SLE 78CX800P

16-bit Security Controller with “Integrity Guard”,
optimized for Payment and Identification
applications in 0.13 µm CMOS technology
80 kBytes E²PROM, 288 kBytes User ROM, 8 kBytes RAM

Crypto@2304T engine
with register lengths of up to 2304 bits, certified RSA and ECC libraries
Symmetric Crypto Processor (SCP)
Triple-key-triple-DES and AES acceleration

Short Product Overview

May 2010

Chip Card & Security

SLE 78CX800P Short Product Overview	Ref.: Chip_Card_Product_Overview_11/09
Revision History: Current Version 05.10	
Previous Releases:	
Page	

Important: Further information is confidential and on request. Please contact:
Infineon Technologies AG in Munich, Germany,
Chip Card & Security
E-Mail: security.chipcard.ics@infineon.com

Edition 2010
Published by Infineon Technologies AG,
Chip Card & Security
81726 Munich, Germany

Legal Disclaimer

The information given in this document shall in no event be regarded as a guarantee of conditions or characteristics. With respect to any examples or hints given herein, any typical values stated herein and/or any information regarding the application of the device, Infineon Technologies hereby disclaims any and all warranties and liabilities of any kind, including without limitation, warranties of non-infringement of intellectual property rights of any third party

Information

For further information on technology, delivery terms and conditions and prices please contact your nearest Infineon Technologies Office (www.infineon.com).

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.

Product name	**SLE 78CX800P** **Secure µSlim EEPROM**
Product description	Security cryptocontroller designed for high-security applications
User-ROM	288 kByte
EEPROM	80 kByte
RAM	8 kByte
CPU	Dual 16-bit
Crypto coprocessors	
Symmetrical Cryptography	3DES, AES up to 256 bit
Asymmetrical Cryptography	RSA up to 4096 bit, ECC up to 521 bit
Clock (int.)	1 - 33 MHz
Clock (ext.)	1-10MHz
Operating voltage	1.62 V - 5.5 V
Max. supply current (at 5 MHz, 5 V)	10 mA
Max. sleep mode current (typical)	100 µA
Ambient temperature	-25 to +85°
Write / erase time	< 2.3 ms
EEPROM page programming	1 to 128 Byte
Security features	Integrity Guard Security System: Digital Full Error/Fault/ DFA Detection; Full CPU-, Memory-, Bus- and Cache-Encryption; Dual encrypted-calculation CPU; Active I2-Shield; MMU with Level Concept; DPA/SPA, DEMA/SEMA Countermeasures; Threshold Sensors: V, F, Light, Temperature; Intelligent Watchdog with Program Flow Check; Tamperproof Design; Chip ID; True RNG (AIS31, FIPS-140)
Peripherals	ICU/PEC, CRC, PLL, UART DF 8
Delivery forms	Module M5.1, MFC5.x, DSO-8, VQFN-8, die
Typical applications	Payment, EMV DDA, ePurse, Loyalty, Access Contol, Health / Social Security, Digital Signature, ID-Card, GSM, UICC
Certifications	CC EAL5+ high, EMVCo

w w w . i n f i n e o n . c o m

Published by Infineon Technologies AG