Security & Chip Card ICs

Eurochip 77

SLE 7736
SLE 7736E

Intelligent 237–Bit EEPROM Counter
for > 20000 Units with Security Logic,
High Security Authentication and
Card-Trash Mechanism

Short Product Information December 2001

SLE 7736/36E Short Product Information	Ref.: SPI_SLE7736_1201.doc
Revision History: Current Version 2001-12-21	
Previous Releases:	
Page	Subjects (changes since last revision)

Important: Further information is confidential and on request. Please contact:
Infineon Technologies AG in Munich, Germany,
Security & Chip Card ICs,
Tel +49 (0)89 / 234-80000
Fax +49 (0)89 / 234-81000
E-Mail: security.chipcard.ics@infineon.com

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

To our valued customers

We constantly strive to improve the quality of all our products and documentation. We have spent an exceptional amount of time to ensure that this document is correct. However, we realise that we may have missed a few things. If you find any information that is missing or appears in error, please use the contact section above to inform us. We appreciate your assistance in making this a better document.

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).

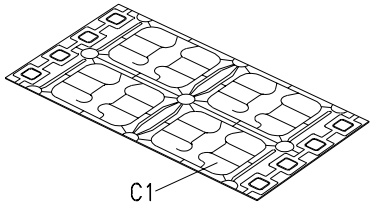
Warnings

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 237–Bit EEPROM Counter for > 20000 Units with Security Logic, High Security Authentication and Card-Trash Mechanism

Features



M3

- **Member of Eurochip Family**
  100% functional compatibility to SLE 5536S/36SE with focus on state of the art security features
- **221 bit EEPROM and 16 bit mask-programmable ROM**

  104 bit user memory
  – 64 bit Identification Area consisting of
    • 16 bit Manufacturer code (mask-programmable ROM)
    • **SLE 7736**:
      8 bit Manufacturer data, card issuer dependent (ROM)
      40 bit for personalization data of card issuer (PROM)
    • **SLE 7736E**:
      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 (PROM/EEPROM)
  – 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**
  – Five stage abacus counter
  – Due to testing purposes a maximum of 21064 count units is guaranteed
- **Counter tearing protection**
  – Backup feature activated at choice
  Counter tearing protection may be disabled by mask option
- **High security authentication unit**
  Individual card authentication fully compatible with Eurochip Family
  – 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
  Additionally activation by terminal
  – Response calculation with cipher block chaining
  – Certification of the counter value
- **Card-Trash mechanism for physical devaluation**
- **Transport Code protection for delivery**

Features (cont'd)

- **Chip circuitry and chip layout optimised for high security against physical and electrical signal analysis**

Advanced 1.2 µm CMOS-technology (IMEM) optimised for security layout

- Exclusive use of EEPROM security cells
- Secure wiring for all security relevant signals
- Shielding of deeper layers via metal
- Sophisticated sensory and logical security functions
- No isolation on backside necessary

Sophisticated electrical characteristics

- Ambient temperature –40 … +80°C
- Supply voltage 5 V ± 10 % (Class A), extension to 3 V ± 10% (Class B)
- Supply current < 1 mA (typical 300 µA)
- EEPROM programming time 5 ms
- ESD protection typical 4000 V
- Endurance minimum 10^5 write/erase cycles / bit[1)]
- Data retention for minimum of 30 years[1)]
- Contact configuration and Answer-to-Reset (synchronous transmission) in accordance to standard ISO/IEC 7816

Document References

– Confidential data sheet
– Qualification report chip

– Chip delivery specification for wafer with chip-layout (die size, orientation, …)

– Module specification containing description of package, product logistic etc.
– Quality report module

– Application Note for use of Card-Trash mechanism

Development Tool Overview

– Evaluation Kit Memories

1) Values are temperature dependent

1 Ordering and Packaging information

Table 1 Ordering Information

Type	Package[2)]	Counter tearing protection	Voltage Range	Access of 3rd byte
SLE 7736 M3	M3	Enabled (on)	4.5 V – 5.5 V	Data of 3rd byte are programmed by Infineon exclusively
SLE 7736 C	C			
SLE 7736-BD M3	M3	Disabled (off)		
SLE 7736-BD C	C			
SLE 7736-V3 M3	M3	Enabled (on)	2.7 V – 5.5 V	
SLE 7736-V3 C	C			
SLE 7736-BD-V3 M3	M3	Disabled (off)		
SLE 7736-BD-V3 C	C			
SLE 7736E M3	M3	Enabled (on)	4.5 V – 5.5 V	Data of 3rd byte are programmed by the card manufacturer at personalisation
SLE 7736E C	C			
SLE 7736E-BD M3	M3	Disabled (off)		
SLE 7736E-BD C	C			
SLE 7736E-V3 M3	M3	Enabled (on)	2.7 V – 5.5 V	
SLE 7736E-V3 C	C			
SLE 7736E-BD-V3 M3	M3	Disabled (off)		
SLE 7736E-BD-V3 C	C			

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

Pin Description

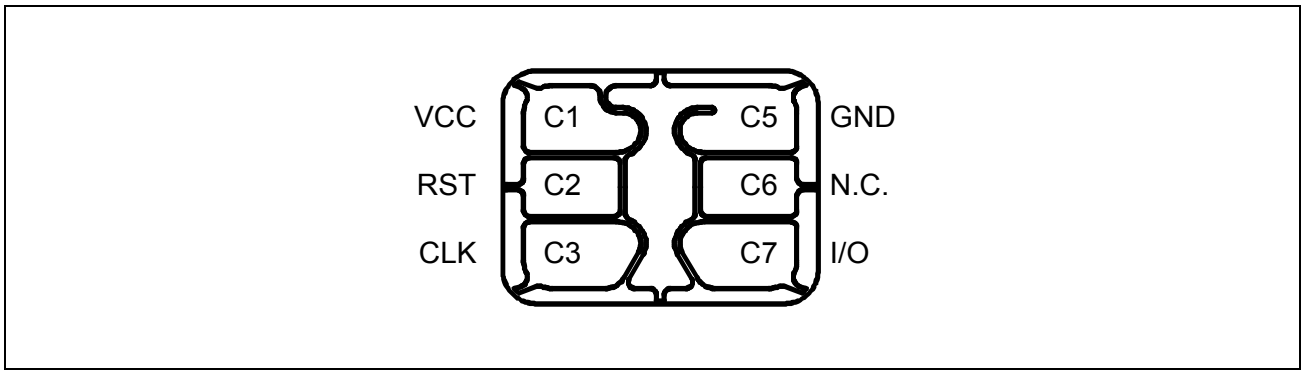


Figure 1 Pin Configuration Wire-bonded Module (top view)

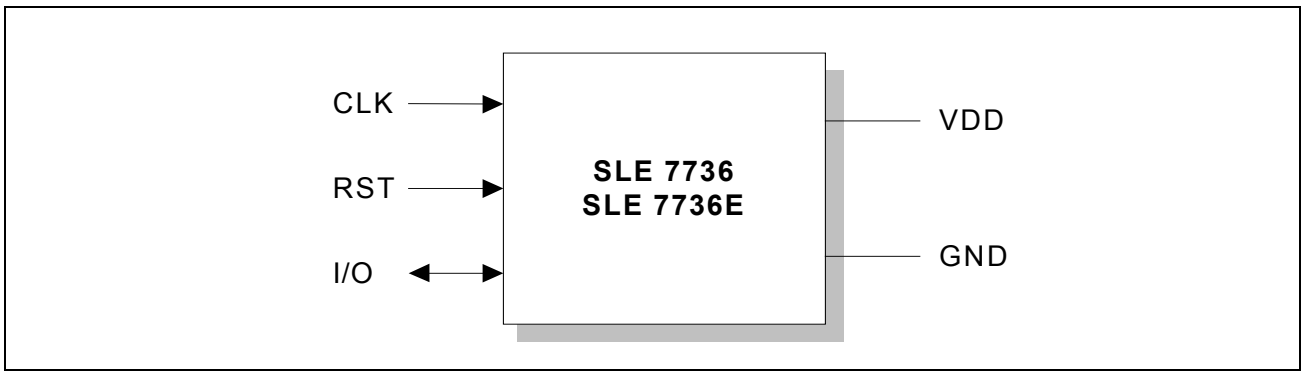


Figure 2 Pad Configuration Die

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)

2 General Description

SLE 7736/36E is designed for applications in prepaid telephone cards and pay TV. 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.

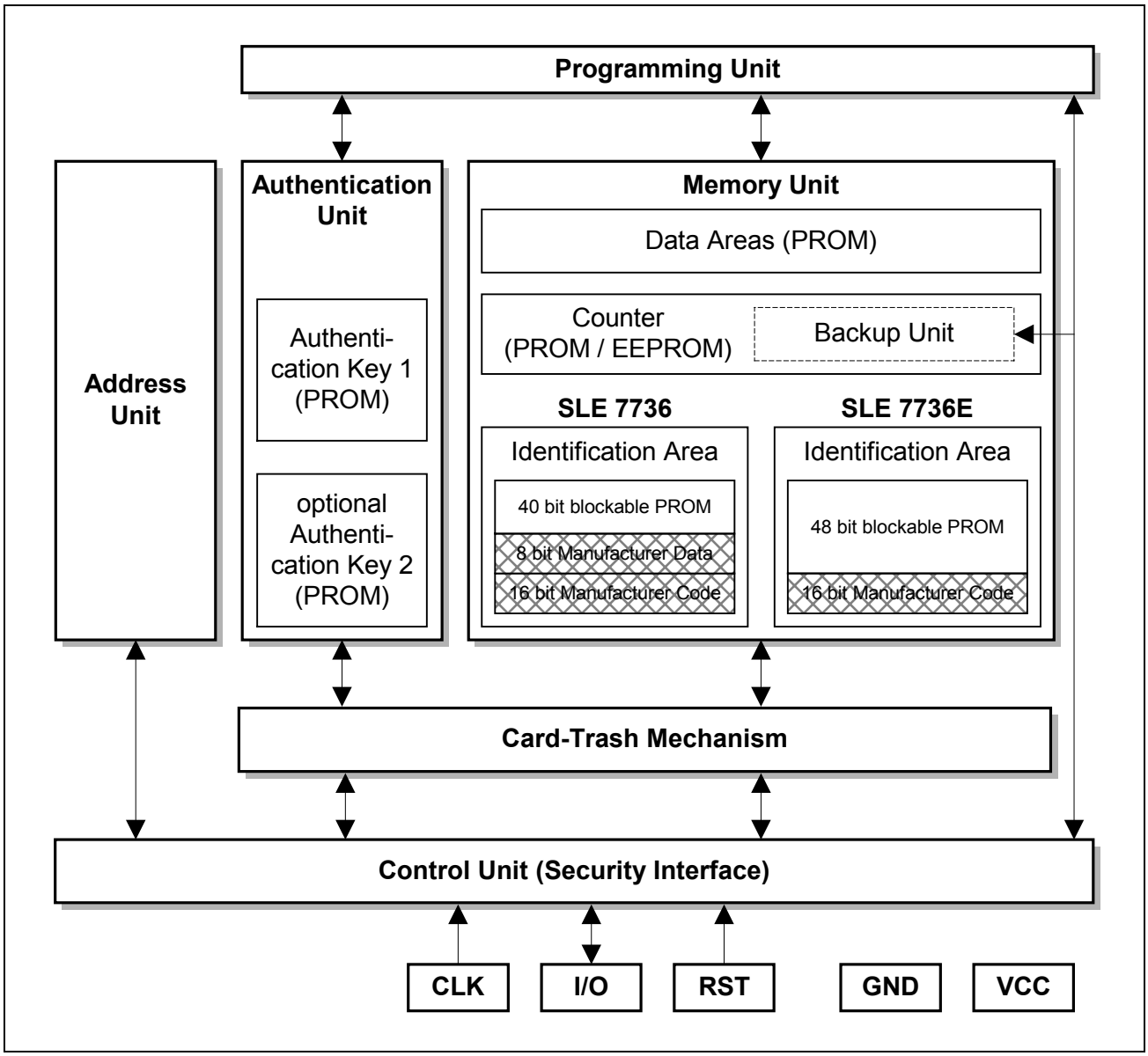


Figure 3 Block Diagram

- **Memory Unit**
  - Manufacturer Code (16-Bit Code) and Manufacturer Data (3rd Byte) for unique coding of an application. For SLE 7736**E** its recommended to use the 3rd byte for administration purpose to uniquely identify the application by the 16-bit manufacturer code and the 3rd byte;
  - Identification Data (e.g. serial number, expiry date);
  - Counter;
  - 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.
  Note: The counter tearing protection may be disabled by mask option
- **Authentication Unit**
  The secret algorithm offers a challenge & response procedure for individual card authentication fully compatible with Eurochip Family.
  The optional activation of cipher block chaining allows the certification of a counter decreasing procedure and is fully compatible with Eurochip Family.
- **Card-Trash mechanism**
  Physical blocking of chip functions such as authentication and generation of programming voltage.
- **Security Interface**
  Ensures a minimum and a maximum frequency and proper logical voltage levels.

3 Migration

Member of Infineon's Telecom ICs family.

IMEM technology offers sophisticated security features compared to NMOS technology. Due to different electrical characteristics (e.g. power consumption) an acceptance test in the terminals is recommended.

Identification and Counter fully functional compatible with existing members of Eurochip Family and SLE 4406S/06SE products for easy upgrade to higher security levels.

Use of authentication is optional and controlled by the terminal. This allows smooth upgrade of the terminals with a Security Module (SAM).