8 bit Manufacturer data (ROM)
  – 104 bit for personalization data of card issuer (PROM)
  160 bit Value Counter (PROM/EEPROM)
  16 bit secret User Code (EEPROM)
  32 bit either secret Security Code or Data Area 3 in Standard User Mode (EEPROM)
  12 bit Data Area 1 (EEPROM)
  32 bit Data Area 2 (EEPROM)
  64 bit Response Counter
  64 bit secret Authentication Key
- **Three Chip modes with secured memory access**
  The memory is secured by different access codes dependent on the mode
  – Issuer Mode: The memory access is secured by the 4 byte Transport Code
  – Security User Mode: The memory access is secured by the 4 byte Security Code
  – Standard User Mode: The memory access is secured by the 2 byte User Code. The verification procedure is fully compatible with SLE 4404
  The different chip modes are set by 3 flag bits.
  Only after a successful code verification the chip logic allows to write or erase the data according to the implemented functionality.
- **Value Counter with up to 135232 count units**
  – Three stage abacus counter
  – Due to testing purposes a maximum of 127040 count units is guaranteed
- **High security authentication unit**
  – 64 bit Random number as challenge
  – 64 bit individual secret Authentication Key
  – Calculation of up to 31 bit response within 60 ms at a clock frequency of 100 kHz
  – Response calculation with cipher block chaining
  – Authentication access and response calculation controlled by the Response Counter
  – Four stage Response Counter with up to 69904 count units (61712 units guaranteed)
  – Certification of the decreasing of the Value Counter
  – Signature of the data content
- **Memory access interface compatible with SLE 4404**
- **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 < 10 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)]
SLE 4466 M2	M2
SLE 4466 C	C

[1)] Values are temperature dependent, for further information please refer to your Infineon Sales Office.
[2)] available as wire-bonded module (M2) for embedding in plastic cards or as die (C) for customer packaging

Pin Description

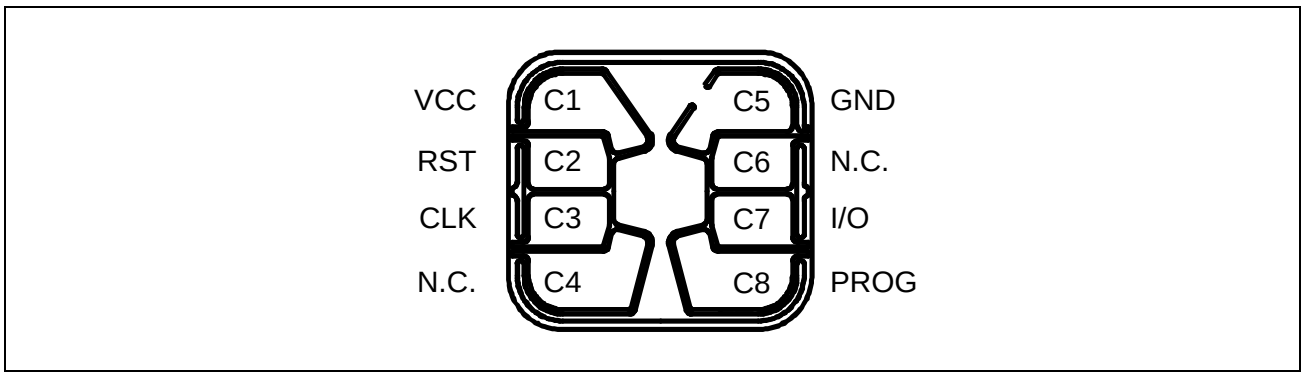


Figure 1 Pin Configuration (top view)

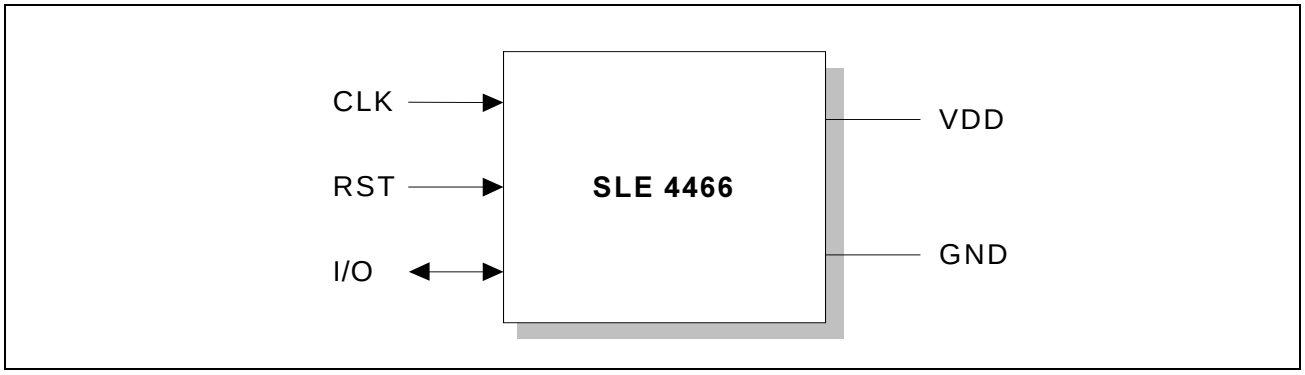


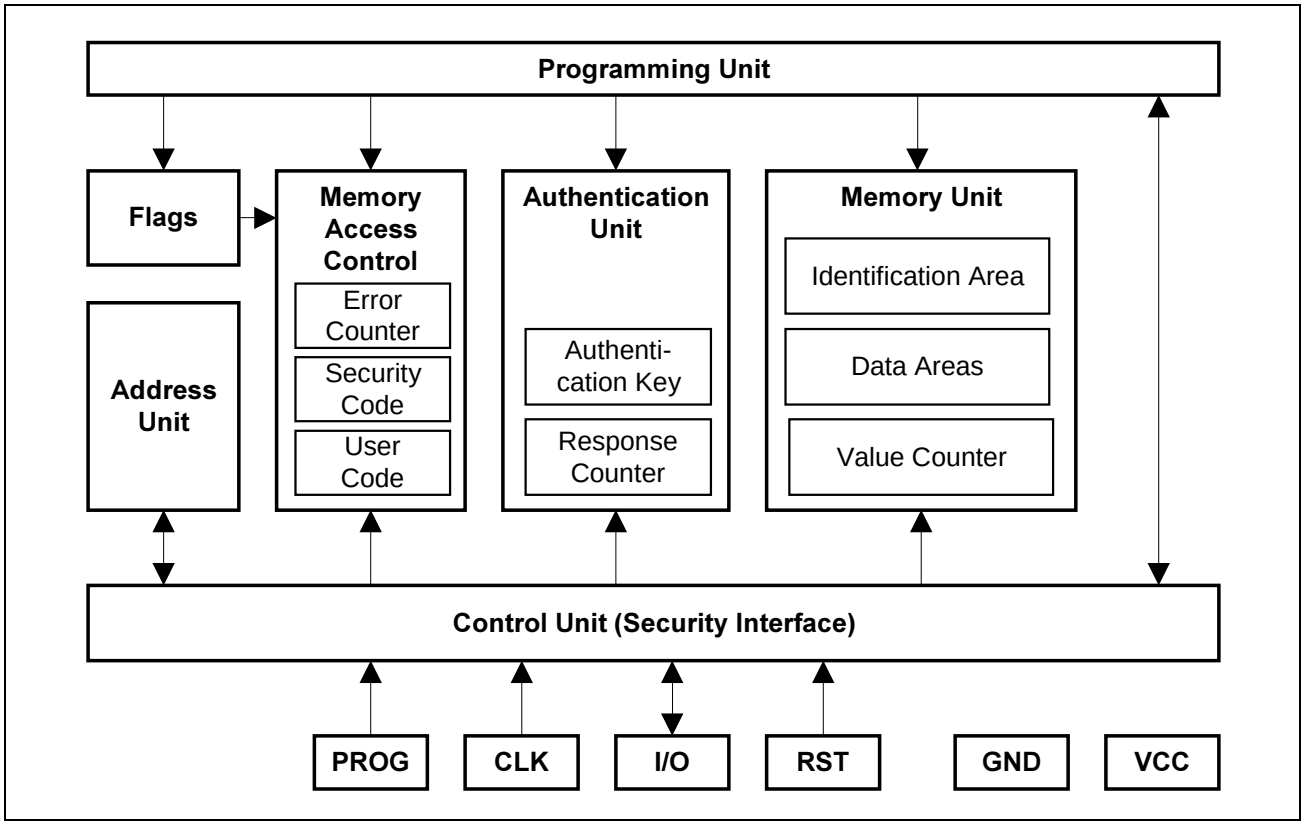
Figure 1 Pad Configuration Die

Table 2 Pin Definitions and Functions

Card Contact	Symbol	Function
C1	VCC	Supply voltage
C2	RST	Control input (Reset Signal)
C3	CLK	Clock input
C4	N.C.	Not connected
C5	GND	Ground
C6	N.C.	Not connected
C7	I/O	Bi-directional data line (open drain)
C8	PROG	Control input (Programming Signal)

General Description

SLE 4466 is designed for prepaid payment applications (e.g. vending machines, electronic metering) and secured payment applications (e.g. loyalty scheme). The chip consists of an EEPROM memory of 496 bit (incl. 8 bit Manufacturer data), a ROM of 16 bit, a control/security unit, a memory access control logic, a special computing unit for chip authentication and 3 flag bits for mode selection.



Block Diagram

- **Memory Unit**
  Value Counter, Identification Data (e.g. serial number, expiry date) and Data Areas.
- **Address Unit**
  Setting of the address counter is synchronously with CLK. The chip provides the Answer to Reset (ATR) for synchronous transmission according to ISO/IEC 7816.
- **Memory Access Control**
  Access to Authentication Unit and Memory Unit is controlled by a secret code (mode dependent).
- **Authentication Unit**
  The secret algorithm offers a challenge & response procedure for card authentication (individual key) and as signature for data and counter status integrity. Additionally cipher block chaining of the responses allows the certification of a Value Counter decreasing procedure. The authentication is controlled and limited by the response counter also avoiding a repetition of identical responses.
- **Programming Unit**
  The programming voltage for the EEPROM/PROM is generated and controlled internally.
- **Security Interface**
  Ensures a minimum and a maximum frequency and proper logical voltage levels.