SLE 77CLF(X)2400P(M)

SOLID FLASH™ 16-bit Security Controller
Optimized for Contactless and Dual-Interface Payment Applications
in 90 nm CMOS Technology

240 kBytes SOLID FLASH™
6 kBytes RAM
27 pF Chip Input Capacitance

ISO/IEC 7816 Contactbased and
ISO/IEC 14443 Type B Compliant Contactless Interfaces
Contactless Interface acc. to ISO/IEC 18092 (NFC Passive Mode)
Optionally ISO/IEC 14443 Type A Contactless Interfaces

Optional Crypto@2304T Engine
with Register Lengths of up to 2304 bits,
certified RSA and ECC Libraries

Symmetric Crypto Processor (SCP)

Short Product Information

Revision 1.0, 2013-09-01

Confidential

Chip Card & Security

Edition 2013-09-01

Published by
Infineon Technologies AG
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 the nearest Infineon Technologies Office (**www.infineon.com**).

SOLID FLASH™: Infineon trademark which stands for security controller using dedicated Flash/EEPROM technologies.

The term "Mifare" in this document is only used as an indicator of product compatibility to the corresponding established technology. This applies to the entire document wherever the term is used.

Warnings

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

Infineon Technologies components may be used in life-support devices or systems only 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.

Revision History	
Page or Item	**Subjects (major changes since previous revision)**
Revision 1.0, 2013-09-01	

Trademarks of Infineon Technologies AG

CIPURSE™, FCOS™, SOLID FLASH™

Other Trademarks:
KEIL™, EMV™ of EMVCo, LLC (Visa Holdings Inc.);

Miscellaneous:

The term "Mifare" in this document is only used as an indicator of product compatibility to the corresponding established technology. This applies to the entire document wherever the term is used.

Last Trademarks Update 2011-02-24

SOLID FLASH™ 16-bit security controller optimized for Contactless and Dual-Interface Payment applications with enhanced instruction set for large memories in 90 nm CMOS technology, 240 kBytes 6 kBytes RAM

1 General Features

- 16-bit microcontroller with 24-bit linear addressing
- Highly efficient proprietary architecture based on 80251 instruction set, with faster execution than a standard 80251 CPU
- Interrupt Control Unit and Peripheral Event Channel (PEC)
  - Interrupt module for I/O interface and peripherals
  - Enabling fast data transfer through peripheral event channels (PEC)
- **Defined migration path from SLE 66C(L)XxxxPE products with minimized customer effort based on an adapted tool set**
- **240 kBytes SOLID FLASH™** with full E²PROM functionality and free partitioning between code and data
- **6 kBytes RAM**
- **27 pF Chip Input Capacitance**
- **1 kByte unified cache** for optimized code and data execution
- **Symmetric Crypto Processor (SCP)** for symmetric cryptography (DES, AES)
- **(Optional) Crypto engine (Crypto@2304T)** for asymmetric cryptography (RSA and ECC)
- **CRC module** with loadable initialization vector supporting ISO/IEC 3309, CCIT v.41 & HDLC X25
- Two 16-bit autoreload & Watch Dog Timers (WDT)
- External clock frequency 1 to 10 MHz
- **Internal clock frequency up to 33 MHz**
- **Adjustable internal frequency according to available power or required performance**
  - Increased internal frequency for maximum performance
  - Internal frequency is automatically adjusted to keep a given power limit
- Supply voltage range: 1.62 V to 5.5 V
- Support of current consumption limits
  - < 10 mA @ 5.5 V
  - < 6 mA @ 3.3 V
  - < 4 mA @ 1.98 V
- Operating temperature range: -25°C to +85°C
- Storing temperature range: -40°C to +125°C
- ESD protection larger than 4 kV (HBM)
- Power-saving sleep mode

2 Contactbased Interface

- **Enhanced UART for handling serial interface** in accordance with ISO/IEC 7816 part 3 **supporting transmission protocols T = 1 and T = 0 (support of clock division factor of 8)**

3 Contactless Interface

- **(Optional) contactless interface according to ISO/IEC 14443 for type A**
- Contactless interface according to ISO/IEC 14443 for type B
- Contactless interface according to ISO/IEC 18092 (NFC passive mode)
- **Data rates in both directions**
  - **up to 848 kbit/s in type A operation**
  - **up to 848 kbit/s in type B operation**
  - up to 424 kbit/s in ISO/IEC 18092 operation
- Anticollision & transmission protocol supported by open source application notes for ISO/IEC 14443 both type A & B
- (Unique) identification number available according to ISO/IEC 14443 (4/7/10 byte fixed, random)
- 256 bytes FIFO buffer for contactless data

4 Mifare Compatible Interface

- **Optional support of 1 Kbyte or 4 Kbyte Mifare compatible functionality**
- Compatible command set and operation controlled by firmware functions
- Support of multiple Mifare compatible memory portions on one controller
- Personalisation of memory portion also via contactbased interface

5 Anti Snooping

- Basic countermeasures against side-channel attacks
- Security Optimized Wiring
- Dedicated smart card controller micro-architecture

6 Memory Security

- **Memory Management and Protection Unit (MMU)** with 8 levels of hardware supported firewalls up to 16 Mbytes linear address space on each level
- Unique chip identification number for each chip
- MED – Memory Encryption/Decryption device for RAM, IFX-ROM and NVM in code and data areas

7 Security features

- **(Optional) Crypto engine with 2304 bit register size (Crypto@2304T)** for public key cryptography with key lengths of up to:
  - 2048 bits w/o CRT
  - 4096 bits with CRT
- (Optional) Support of Elliptic Curve Cryptography (ECC) based on GF(p) and GF(2^n) for up to 521 bits key length
- **Symmetric Crypto Processor (SCP)** for DES (incl. triple-key triple-DES) and AES acceleration (128, 192 and 256 bit key)
- **Pseudo Random Number Generator (PRNG)** and AIS-31 compliant **True Random Number Generator (TRNG)** – two independent modules
- Special Function Register (SFR) bus encryption
- Separate Watchdog Timer (WDT) incl. extended check point register for runtime check
- Self-Test Software (STS) concept
- Security reset mechanism
- **Sensors:**
  - Temperature sensor
  - Glitch sensor
  - Light sensors
  - Voltage sensors
  - Frequency sensors
  - Life test function for sensors (UMSLC)
- Security Optimized Wiring

8 Certification

- CC EAL 4+(high) targeted
- EMVCo targeted

9 SOLID FLASH™

- **Certified SOLID FLASH™ loader concept**
  - High speed flash loading for fast personalization (<10 s/512 Kbytes)
  - Optional SOLID FLASH™ programming service by Infineon
- Fast personalization mode = 1 ms per page
- Flexible page mode for 1 to 256 bytes write/erase operation for the whole NVM size
- Minimum of 500.000 write/erase cycles per page
- Typical data retention of >12 years @ 25°C
- Flash programming voltage generated on chip

10 Development Tools Overview

- Software Development Kit, SDK 70 (based on the DK251 kit from KEIL tools by ARM Ltd)
- FPGA based emulator ET70
- Contactless Reader Evaluation Kit
- Certified symmetric and asymmetric libraries on request
- Application Notes
- Worldwide application engineer team & customer dedicated field application engineers
- Regular customer trainings on hardware & software tools
- On-site trainings available on request

11 Supported Standards

- ISO/IEC 7816-3 3rd Edition, 2006-11-01
- ISO/IEC 14443 2nd Edition
- ISO/IEC 18092
- GSM 11.11, 11.12, 11.18
- ETSI TS 102 221 V9.2.0 (2010-10)
- EMV 4.2
- EMV Contactless V2.1

12 Document References

- Confidential Hardware Reference Manual (HRM)
- Confidential Product List
- Confidential Programmers Reference Manual (PRM)
- Confidential Security Guidance
- Confidential Card Coil Design Guide and Card Coil Calculator
- Confidential Chip qualification report
- Confidential Chip delivery specification for wafer with chip-layout (die size, orientation, step size)
- Confidential Module specification containing package descriptions
- Confidential Module qualification report

13 Ordering Information

Table 1 Package Product Information [1)]

Type	Package	Voltage Range	Temperature Range	Frequency Range (external UART clock)	Frequency Range (internal CPU clock)
SLE 77CLF(X)2400P(M) – M8.4	M8.4 [2)]	1.62 V to 5.5 V	– 25°C to +85°C	1 MHz to 10 MHz	Up to 33 MHz
SLE 77CLF(X)2400P(M) – MCC8	MCC8 [3)]				
SLE 77CLF(X)2400P(M) – C	Die sawn				

1) Ordering Codes are available on request

2) Dual Interface Module (M8.4)

3) Pure Contactless Module (MCC8): for standard thickness inlays (330 µm)

Flash initialization/personalization and additional delivery forms available upon request. For ordering information please refer to the Hardware Reference Manual and contact your sales representative.

14 Pin Description & Module

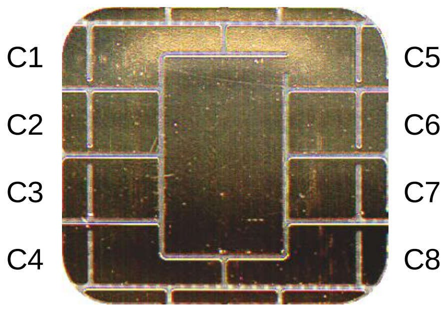

Figure 1 M8.4 Pin Configuration Wire-bonded Module (top view)

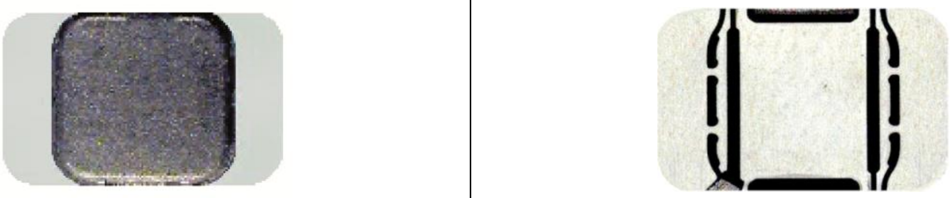

Figure 2 MCC8 Mold Module (top and rear view)

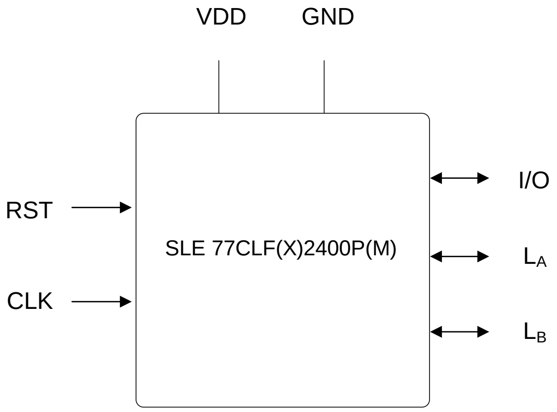

Figure 3 Pin Configuration

Figure 4

Table 2 Pin Definitions and Functions

Card Contact	Symbol	Function
C1	VDD	Positive Supply Voltage
C2	RST	UART reset input
C3	CLK	UART clock input
C5	GND	Ground
C7	I/O	Bi-directional data port for UART communication
	LA	Coil connection pin L_A
	LB	Coil connection pin L_B

15 General Description

The SLE 77CLF(X)2400P(M) is a member of the SLE 77P-series of Infineon Technologies, optimized for Dual Interface Payment and applications. This security controller is manufactured in advanced 90 nm technology.

Infineon SOLID FLASH™ concept: The unique NVM combines the advantages of a high speed code Flash with the flexibility and reliability of a true E²PROM with regard to byte-wise addressable pages and data retention.

16 Performance

The internal clock frequency can be adjusted to a level of up to 33 MHz either as a multiple of 1 to 8 of the external frequency or independent of the clock rate of the terminal with the help of the internal clock. It is adjustable according to either available power requirements or required performance:

- Increased internal clock frequency for maximum performance, e.g. for high performance with max. frequency.
- Automatically adjusted frequency to keep a given maximum power consumption.

17 Security

The overall security concept of this family is based upon the combination of security measures in hardware and in software, which enables the customer to bring in their own security software expertise. Software countermeasures are an important part of the overall security concept in order to achieve the targeted certificates. The security guideline for software development shall be respected.

The set of security features has been tailored to fit the requirements of mid range payment applications, and contains

- Basic protection mechanism against fault attacks
- Basic protection mechanism against probing & forcing
- Basic protection mechanism against side channel attacks

18 Memory & Block Diagram

The SLE 77CLF(X)2400P(M) offers 6 Kbytes RAM and 240 Kbytes SOLID FLASH™ to fulfill the increased requirements of payment applications

Unlike the SLE 66CxxxPE family, for example, SLE 70 controllers store both code and data in a linear 16 MB memory space, allowing direct access without the need to swap memory segments.

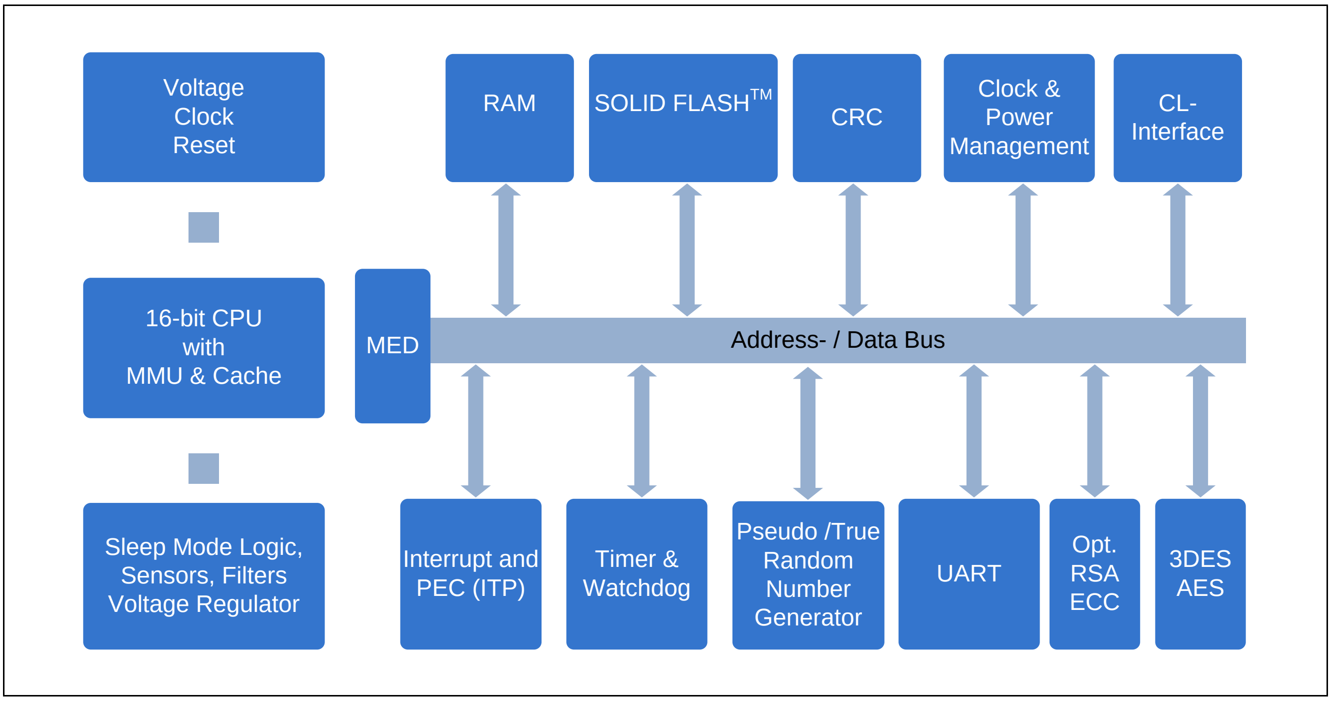

Figure 5 Block Diagram SLE 77CLF(X)2400P(M)

19 Peripherals

To enable high performance cryptography, the SLE 70 controllers provide two cryptographic coprocessors. The Crypto@2304T for modular arithmetic and asymmetric cryptographic algorithms, plus the Symmetric Crypto Processor (SCP) for symmetric cryptographic algorithms.

(Optional) Crypto@2304T

The (optional) Crypto@2304T is a high security and high performance crypto coprocessor. It is equipped with its own RAM of 1152 bytes and supports all of today’s known public key algorithms based on large integer modular arithmetic with operands. It allows fast and efficient calculation of arithmetic operations such as RSA and ECC with register lengths of up to 2304 bits. The features of the Crypto@2304 will be supported by the RSA2048, RSA4096 and ECC521 (ECDSA, ECDH) libraries.

SCP

The SCP (Symmetric Crypto Processor) module supports symmetrical crypto algorithms according to the Data Encryption Standard (DES) in the Electronic Code Book Mode, as well as Cipher Block Chaining. The AES (Advanced Encryption Standard) component of the SCP module performs AES-compliant operations for three different key lengths (128, 192, 256 bit).

ICU and PEC

The Interrupt Control Unit processes interrupt requests from different sources to run an interrupt service routine (ISR). Data can be directly transferred between memory locations with minimal CPU activity for fast interaction with peripherals by using so-called Peripheral Event Channels (PECs). The channels can be assigned individually to peripherals or chained together to enable continuous transfer without handover delay between the channels. This is of particular advantage when power aware programming is required.

CRC

The enhanced CRC module allows the easy generation of checksums according to ISO/IEC 3309 (16-bit-CRC) and offers a loadable initialization vector for optimized Java support.

UART

The improved Universal Asynchronous Receiver/Transmitter Interface (UART) provides serial communication between the controller and the interface device (e.g. card reader). It supports the half-duplex transmission protocols T = 0 and T = 1 according to ISO/IEC 7816-3 as well as a larger FIFO and a clock division factor of 8. All relevant transmission parameters can be adjusted by software, such as the clock division factor, direct/inverse convention and the number of stop bits. Additionally, the I/O port can be driven by communication routines realized in software.

CL-Interface

The SLE 77 supports all contactless controller standards (ISO/IEC 14443 Type A & B (optional); ISO/IEC 18092 passive mode) and is prepared for future contactless applications thanks to an interface management module (IMM). Its outstanding communication robustness allows an easy integration in existing infrastructure. Data transfer rates for both ISO/IEC 14443 type A and type B from 106 kbit/s of up to 848 kbit/s in both directions are supported over the full ISO-range.

Timer and Watchdog

The two integrated 16-bit auto-reload timers support an easy implementation of advanced communication protocols (T = 0 and T = 1) and all other critical timing processes. Both timers have the same functionality and support the same features. The Watch Dog Timer (WDT) is a circuit that monitors controller operation by automatically initiating a security reset if a specified period without an adequate response elapses after occurrence of a hardware or software irregularity.

RNG

There are two different Random Number Generators (RNGs) on the SLE 77: a pseudo RNG (PRNG), and a separate, AIS-31 compliant true RNG (TRNG). The PRNG provides a key-loading mode and streaming mode.

Power Management Module

The SLE 77 controllers power management module offers advanced specific power-saving modes. In the halt mode the CPU clock is stopped, but the clocks serving the peripheral units continue running. In the sleep mode the chip’s oscillator stops and the controller remains in a static state. The chip is returned to the normal operating mode in response to an interrupt or a reset.

20 Glossary

AES	Advanced Encryption Standard
CLK	Clock
CRC	Cyclic Redundancy Check
CRT	Chinese Remainder Theorem
CPU	Central Processing Unit
CMOS	Complementary Metal-Oxide Semiconductor
DES	Data Encryption Standard
DFA	Differential Fault Analysis
DPA	Differential Power Analysis
DEMA	Differential Electromagnetic Analysis
ECC	Elliptic Curve Cryptography
ECDH	Elliptic Curve Diffie Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
EDC	Error Detection Code
EMV	Europay Mastercard Visa Co compliance testing
E^2PROM	Electrically Erasable Programmable Read-Only Memory (equivalent to NVM)
ESD	Electrostatic Discharge, release of static electricity that can damage a chip
ETSI	European Telecommunication Standards Institute
FIFO	First In, First Out
FPGA	Field Programmable Gate Array
GND	Ground
GSM	Global System for Mobile Communication
HBM	Human Body Model
ID	Identification
I/O	Input/Output
ISO/IEC	International Organization for Standardization/International Electrotechnical Commission
ISR	Interrupt Service Routine
MED	Memory Encryption Decryption unit
MMU	Memory Management Unit
NVM	Non Volatile Memory
OS	Operating System
PEC	Peripheral Event Channel
PFD	Post Failure Detection
PRNG	Pseudo Random Number Generator
RAM	Random Access Memory
ROM	Read-Only Memory
RSA	Rivest Shamir Adleman algorithm
RST	Reset
SCP	Symmetric Crypto Processor
SDK CC	Software Development Kit Chip Card
SEMA	Simple Electromagnetic Analysis
SFR	Special Function Register
SPA	Simple Power Analysis
STS	Self-Test Software

T = 0, T = 1	Communication Protocols defined in ISO 7816 standard
TRNG	True Random Number Generator
UART	Universal Asynchronous Receiver/Transmitter
UmSLC	User mode Security Life Control
VDD	Positive Supply Voltage
PLL	Phase-Locked Loop
WDT	Watch Dog Timer

21 Sales Code Description

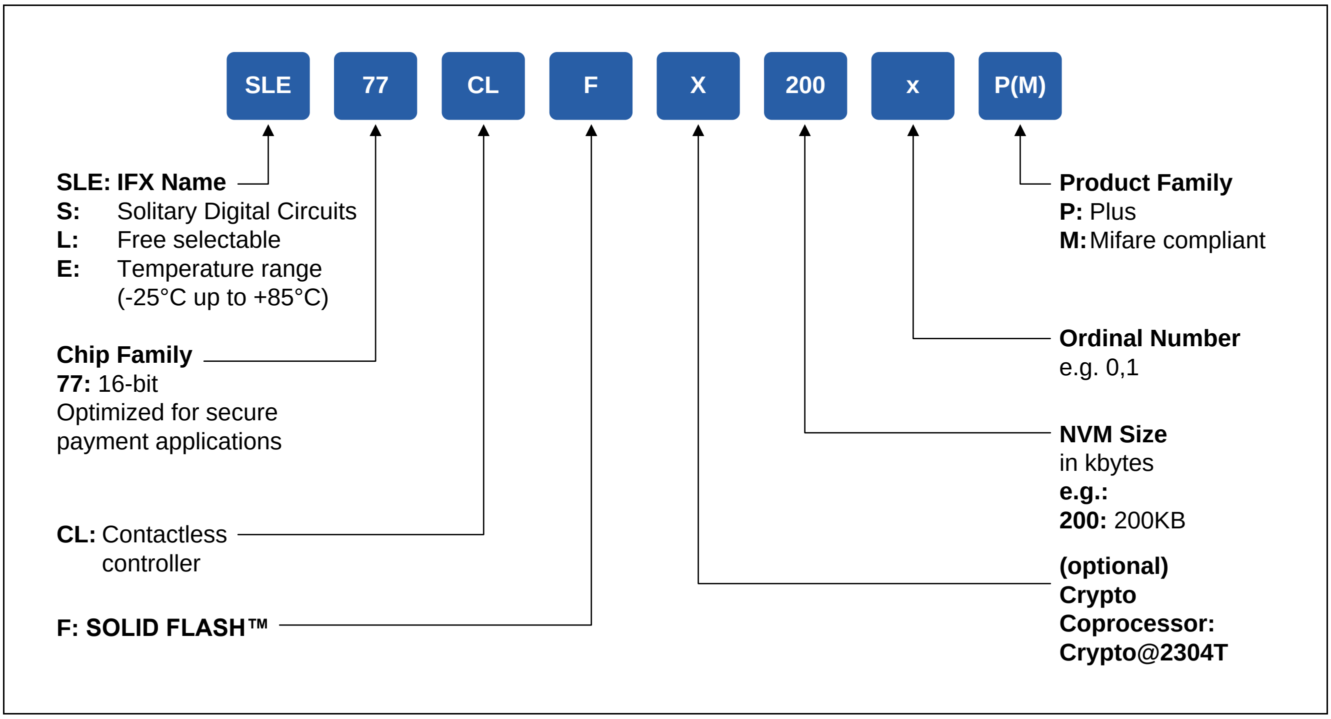

Figure 6 Sales Code Description (example)

Infineon Technologies – innovative semiconductor solutions for energy efficiency, mobility and security.

www.infineon.com

Published by Infineon Technologies AG