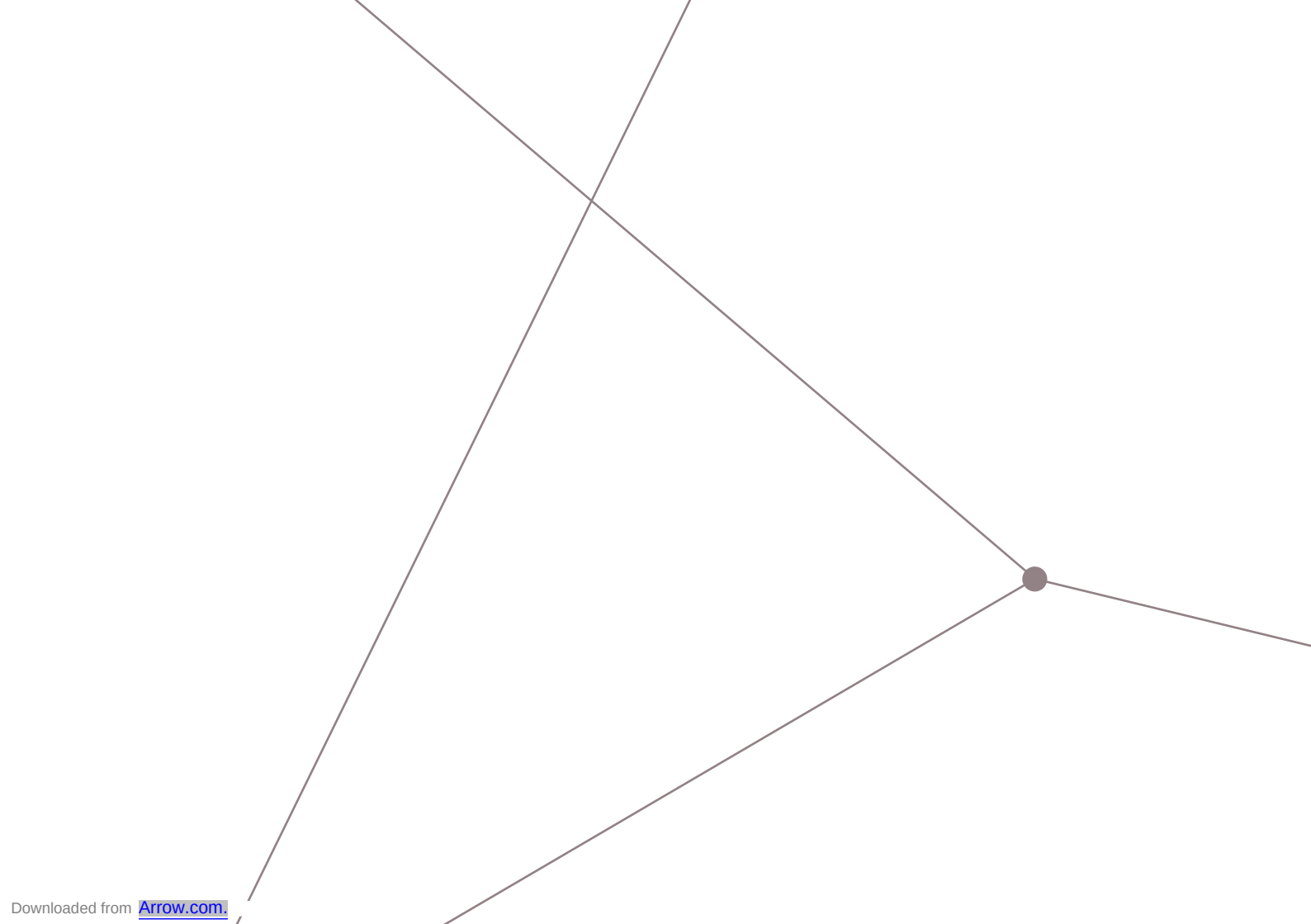
Infineon's Security Solutions Portfolio

Security for the connected world

www.infineon.com/security



Security for the connected world

In an increasingly connected world, securing interaction and communication between people, electronic devices and infrastructures has become a number one priority. As the leading provider of security solutions, Infineon offers tailored, ready-to-use security solutions serving a wide range of applications from smart cards to new, emerging use cases. Infineon is the partner of choice for countless customers across multiple markets thanks to its outstanding security expertise based on almost 30 years of experience, a steady stream of customer-driven technology innovations, in-depth and holistic system competence and the broadest security solution portfolio in the market.

www.infineon.com/security

Technologies

Integrity Guard

The smartest security concept in the industry
Rely on Integrity Guard's highly sophisticated digital security architecture, including a fully encrypted data path and self-checking dual CPU core.

Boosted NFC

NFC security solution for smallest form factors
Deliver payment solutions for connected devices with ultra-low power consumption, small PCB footprints and extraordinary contactless performance.

SOLID FLASH™

Flexible and robust memory built on a comprehensive security concept
Master your security applications quickly with SOLID FLASH™ – a flexible, non-volatile memory technology.

Mega Memory

Unrivalled total memory sizes
Enable your next-generation eGovernment documents such as ePassports and multi-application eID cards based on LDS 2.0.

Coil on Module

Simplified dual-interface card design and manufacturing
Get to market significantly faster than the competition with our award-winning Coil on Module package technology.

VHBR

The fastest contactless performance
Accelerate your applications with support for Very High Bit Rates (VHBR) of up to 6.8 Mbit/s.

Open standard & trademark solutions

cipurse

CIPURSE™ – Open security standard

- Is built on proven standards such as ISO/IEC 7816, AES-128 and ISO/IEC 14443-4.
- Provides a single, consistent set of security, personalization, administration and lifecycle management functions.
- Includes advanced security mechanisms such as unique cryptographic protocol for inherent protection against differential power analysis (DPA) and differential fault attacks (DFA).
- Offers three distinct development profiles enabling a complete range of products spanning tickets, cards and mobile phones.

CIPURSE™ is a trademark of the OSPT Alliance

SECORA™

SECORA™ is Infineon's family of one-stop security solutions with integrated operating system (OS) providing a cost-efficient way to fast and agile implementations

SECORA™ Pay offers card issuers, card manufacturers and personalizers a cost-effective route to fast and agile implementation. Based on a solid chip platform with an integrated Java Card operating system, SECORA™ Pay is highly secure and reliable, also delivering the best price-performance ratio.

SECORA™ Connect empowers smart wearables and IoT devices with NFC security capabilities such as payment, transport and access. The solution family consists of various products and complementary services for connected devices and enables ultra-low power consumption for longest battery life-time.

SECORA™ ID is our new ready-to-go Java Card™ solution optimized for all electronic identification (eID) applications. It enables security printers and card manufacturers to accelerate their time-to-market through ready-to-use applets supporting rapid project migration.

OPTIGA™

OPTIGA™ security solutions are designed for easy integration into embedded systems to protect the confidentiality, integrity and authenticity of information and devices. These hardware-based security solutions scale from basic authentication chips to sophisticated implementations.

OPTIGA™ Trust includes turnkey products for smaller platforms as well as programmable solutions, supporting individual needs in the field of embedded authentication and brand protection as well as a host of other security applications.

OPTIGA™ TPM is a standardized security building block used in Trusted Computing and embedded applications. OPTIGA™ TPMs are serving as the basis of a robust implementation of IoT use cases such as secured communication, device authentication, remote management and maintenance, in-field remote feature upgrade, and activation. OPTIGA™ TPM is fully compliant with the Trusted Computing Group (TCG) Standards and ISO/IEC11889:2015.

Contents

Payment

	Dual-interface security controllers			
Product name [1]	**SLC37PDzxxx** new SOLID FLASH™ Coil on Module	**SLC36PDzxxx** new SOLID FLASH™ Coil on Module	**SLC32PDzxxx** SOLID FLASH™ Coil on Module	**SLC32PMzxxx** SOLID FLASH™ Coil on Module
Product description	Dual-interface security cryptocontroller for multi-application and wearables payment use cases supporting multi-interface	Dual-interface security cryptocontroller for traditional payment use cases	Dual-interface security cryptocontroller for traditional payment use cases	Dual-interface security cryptocontroller for multi-application and wearables payment use cases supporting multi-interface
Interfaces	ISO 7816, ISO 14443 A/B, ISO 18092 passive mode, optimized for small antenna sizes, optional NRG™ (ISO/IEC 14443-3 type A with CRYPTO1)	ISO 7816 / I2C, ISO 14443 A/B, ISO 18092 passive mode, optimized for small antenna sizes, optional NRG™ (ISO/IEC 14443-3 type A with CRYPTO1)	ISO 7816, ISO 14443 A/B, ISO 18092 passive mode, optimized for small antenna sizes, optional NRG™ (ISO/IEC 14443-3 type A with CRYPTO1)	ISO 7816 / I2C, ISO 14443 A/B, ISO 18092 passive mode, optimized for small antenna sizes, optional NRG™ (ISO/IEC 14443-3 type A with CRYPTO1)
NVM	512, 448, 400 kByte	352, 280 kByte	180, 212, 228, 268, 300, 348 kByte	400, 448 kByte
RAM	14 kByte	12 kByte	10 kByte	12 kByte
CPU	32-bit Arm® SecurCore® SC300	32-bit Arm® SecurCore® SC300	16-bit	16-bit
Symmetrical cryptography	AES up to 256-bit, DES, 3DES	AES up to 256-bit, DES, 3DES	AES up to 256-bit, DES, 3DES	AES up to 256-bit, DES, 3DES
Asymmetrical cryptography	ECC up to 521-bit, RSA up to 4096-bit	ECC up to 521-bit, RSA up to 4096-bit	ECC up to 521-bit, RSA up to 4096-bit	ECC up to 521-bit, RSA up to 4096-bit
Ambient temperature	-25°C to +85°C	-25°C to +85°C	-25°C to +85°C	-25°C to +85°C
Delivery forms	Coil on Module, sawn wafer, 6/8 pin dual-interface modules and contactless modules	Coil on Module, sawn wafer, bumped wafer, 6/8 pin dual- interface modules and contactless modules	Coil on Module, sawn wafer, 6/8 pin dual-interface modules and contactless modules	Coil on Module, sawn wafer, bumped wafer, 6/8 pin dual-interface modules and contactless modules
Certifications	Targeted EMVCo, CC EAL6+ high, CUP	Targeted EMVCo, CC EAL6+ high, CUP	CC EAL6+ high, CUP, EMVCo	CC EAL6+ high, EMVCo

[1] Please note that xxx stands for NVM size, z – different interfaces

Payment

	Dual-interface security controllers		Contact-based security controllers	
Product name [1]	**SLC52WMzxxx** SOLID FLASH™ Integrity Guard	**SLC52BMzxxx** new SOLID FLASH™ Integrity Guard	**SLC37PCB240** SOLID FLASH™	**SLC32PCAxxx** SOLID FLASH™
Product description	Boosted NFC SE	Biometric system authentication with a biometric sensor in payment smart cards	Contact-based security cryptocontroller	Contact-based security cryptocontroller
Interfaces	ISO 7816 / I2C, ISO 14443 A/B, ISO 18092 passive mode, optimized for small antenna sizes, optional NRG™ (ISO/IEC 14443-3 type A with CRYPTO1)	ISO 7816 / I2C, ISO 14443 A/B, ISO 18092 passive mode, optimized for small antenna sizes, optional NRG™ (ISO/IEC 14443-3 type A with CRYPTO1)	ISO 7816	ISO 7816
NVM	448, 800 kByte	448, 800 kByte	240 kByte	160, 180, 212, 228, 268, 300 kByte
RAM	12 kByte	12, 16 kByte	10 kByte	8 kByte
CPU	16-bit	16-bit	32-bit Arm® SecurCore® SC300	16-bit
Symmetrical cryptography	AES up to 256-bit, DES, 3DES	AES up to 256-bit, DES, 3DES	DES, AES	AES up to 256-bit, DES, 3DES
Asymmetrical cryptography	ECC up to 521-bit, RSA up to 4096-bit	ECC up to 521-bit, RSA up to 4096-bit	–	ECC up to 521-bit, RSA up to 4096-bit
Ambient temperature	-25°C to +85°C	-25°C to +85°C	-25°C to +85°C	-25°C to +85°C
Delivery forms	Sawn wafer, USON-10-2	Sawn wafer	Sawn wafer, 6/8 contact-based modules (MFC6.6, MFC6.8)	Sawn wafer, 6/8 contact-based modules (MFC6.6, MFC6.8)
Certifications	CC EAL6+ high, EMVCo	CC EAL6+ high, EMVCo	EMVCo	CC EAL6+ high, EMVCo

[1] Please note that xxx stands for NVM size, z – different interfaces

	SECORA™ Pay [2]		
Product variants	**SECORA™ Pay S** SOLID FLASH™ Coil on Module	**SECORA™ Pay X** SOLID FLASH™ Coil on Module	**SECORA™ Pay W** SOLID FLASH™
Product description	Ready-to-use and optimized chip solution portfolio for standard payment cards for global schemes such as Visa, Mastercard, American Express and Discover.	Flexible platform to address multi-application payment cards and domestic schemes. SECORA™ Pay X is an enablement platform giving customers flexibility to support EMV-based payment schemes and local content in combination with Infineon's ready-to-use reference solutions for Visa, Mastercard, American Express, Discover and CIPURSE™.	Turnkey solution for payment accessories, SECORA™ Pay W is based on innovative and alternative packaging. It is designed to meet market needs for non-connected, passive wearable devices such as rings, wristbands or key fobs that are not powered by a battery.
Operating system	Java Card S GlobalPlatform 2.2.1	Java Card 3.0.4 GlobalPlatform 2.2.1	Java Card 3.0.4 GlobalPlatform 2.2.1
Interfaces	ISO 7816, ISO 14443	ISO 7816, ISO 14443	ISO 14443
Typical application	Standard payment cards	Multi-application payment cards	Smart Accessories

[2] For further information on SECORA™ Pay, available products and applets, available configurations, delivery forms, sample availability, support, tools and conditions, please contact your Infineon Technologies sales representative.

Payment

	SECORA™ Connect	
Product Variants	**SECORA™ Connect boosted** new SOLID FLASH™ Boosted NFC	**SECORA™ Connect passive NFC** new SOLID FLASH™
Product description	SECORA™ Connect Boosted is an all-in-one turnkey NFC solution for connected smart wearables enabling ultra-small physical footprint.	SECORA™ Connect Passive NFC is a security solution for smart wearables enabling battery-less NFC transaction.
Operating sytem and Applications	Java card 3.0.4, Global platform 2.2.1, Visa Mobile Payment Application, Mastercard M/Chip Mobile application, Proximity Payment System Environment (PPSE), CDCVM, CIPURSE™, and many more upon request	Java card 3.0.4, Global platform 2.2.1, Visa Mobile Payment Application, Mastercard M/Chip Mobile application, Proximity Payment System Environment (PPSE), CDCVM, CIPURSE™, and many more upon request
Interfaces	ISO7816, ISO 14443, I2C	ISO7816, ISO 14443, I2C
Delivery forms	System-in-package with integrated antenna, Multi-Chip-Package	SMD package PG-USON-8-3
Typical applications	Payment, transport ticketing, access control	Payment, transport ticketing, access control
Customer benefits	Fast and easy host integration, longest battery lifetime, one SE fits all, efficient SE management in the field, increased design flexibilty	Fast and easy host integration, longest battery lifetime, one SE fits all, efficient SE management in the field, increased design flexibilty

Mobile Communication

	SIM & UICCs			
Product name [3]	**SLC 14MCOxxx**	**SLC 14MCOxxx**	**SLE 76CF2564P**	**SLE 76CFxxx2P**
Product description	32-bit SIM card controller	32-bit SIM card controller	16-bit SIM card controller	16-bit SIM card controller
Interfaces	ISO 7816	ISO 7816	ISO 7816	ISO 7816
NVM	256, 288, 312, 340 kByte	384, 420, 480 kByte	256 kByte	296, 320, 344, 360 kByte
RAM	10 kByte	12 kByte	9 kByte	9 kByte
CPU	32-bit	32-bit	16-bit	16-bit
Symmetrical cryptography	–	–	–	–
Asymmetrical cryptography	–	–	–	–
Ambient temperature	-25°C to +85°C	-25°C to +85°C	-25°C to +85°C	-25°C to +85°C
Delivery forms	Sawn wafer	Sawn wafer	Sawn wafer	Sawn wafer
Typical applications	SIM and UICC for mobile communication	SIM and UICC for mobile communication	SIM and UICC for mobile communication	SIM and UICC for mobile communication
Certifications	–	–	–	–

[3] Please note that xxx in product names stands for NVM size

SLE 76CF4002P	SLE 76CFxxx0P	SLE 97CNFXxxx0PE Optimized SOLID FLASH™	SLE 97CUNFXxxx0PE SOLID FLASH™	SLC17ECB800B SOLID FLASH™
16-bit SIM card controller	16-bit SIM card controller	32-bit SWP SIM card security cryptocontroller	32-bit USB and SWP SIM card security cryptocontroller	32-bit security cryptocontroller for SIM and eSIM applications
ISO 7816	ISO 7816	ISO 7816, NRG™ (ISO/IEC 14443-3 type A with CRYPTO1), SWP	ISO 7816, NRG™ (ISO/IEC 14443-3 type A with CRYPTO1), SWP, USB	ISO 7816, GPIO
400 kByte	448, 504 kByte	600, 800 kByte, 1, 1.3, 1.5 MByte	800 kByte, 1 MByte	800 kByte
12 kByte	12 kByte	32 kByte	32 kByte	20 kByte
16-bit	16-bit	32-bit	32-bit	32-bit
–	AES up to 256-bit, DES, 3DES	AES up to 256-bit, DES, 3DES	AES up to 256-bit, DES, 3DES	AES up to 256-bit, DES, 3DES
–	–	ECC up to 521-bit, RSA up to 4096-bit	ECC up to 521-bit, RSA up to 4096-bit	–
-25°C to +85°C	-25°C to +85°C	-25°C to +85°C	-25°C to +85°C	-25°C to +85°C
Sawn wafer	Sawn wafer	SMD, sawn wafer	SMD, sawn wafer	Sawn wafer, MFF2, USON-8-6, USON-6-2, USON-10-2, XFWLB-6-2
SIM and UICC for mobile communication	SIM and UICC for mobile communication	SIM and UICC for mobile communication, SWP UICC for NFC	SIM and UICC for mobile communication	SIM and eSIM for cellular IoT devices
–	–	CC EAL5+ high, EMVCo	CC EAL5+ high, EMVCo	CC EAL5+ high

Mobile Communication

	SIM & UICCs	
Product name [3]	**SLC16ECB240B** SOLID FLASH™	**SLC37MWAxxx** new NFC Optimized SOLID FLASH™
Product description	32-bit security cryptocontroller for SIM and NB-IoT SIM applications	32-bit USB and SWP SIM card security cryptocontroller
Interfaces	ISO 7816	GPIOs, ISO 7816, NRG™ (ISO/IEC 14443-3 type A with CRYPTO1), SPI, SWP, I2C, USB
NVM	240 kByte	1.0, 1.2, 1.5, 2.0 MByte
RAM	12 kByte	48 kByte
CPU	32-bit	32-bit
Symmetrical cryptography	AES up to 256-bit, DES, 3DES	AES up to 256-bit, DES, 3DES
Asymmetrical cryptography	–	ECC up to 521-bit, RSA up to 4096-bit
Ambient temperature	-25°C to +85°C	-25°C to +85°C
Delivery forms	Sawn wafer, USON-8-5, USON-10-2, XFWLB-6-3	Sawn wafer, CSP, SMD
Typical applications	NB-IoT SIM for cellular IoT devices	SIM and UICC for mobile communication
Certifications	CC EAL5+ high	CC EAL6+ high, EMVCo

[3] Please note that xxx in product names stands for NVM size

SIM/eSIM/V2X Automotive

	eUICC automotive (V2X)			
Product name [3]	**SLI 76CF3600P** SOLID FLASH™	**SLI 76CF5120P** SOLID FLASH™	**SLI 97Cxxx0PE** SOLID FLASH™	**SLI 97CSINFXxxx0PE** SOLID FLASH™
Product description	Security cryptocontroller, optimized for automotive applications	Security cryptocontroller, optimized for automotive applications	Security cryptocontroller, optimized for automotive applications	Security cryptocontroller, optimized for automotive applications
Interfaces	ISO 7816	ISO 7816	ISO 7816, SWP	ISO 7816, SWP, I2C, SPI
NVM	360 kByte	504 kByte	608 kByte, 800 kByte, 1 MByte	800 kByte, 1 MByte
RAM	8 kByte	12 kByte	32 kByte	32 kByte
CPU	16-bit	16-bit	32-bit	32-bit
Symmetrical cryptography	AES up to 256-bit, DES, 3DES	AES up to 256-bit, DES, 3DES	AES up to 256-bit, DES, 3DES	AES up to 256-bit, DES, 3DES
Asymmetrical cryptography	–	–	ECC up to 521-bit, RSA up to 4096-bit	ECC up to 521-bit, RSA up to 4096-bit
Ambient temperature	-40°C to +105°C	-40°C to +105°C	-40°C to +105°C	-40°C to +105°C
Delivery forms	MFF2 (VQFN-8-4)	MFF2 (VQFN-8-4)	MFF2 (VQFN-8-4)	VQFN-32-13
Typical applications	Automotive SIM	Automotive SIM	Automotive eSIM, eCall	Automotive eSIM, eCall, V2X
Certifications	–	–	CC EAL5+ high	CC EAL5+ high

[3] Please note that xxx in product names stands for NVM size

SLI37CMxxx new SOLID FLASH™
Security cryptocontroller, optimized for automotive applications
ISO 7816, SWP, I2C, SPI and GPIO's
1 MByte, 1332 kByte, 1536 kByte, 2 MByte
48 kByte
32-bit
AES up to 256-bit, DES, 3DES
ECC up to 521-bit, RSA up to 4096-bit
-40°C to +105°C
MFF2 (VQFN-8-4), VQFN-32-13
Automotive eSIM, eCall, V2X, Trust Anchor
CC EAL6+ high

SIM/eSIM Industrial

	eUICC industrial (M2M)			
Product name [3]	**SLM 76CFxxx1P** SOLID FLASH™	**SLM 76CF5120P** SOLID FLASH™	**SLM 97CFxxx0PE** SOLID FLASH™	**SLM 97CFXxxx0PE** SOLID FLASH™
Product description	Security controller, optimized for industrial applications (SIM)	Security controller, optimized for industrial applications (SIM)	Security controller, optimized for industrial applications (eSIM)	Security cryptocontroller, optimized for industrial applications (eSIM)
Interfaces	ISO 7816	ISO 7816	ISO 7816	ISO 7816
NVM	256, 320, 360 kByte	504 kByte	608, 800 kByte, 1 MByte	608, 800 kByte, 1 MByte
RAM	8 kByte	12 kByte	32 kByte	32 kByte
CPU	16-bit	16-bit	32-bit	32-bit
Symmetrical cryptography	AES up to 256-bit, DES, 3DES	AES up to 256-bit, DES, 3DES	–	AES up to 256-bit, DES, 3DES
Asymmetrical cryptography	–	–	–	ECC up to 521-bit, RSA up to 4096-bit
Ambient temperature	-40°C to +105°C	-40°C to +105°C	-40°C to +105°C	-40°C to +105°C
Delivery forms	MFF2, P-M2M4.7, sawn wafer	MFF2, P-M2M4.7, sawn wafer	MFF2, P-M2M4.7, sawn wafer, WF WLB-16	MFF2, P-M2M4.7, sawn wafer, WF WLB-16
Typical applications	–	–	–	–
Certifications	–	–	CC EAL5+ high	CC EAL5+ high

[3] Please note that xxx in product names stands for NVM size

SLM 97CNFxxx0PE SOLID FLASH™	SLM 97CNFXxxx0PE SOLID FLASH™	SLM 97CSINFXxxx0PE SOLID FLASH™	SLM17ECB800B new SOLID FLASH™	SLM16ECB240B new SOLID FLASH™
Security controller, optimized for industrial applications (eSIM, NFC-enabled)	Security cryptocontroller, optimized for industrial applications (eSIM, NFC-enabled)	Security cryptocontroller, optimized for industrial applications	Security cryptocontroller, optimized for industrial applications (M2M SIM and eSIM)	Security cryptocontroller, optimized for industrial applications (M2M SIM)
ISO 7816, SWP	ISO 7816, SWP	I2C, ISO 7816, SPI, SWP	ISO 7816, GPIO	ISO 7816
608, 800 kByte, 1 MByte	608, 800 kByte, 1 MByte	800 kByte, 1 MByte	800 kByte	240 kByte
32 kByte	32 kByte	32 kByte	20 kByte	12 kByte
32-bit	32-bit	32-bit	32-bit	32-bit
–	AES up to 256-bit, DES, 3DES	AES up to 256-bit, DES, 3DES	AES up to 256-bit, DES, 3DES	AES up to 256-bit, DES, 3DES
–	ECC up to 521-bit, RSA up to 4096-bit	ECC up to 521-bit, RSA up to 4096-bit	–	–
-40°C to +105°C	-40°C to +105°C	-40°C to +105°C	-40°C to +105°C	-40°C to +105°C
MFF2, P-M2M4.7, sawn wafer, WF WLB-16	MFF2, P-M2M4.7, sawn wafer, WF WLB-16	VQFN-32-13	MFF2, sawn wafer, USON-8-6, USON-6-2, USON-10-2, XFWLB-6-2	Sawn wafer, USON-8-5, USON-10-2, XFWLB-6-3
–	–	–	–	–
CC EAL5+ high	CC EAL5+ high	CC EAL5+ high	CC EAL5+ high	CC EAL5+ high

Near-Field Communication

	SWP UICCs		Embedded Secure Elements (eSE)
Product name [3]	**SLE 97CUNFXxxx0PE** SOLID FLASH™	**SLC37MWAxxx** new NFC Optimized SOLID FLASH™	**SLC37ESAxxx** NFC Optimized SOLID FLASH™
Product description	32-bit USB and SWP SIM card security cryptocontroller	32-bit USB and SWP SIM card security cryptocontroller	32-bit SWP security cryptocontroller for embedded secure element
Interfaces	ISO 7816, NRG™ (ISO/IEC 14443-3 type A with CRYPTO1), SWP, USB	GPIOs, ISO 7816, NRG™ (ISO/IEC 14443-3 type A with CRYPTO1), SPI, SWP, I2C, USB	GPIOs, ISO 7816, NRG (ISO/IEC 14443-3 type A with CRYPTO1), SPI, SWP
NVM	600, 800 kByte, 1, 1.3, 1.5 MByte	1.0, 1.2, 1.5, 2.0 MByte	1.2, 1.5, 2.0 MByte
RAM	32 kByte	48 kByte	48 kByte
ROM	–	–	–
CPU	32-bit	32-bit	32-bit
Symmetrical cryptography	AES up to 256-bit, DES, 3DES	AES up to 256-bit, DES, 3DES	AES up to 256-bit, DES, 3DES
Asymmetrical cryptography	ECC up to 521-bit, RSA up to 4096-bit	ECC up to 521-bit, RSA up to 4096-bit	ECC up to 521-bit, RSA up to 4096-bit
Ambient temperature	-25°C to +85°C	-25°C to +85°C	-25°C to +85°C
Delivery forms	SMD (VQFN-8), sawn wafer	Sawn wafer, CSP, SMD	CSP, SMD, sawn wafer
Typical applications	SIM and UICC for mobile communication	SIM and UICC for mobile communication	NFC embedded secure element - IC
Certifications	CC EAL5+ high, EMVCo	CC EAL6+ high, EMVCo	CC EAL6+ high, EMVCo

[3] Please note that xxx in product names stands for NVM size

Boosted NFC Secure Elements		
SLE 77CAFX2400P(M) Optimized SOLID FLASH™	**SLE 78CAFX1M1SPHM** Integrity Guard Optimized SOLID FLASH™	**SLE 78CAFX4000P(M)** Integrity Guard Optimized SOLID FLASH™
Security cryptocontroller designed for boosted NFC	Boosted NFC secure element (SE)	Boosted NFC secure element (SE)
ISO 7816, ISO 14443 A/B, ISO 18092 via ACLB interface and external active booster, optional NRG™ (ISO/IEC 14443-3 type A with CRYPTO1)	ACLB, I2C, ISO 7816, NRG™ (ISO/IEC 14443-3 type A with CRYPTO1)	ACLB, ISO 7816, NRG™ (ISO/IEC 14443-3 type A with CRYPTO1)
240 kByte	628 kByte	400 kByte
6 kByte	12 kByte	8 kByte
–	444 kByte	–
16-bit	Dual 16-bit	Dual 16-bit
DES, 3DES	AES up to 256-bit, DES, 3DES, ECC, RSA	AES up to 256-bit, DES, 3DES, ECC, RSA
ECC up to 521-bit, RSA up to 4096-bit	ECC up to 521-bit, RSA up to 4096-bit	ECC up to 521-bit, RSA up to 4096-bit
-25°C to +85°C	-25°C to +85°C	-25°C to +85°C
Sawn wafer	Sawn wafer	Sawn wafer
Secure element with ultra-small antenna for wearable or other smart devices	–	–
CC EAL5+ high, EMVCo	CC EAL6+ high, EMVCo	CC EAL6+ high, EMVCo

Near-Field Communication

	Boosted NFC Secure Elements		
Product name [4]	**SLE 78CAFX5xxxSPHM** Integrity Guard, Optimized, SOLID FLASH™	**SLE 78CAFX628SPHM** Integrity Guard, Optimized, SOLID FLASH™	**SLE 78CAX5xxxSPHM** Integrity Guard, Optimized, SOLID FLASH™
Product description	Boosted NFC secure element (SE)	Boosted NFC secure element (SE)	Boosted NFC secure element (SE)
Interfaces	ACLB, GPIOs, ISO 7816, NRG™ (ISO/IEC 14443-3 type A with CRYPTO1), SPI	ACLB, I2C, ISO 7816, NRG™ (ISO/IEC 14443-3 type A with CRYPTO1)	ACLB, GPIOs, ISO 7816, NRG™ (ISO/IEC 14443-3 type A with CRYPTO1), SPI
NVM	500 kByte	628 kByte	500 kByte
RAM	8, 12, 18 kByte	12 kByte	8, 12, 18 kByte
ROM	–	–	182 kByte
CPU	Dual 16-bit	Dual 16-bit	Dual 16-bit
Symmetrical cryptography	AES up to 256-bit, DES, 3DES, ECC, RSA	AES up to 256-bit, DES, 3DES, ECC, RSA	AES up to 256-bit, DES, 3DES, ECC, RSA
Asymmetrical cryptography	ECC up to 521-bit, RSA up to 4096-bit	ECC up to 521-bit, RSA up to 4096-bit	ECC up to 521-bit, RSA up to 4096-bit
Ambient temperature	-25°C to +85°C	-25°C to +85°C	-25°C to +85°C
Delivery forms	Sawn wafer	Sawn wafer	Sawn wafer
Typical applications	–	–	–
Certifications	CC EAL6+ high, EMVCo	CC EAL6+ high, EMVCo	CC EAL6+ high, EMVCo

[4] Please note that xxx in product names stands for RAM size

	NFC tags	
Product name	**SLE 66R01LN** NFC Ready	**SLE 66R01PN** NFC Ready
Product description	my-d™ move lean NFC, pre-configured NFC memory, NFC Forum Type 2 Tag certified	my-d™ move NFC, pre-configured NFC memory, NFC Forum Type 2 Tag certified
Interfaces	ISO/IEC 14443-3 Type A, NFC Forum Type 2 Tag operation	ISO/IEC 14443-3 Type A, NFC Forum Type 2 Tag operation
Memory organization	1 fixed sector, pre-configured NFC memory	1 fixed sector, pre-configured NFC memory
Counter	–	16-bit counter, anti-tearing support
EEPROM	48 byte (user), 24 byte (admin)	128 byte (user), 24 byte (admin)
Security features	Block locking, individual page locking, unique serial number	32-bit password protection for read and/or write access, block locking, individual page locking, password retry counter, unique serial number
Distance (read/write)	Typically up to 10 cm and above	Typically up to 10 cm and above
Data rate	106 kbit/s to card, 106 kbit/s to reader	106 kbit/s to card, 106 kbit/s to reader
Endurance	10000	10000
Retention time	>5 years	>5 years
Tools	Evaluation kit contactless	Evaluation kit contactless
Delivery forms	NiAu-bump, sawn wafer	NiAu-bump, sawn wafer
Typical applications	NFC device pairing, smart posters, consumer goods information	NFC device pairing, smart posters, consumer goods information
Certifications	NFC Forum Type 2 Tag	NFC Forum Type 2 Tag

Government Identification

	Dual-interface & contactless security controllers			
Product name [3]	**SLE 77CLF1001P** SOLID FLASH™	**SLE 77CLFXxxx0PH** SOLID FLASH™	**SLE 78CLFXxxx0PH** Integrity Guard SOLID FLASH™	**SLE 78CLFXxxx0PH** Integrity Guard SOLID FLASH™ Mega Memory
Product description	Contactless security controller	Contactless security cryptocontroller with dual-interface	Contactless security cryptocontroller with dual-interface	Contactless security cryptocontroller with dual-interface
Interfaces	ISO 14443 A/B, ISO 18092 passive mode, NRG™ (ISO/IEC 14443-3 type A with CRYPTO1)	ISO 14443 A/B, ISO 18092 passive mode, ISO 7816, NRG™ (ISO/IEC 14443-3 type A with CRYPTO1)	ISO 14443 A/B, ISO 18092 passive mode, ISO 7816, NRG™ (ISO/IEC 14443-3 type A with CRYPTO1)	ISO 14443 A/B, ISO 18092 passive mode, ISO 7816, NRG™ (ISO/IEC 14443-3 type A with CRYPTO1)
NVM	100 kByte	200, 240 kByte	240, 300, 404 kByte	528, 628 kByte
RAM	4 kByte	6 kByte	8 kByte	12 kByte
ROM	–	–	–	–
CPU	16-bit	16-bit	Dual 16-bit	Dual 16-bit
Symmetrical cryptography	AES up to 256-bit, DES, 3DES	AES up to 256-bit, DES, 3DES	AES up to 256-bit, DES, 3DES	AES up to 256-bit, DES, 3DES
Asymmetrical cryptography	–	ECC up to 521-bit, RSA up to 4096-bit	ECC up to 521-bit, RSA up to 4096-bit	ECC up to 521-bit, RSA up to 4096-bit
Ambient temperature	-25°C to +85°C	-25°C to +85°C	-25°C to +85°C	-25°C to +85°C
Delivery forms	Sawn wafer, contactless module	Sawn wafer, contactless module, dual-interface module	Sawn wafer, contactless module, dual-interface module	Sawn wafer, contactless module, dual-interface module
Typical applications	National eID, eHealth card / eSocial card, eDriver's license, eVehicle registration card / eCar registration	National eID, eHealth card / eSocial card, eDriver's license, eVehicle registration card / eCar registration	National eID, ePassport, eHealth card / eSocial card, eDriver's license, eVisa, eResidence permit, eTachograph, eVehicle registration card / eCar registration, eSignature	National eID, ePassport, eHealth card / eSocial card, eDriver's license, eVisa, eResidence permit, eTachograph, eVehicle registration card / eCar registration, eSignature
Certifications	CC EAL5+ high	CC EAL5+ high	CC EAL6+ high, EMVCo	CC EAL6+ high, EMVCo

[3] Please note that xxx in product names stands for NVM size

SLE 78CLFXxxxVPH Integrity Guard, SOLID FLASH™, VHBR	SLE 78CLFXxxxVPH Integrity Guard, SOLID FLASH™, VHBR, Mega Memory	SLE 78CLFX1M10PH Integrity Guard, SOLID FLASH™, Mega Memory	SLE 78CLFX1M1VPH Integrity Guard, SOLID FLASH™, VHBR, Mega Memory	SLC52GDAxxx Integrity Guard, SOLID FLASH™, VHBR
Contactless security cryptocontroller with dual-interface	Contactless security cryptocontroller with dual-interface	Contactless security cryptocontroller with dual-interface	Contactless security cryptocontroller with dual-interface	Contactless security cryptocontroller with dual-interface
ISO 14443 A/B, ISO 18092 passive mode, ISO 7816, NRG™ (ISO/IEC 14443-3 type A with CRYPTO1)	ISO 14443 A/B, ISO 18092 passive mode, ISO 7816, NRG™ (ISO/IEC 14443-3 type A with CRYPTO1)	ISO 14443 A/B, ISO 18092 passive mode, ISO 7816, NRG™ (ISO/IEC 14443-3 type A with CRYPTO1)	ISO 14443 A/B, ISO 18092 passive mode, ISO 7816, NRG™ (ISO/IEC 14443-3 type A with CRYPTO1)	ISO 14443 A/B, ISO 18092 passive mode, ISO 7816, NRG™ (ISO/IEC 14443-3 type A with CRYPTO1)
300, 404 kByte	528, 628 kByte	628 kByte	628 kByte	248, 348, 448 kBytes
8 kByte	12 kByte	12 kByte	12 kByte	12 kByte
–	–	444 kByte	444 kByte	–
Dual 16-bit	Dual 16-bit	Dual 16-bit	Dual 16-bit	Dual 16-bit
AES up to 256-bit, DES, 3DES	AES up to 256-bit, DES, 3DES	AES up to 256-bit, DES, 3DES	AES up to 256-bit, DES, 3DES	AES up to 256-bit, DES, 3DES
ECC up to 521-bit, RSA up to 4096-bit	ECC up to 521-bit, RSA up to 4096-bit	ECC up to 521-bit, RSA up to 4096-bit	ECC up to 521-bit, RSA up to 4096-bit	ECC up to 521-bit, RSA up to 4096-bit
-25°C to +85°C	-25°C to +85°C	-25°C to +85°C	-25°C to +85°C	-25°C to +85°C
Sawn wafer, contactless module, dual-interface module	Sawn wafer, contactless module, dual-interface module	Sawn wafer, contactless module, dual-interface module	Sawn wafer, contactless module, dual-interface module	Sawn wafer, contactless module, dual-interface module
National eID, ePassport, eHealth card / eSocial card, eDriver's license, eVisa, eResidence permit, eTachograph, eVehicle registration card / eCar registration, eSignature	National eID, ePassport, eHealth card / eSocial card, eDriver's license, eVisa, eResidence permit, eTachograph, eVehicle registration card / eCar registration, eSignature	National eID, ePassport, eHealth card / eSocial card, eDriver's license, eVisa, eResidence permit, eTachograph, eVehicle registration card / eCar registration, eSignature	National eID, ePassport, eHealth card / eSocial card, eDriver's license, eVisa, eResidence permit, eTachograph, eVehicle registration card / eCar registration, eSignature	National eID, ePassport, eHealth card / eSocial card, eDriver's license, eVisa, eResidence permit, eTachograph, eVehicle registration card / eCar registration, eSignature
CC EAL6+ high, EMVCo	CC EAL6+ high, EMVCo	CC EAL6+ high, EMVCo	CC EAL6+ high, EMVCo	CC EAL6+ high, EMVCo

Government Identification

			Contact-based security controllers	
Product name [3]	**SLC52GDAxxx** Integrity Guard, SOLID FLASH™, VHBR, Mega Memory	**SLC37GDAxxx** new SOLID FLASH™, VHBR	**SLC37GCB240** SOLID FLASH™	**SLE 78CFXxxx0PH** Integrity Guard, SOLID FLASH™
Product description	Contactless security cryptocontroller with dual-interface	Contactless security cryptocontroller with dual-interface	Security controller	Security cryptocontroller
Interfaces	ISO 14443 A/B, ISO 18092 passive mode, ISO 7816, NRG™ (ISO/IEC 14443-3 type A with CRYPTO1)	ISO 14443 A/B, ISO 18092 passive mode, ISO 7816, NRG™ (ISO/IEC 14443-3 type A with CRYPTO1)	ISO 7816	ISO 7816
NVM	600, 700, 804 kBytes	448, 512 kBytes	240 kByte	240, 300, 404 kByte
RAM	16 kByte	16 kByte	12 kByte	8 kByte
ROM	–	–	–	–
CPU	Dual 16-bit	32-bit Arm® SecurCore® SC300	32-bit Arm® SecurCore® SC300	Dual 16-bit
Symmetrical cryptography	AES up to 256-bit, DES, 3DES	AES up to 256-bit, DES, 3DES	AES, DES	AES up to 256-bit, DES, 3DES
Asymmetrical cryptography	ECC up to 521-bit, RSA up to 4096-bit	ECC up to 521-bit, RSA up to 4096-bit	–	ECC up to 521-bit, RSA up to 4096-bit
Ambient temperature	-25°C to +85°C	-25°C to +85°C	-25°C to +85°C	-25°C to +85°C
Delivery forms	Sawn wafer, contactless module, dual-interface module	Sawn wafer, contactless module, dual-interface module	Sawn wafer, contact-based module	Sawn wafer, contact-based module
Typical applications	National eID, ePassport, eHealth card / eSocial card, eDriver's license, eVisa, eResidence permit, eTachograph, eVehicle registration card / eCar registration, eSignature	National eID, ePassport, eHealth card / eSocial card, eDriver's license, eVisa, eResidence permit, eTachograph, eVehicle registration card / eCar registration, eSignature	National eID, eHealth card / eSocial card	National eID, eHealth card / eSocial card, eDriver's license, eTachograph, eVehicle registration card / eCar registration, eSignature
Certifications	CC EAL6+ high, EMVCo	Targeted CC EAL6+ high, EMVCo	CC EAL5+ high	CC EAL6+ high, EMVCo

[3] Please note that xxx in product names stands for NVM size

SLE 78CFXxxx0PH Integrity Guard SOLID FLASH™ Mega Memory	**SLE 78CFX1M10PH** Integrity Guard SOLID FLASH™ Mega Memory	**SLC52GCAxxx** Integrity Guard SOLID FLASH™	**SLC52GCAxxx** Integrity Guard SOLID FLASH™ Mega Memory	**SLC37GCAxxx** new SOLID FLASH™
Security cryptocontroller	Security cryptocontroller	Security cryptocontroller	Security cryptocontroller	Security cryptocontroller
ISO 7816	ISO 7816	ISO 7816	ISO 7816	ISO 7816
528, 628 kByte	628 kByte	200, 300, 448 kByte	600, 700, 804 kByte	448, 512 kByte
12 kByte	12 kByte	12 kByte	16 kByte	16 kByte
–	444 kByte	–	–	–
Dual 16-bit	Dual 16-bit	Dual 16-bit	Dual 16-bit	32-bit Arm® SecurCore® SC300
AES up to 256-bit, DES, 3DES	AES up to 256-bit, DES, 3DES	AES up to 256-bit, DES, 3DES	AES up to 256-bit, DES, 3DES	AES up to 256-bit, DES, 3DES
ECC up to 521-bit, RSA up to 4096-bit	ECC up to 521-bit, RSA up to 4096-bit	ECC up to 521-bit, RSA up to 4096-bit	ECC up to 521-bit, RSA up to 4096-bit	ECC up to 521-bit, RSA up to 4096-bit
-25°C to +85°C	-25°C to +85°C	-25°C to +85°C	-25°C to +85°C	-25°C to +85°C
Sawn wafer, contact-based module	Sawn wafer, contact-based module	Sawn wafer, contact-based module	Sawn wafer, contact-based module	Sawn wafer, contact-based module
National eID, eHealth card / eSocial card, eDriver's license, eTachograph, eVehicle registration card / eCar registration, eSignature	National eID, eHealth card / eSocial card, eDriver's license, eTachograph, eVehicle registration card / eCar registration, eSignature	National eID, eHealth card / eSocial card, eDriver's license, eTachograph, eVehicle registration card / eCar registration, eSignature	National eID, eHealth card / eSocial card, eDriver's license, eTachograph, eVehicle registration card / eCar registration, eSignature	National eID, eHealth card / eSocial card, eDriver's license, eTachograph, eVehicle registration card / eCar registration, eSignature
CC EAL6+ high, EMVCo	CC EAL6+ high, EMVCo	CC EAL6+ high, EMVCo	CC EAL6+ high, EMVCo	Targeted CC EAL6+ high, EMVCo

[5] Please note that xxx in product names stands for NVM size

Government Identification Solutions

	Java Card™ platform on SLE 78			
Product name [5]	**SLJ 52GLLxxxCR** Integrity Guard SOLID FLASH™	**SLJ 52GCAxxxCR** Integrity Guard SOLID FLASH™	**SLJ 52GDAxxxCC** Integrity Guard SOLID FLASH™	**SLJ 52GDAxxxVC** Integrity Guard SOLID FLASH™ VHBR
Product description	Java Card platform	Java Card platform	Java Card platform	Java Card platform
Communication interfaces	ISO 14443 A/B, NRG™ (ISO/IEC 14443-3 type A with CRYPTO1)	ISO 7816	ISO 14443 A/B, ISO 7816	ISO 14443 A/B, ISO 7816
Supported standards	GP2.2.1, JC3.0	GP2.2.1, JC3.0	GP2.2.1, JC3.0	GP2.2.1, JC3.0
NVM	36, 80, 128 kByte	36, 80, 128 kByte	36, 80, 128 kByte	36, 80, 128 kByte
Operating system	Oracle (Oracle JCOS Edition 1)	Oracle (Oracle JCOS Edition 1)	Oracle (Oracle JCOS Edition 2)	Oracle (Oracle JCOS Edition 2)
Symmetrical cryptography	AES up to 256-bit, DES, 3DES	AES up to 256-bit, DES, 3DES	AES up to 256-bit, DES, 3DES	AES up to 256-bit, DES, 3DES
Asymmetrical cryptography	ECC up to 521-bit, RSA up to 3072-bit	ECC up to 521-bit, RSA up to 3072-bit	ECC up to 521-bit, RSA up to 2048-bit	ECC up to 521-bit, RSA up to 2048-bit
Typical applications	All applications such as national eID, ePassport, eHealth card / eSocial Security card, eDriver's License, eVisa, eResidence permit, eTachograph, eVehicle registration card, eSignature	All applications such as national eID, ePassport, eHealth card / eSocial card, eDriver's license, eVisa, eResidence permit, eTachograph, eVehicle registration card / eCar registration, eSignature	All applications such as national eID, ePassport, eHealth card / eSocial card, eDriver's license, eVisa, eResidence permit, eTachograph, eVehicle registration card / eCar registration, eSignature	All applications such as national eID, ePassport, eHealth card / eSocial card, eDriver's license, eVisa, eResidence permit, eTachograph, eVehicle registration card / eCar registration, eSignature
Certifications	CC EAL5+ high, FIPS 140-2	CC EAL5+ high, FIPS 140-2	CC EAL5+ high	CC EAL5+ high

[5] Please note that xxx in product names stands for NVM size

Java Card™ platform on SLE 78 with applet				
SLJ 52GCA080BL Integrity Guard	**SLJ 52GDA080BL** Integrity Guard	**SLJ 52GCA080BR** Integrity Guard SOLID FLASH™	**SLJ 52GCA080BC** Integrity Guard SOLID FLASH™	**SLJ 52GDA080RC** Integrity Guard SOLID FLASH™ VHBR
Java Card platform including eDriver's License (eMRTD applet)	Java Card platform including eDriver's License (eMRTD applet)	Java Card platform including eDriver's License (eMRTD applet)	Java Card platform including eDriver's License (eMRTD applet)	Java Card platform including eDriver's License (eMRTD applet)
ISO 7816	ISO 14443 A/B, ISO 7816	ISO 7816	ISO 7816	ISO 14443 A/B, ISO 7816
ISO 18013 BAP, EAP config 1-4, ISO 7816-4, 8, 9	ISO 18013 BAP, EAP config 1-4, ISO 7816-4, 8, 9	ISO 18013 BAP, EAP config 1-4, ISO 7816-4, 8, 9	ISO 18013 BAP, EAC, SAC, ISO 7816-4, 8, 9	ISO 18013 BAP, EAC, SAC, ISO 7816-4, 8, 9
80 kByte	80 kByte	80 kByte	80 kByte	80 kByte
Trusted Logic (jTOP ID)	Trusted Logic (jTOP ID)	Oracle (Oracle JCOS I)	Oracle (Oracle JCOS Edition 2)	Oracle (Oracle JCOS Edition 2)
AES up to 256-bit, DES, 3DES	AES up to 256-bit, DES, 3DES	AES up to 256-bit, DES, 3DES	AES up to 256-bit, DES, 3DES	AES up to 256-bit, DES, 3DES
ECC up to 521-bit, RSA up to 2048-bit	ECC up to 521-bit, RSA up to 2048-bit	ECC up to 384-bit, RSA up to 1536-bit	ECC up to 384-bit, RSA up to 1536-bit	ECC up to 384-bit, RSA up to 1536-bit
eDriver's license	eDriver's license	eDriver's license	eDriver's license	eDriver's license
–	–	–	–	–

Government Identification Solutions

	Java Card™ platform on SLE 78 with applet			
Product name	**SLJ 52GDA128AL** Integrity Guard	**SLJ 52GLA080AR** Integrity Guard SOLID FLASH™	**SLJ 52GDA080HC** Integrity Guard SOLID FLASH™ VHBR	**SLJ 52GCA080DC** Integrity Guard SOLID FLASH™
Product description	Java Card platform including eMRTD applet	Java Card platform including eMRTD applet	Java Card platform including eMRTD applet	Java Card platform including PKI applet
Communication interfaces	ISO 14443 A/B, ISO 7816	ISO 14443 A/B	ISO 14443 A/B, ISO 7816	ISO 7816
Supported standards	ICAO BAC, EAC, SAC, ISO 7816-4, 8, 9	ICAO BAC, EAC, SAC, ISO 7816-4, 8, 9	ICAO BAC, EAC, SAC, ISO 7816-4, 8, 9	ICAO EAC, SAC, PKCS#15
NVM	128 kByte	80 kByte	80 kByte	80 kByte
Operating system	Trusted Logic (jTOP ID)	Oracle (Oracle JCOS Edition 1)	Oracle (Oracle JCOS Edition 2)	Oracle (Oracle JCOS Edition 1)
Symmetrical cryptography	AES up to 256-bit, DES, 3DES	AES up to 256-bit, DES, 3DES	AES up to 256-bit, DES, 3DES	AES up to 256-bit, DES, 3DES
Asymmetrical cryptography	ECC up to 521-bit, RSA up to 2048-bit	ECC up to 384-bit, RSA up to 1536-bit	ECC up to 384-bit, RSA up to 1536-bit	ECC up to 384-bit, RSA up to 2048-bit
Typical applications	ePassport, eResidence permit, eIdentity card	ePassport, eResidence permit, eIdentity card	ePassport, eResidence permit, eIdentity card	eAuthentication, eHealthcare, eSignature, eWelfare social security, secured file transfer
Certifications	CC EAL4+ high	–	–	–

[6] Please note that xxx in product names stands for NVM size

	SECORA™ ID Java Card™ platform on SLC 52			
SLJ 52GDA080KC Integrity Guard SOLID FLASH™ VHBR	**SLJ 52GDTxxxCS** new Integrity Guard SOLID FLASH™	**SLJ 52GDT120VS** new Integrity Guard SOLID FLASH™ VHBR	**SLJ 52GLT120CS** new Integrity Guard SOLID FLASH™	**SLJ 52GDA110CS** new Integrity Guard SOLID FLASH™
Java Card platform including PKI applet	Java Card platform with Eclipse development tool	Java Card platform with Eclipse development tool	Java Card platform with Eclipse development tool	Java Card platform with Eclipse development tool
ISO 14443 A/B, ISO 7816	ISO 14443 A/B, ISO 7816	ISO 14443 A/B, ISO 14443 VHBR, ISO 7816	ISO 14443 A/B, ISO 7816	ISO 14443 A/B, ISO 7816
ICAO EAC, SAC, PKCS#15	GP 2.3.1, JC 3.0.5	GP 2.3.1, JC 3.0.5	GP 2.3.1, JC 3.0.5	GP 2.3.1, JC 3.0.5
80 kByte	80, 120 kByte	120 kByte	120 kByte	110 kByte
Oracle (Oracle JCOS Edition 2)	SECORA™ ID S Version 1.0	SECORA™ ID S Version 1.0	SECORA™ ID S Version 1.0	SECORA™ ID S Version 1.0
AES up to 256-bit, DES, 3DES	AES up to 256-bit, 3DES	AES up to 256-bit, 3DES	AES up to 256-bit, 3DES	AES up to 256-bit, 3DES
ECC up to 384-bit, RSA up to 2048-bit	ECC up to 521-bit, RSA up to 2048-bit	ECC up to 521-bit, RSA up to 2048-bit	ECC up to 521-bit, RSA up to 2048-bit	ECC up to 521-bit, RSA up to 4096-bit
eAuthentication, eHealthcare, eSignature, eWelfare social security, secured file transfer	National eID, ePassport, eHealth card, eDriver's License, eSignature, ISO 7816-4 data structure for customization	National eID, ePassport, eHealth card, eDriver's License, eSignature, ISO 7816-4 data structure for customization	National eID, ePassport, eHealth card, eDriver's License, eSignature, ISO 7816-4 data structure for customization	National eID, ePassport, eHealth card, eDriver's License, eSignature, ISO 7816-4 data structure for customization
–	CC EAL6+ high, EMVCo targeted	CC EAL6+ high, EMVCo targeted	CC EAL6+ high, EMVCo targeted	CC EAL6+ high, EMVCo targeted

Government Identification Solutions

	SECORA™ ID Java Card™ platform on SLC 52		SECORA™ ID Java Card™ platform with applet on SLC 52	
Product name	**SLJ 52GLA110CS** new Integrity Guard, SOLID FLASH™	**SLJ 52GDA110VS** new Integrity Guard, SOLID FLASH™, VHBR	**SLJ 52GDAxxxRS** new Integrity Guard, SOLID FLASH™	**SLJ 52GDAxxxYS** new Integrity Guard, SOLID FLASH™, VHBR
Product description	Java Card platform with Eclipse development tool	Java Card platform with Eclipse development tool	Applet Collection by Masktech GmbH, Java Card platform including eMRTD applet (ICAO)	Applet Collection by Masktech GmbH, Java Card platform including eMRTD applet (ICAO)
Communication interfaces	ISO 14443 A/B, ISO 7816	ISO 14443 A/B, ISO 14443 VHBR, ISO 7816	ISO 14443 A/B, ISO 7816	ISO 14443 A/B, ISO 14443 VHBR, ISO 7816
Supported standards	GP 2.3.1, JC 3.0.5	GP 2.3.1, JC 3.0.5	GP 2.3.1, JC 3.0.5	GP 2.3.1, JC 3.0.5
NVM	110 kByte	110 kByte	xxx kByte	xxx kByte
Operating system	SECORA™ ID S Version 1.0	SECORA™ ID S Version 1.0	SECORA™ ID S Version 1.0	SECORA™ ID S Version 1.0
Symmetrical cryptography	AES up to 256-bit, 3DES	AES up to 256-bit, 3DES	AES up to 256-bit, 3DES	AES up to 256-bit, 3DES
Asymmetrical cryptography	ECC up to 521-bit, RSA up to 4096-bit	ECC up to 521-bit, RSA up to 4096-bit	ECC up to xxx-bit, RSA up to xxxx-bit	ECC up to xxx-bit, RSA up to xxxx-bit
Typical applications	National eID, ePassport, eHealth card, eDriver's License, eSignature, ISO 7816-4 data structure for customization	National eID, ePassport, eHealth card, eDriver's License, eSignature, ISO 7816-4 data structure for customization	National eID, ePassport, eHealth card, eDriver's License, eSignature, ISO 7816-4 data structure for customization	National eID, ePassport, eHealth card, eDriver's License, eSignature, ISO 7816-4 data structure for customization
Certifications	CC EAL6+ high, EMVCo targeted	CC EAL6+ high, EMVCo targeted	eMRTD CC EAL5+ high targeted	eMRTD CC EAL5+ high targeted

[6] Please note that xxx in product names stands for EEPROM size, y specifies an application (e.g. eAuthentication, eHealthcare, eSignature, etc.)

SLJ 52GDT080AS new Integrity Guard SOLID FLASH™	SLJ 52GDT080HS new Integrity Guard SOLID FLASH™ VHBR	SLJ 52GDAxxxNS new Integrity Guard SOLID FLASH™
Infineon Applet Collection eMRTD V1.0, Java Card platform including eMRTD applet (ICAO)	Infineon Applet Collection eMRTD V1.0, Java Card platform including eMRTD applet (ICAO)	Applet Collection by Masktech GmbH, Java Card platform including ePKI applet
ISO 14443 A/B, ISO 7816	ISO 14443 A/B, ISO 14443 VHBR, ISO 7816	ISO 14443 A/B, ISO 7816
GP 2.3.1, JC 3.0.5	GP 2.3.1, JC 3.0.5	GP 2.3.1, JC 3.0.5
80 kByte	80 kByte	xxx kByte
SECORA™ ID S Version 1.0	SECORA™ ID S Version 1.0	SECORA™ ID S Version 1.0
AES up to 256-bit, 3DES	AES up to 256-bit, 3DES	AES up to 256-bit, 3DES
ECC up to 521-bit, RSA up to 2048-bit	ECC up to 521-bit, RSA up to 2048-bit	ECC up to xxx-bit, RSA up to xxxx-bit
National eID, ePassport, eHealth card, eDriver's License, eSignature, ISO 7816-4 data structure for customization	National eID, ePassport, eHealth card, eDriver's License, eSignature, ISO 7816-4 data structure for customization	National eID, ePassport, eHealth card, eDriver's License, eSignature, ISO 7816-4 data structure for customization
eMRTD CC EAL5+ high targeted	eMRTD CC EAL5+ high targeted	ePKI CC EAL5+ high targeted

Government Identification Solutions

	Native MTCOS ID 2.5 platform on SLE 78
Product name [6]	**SLN 52GDAxxxyK** Integrity Guard SOLID FLASH™ VHBR
Product description	Native MTCOS ID 2.5 platform including ePass, eDriver's license and eSign use case
Communication interfaces	ISO 14443 A/B, ISO 7816
Supported standards	BSI-TR03110 v1.11 and v2.05 EAC, ICAO BAC, SAC, AA, ISO 18013 BAP, EAP config 1-4, ISO 7816-4, 8, 9, PKCS#15
NVM	36, 80, 128 kByte
Operating system	Masktech (MTCOS ID 2.5)
Symmetrical cryptography	AES up to 256-bit, DES, 3DES
Asymmetrical cryptography	ECC up to 521-bit, RSA up to 4096-bit
Typical applications	eAuthentication, eDriver's license, eHealthcare, eIdentity card, ePassport, eSignature, eWelfare social security, secured file transfer
Certifications	ePass eSign CC EAL5+ high

[6] Please note that xxx in product names stands for NVM size, y specifies an application (e.g. eAuthentication, eHealthcare, eSignature, etc.)

USB Tokens

	USB tokens (16-bit)			
Product name [3]	**SLE 78CUFXxxx9PH** Integrity Guard SOLID FLASH™	**SLE 78CUFX3000PH** Integrity Guard SOLID FLASH™	**SLE 78CLUFX3000PH** Integrity Guard SOLID FLASH™	**SLE 78CLUFX5000PH** Integrity Guard SOLID FLASH™
Product description	USB security cryptocontroller for use in chipcard form factor	USB security cryptocontroller	Multi-interface USB security cryptocontroller with a contactless interface	Multi-interface USB security cryptocontroller with a contactless interface
Interfaces	ISO 7816, USB 2.0	4 GPIOs, ISO 7816, USB 2.0	4 GPIOs, I2C, ISO 14443 A/B, ISO 18092 passive mode, ISO 7816, NRG™ (ISO/IEC 14443-3 type A with CRYPTO1), USB 2.0	12 GPIOs, I2C, ISO 14443 A/B, ISO 18092 passive mode, ISO 7816, NRG™ (ISO/IEC 14443-3 type A with CRYPTO1), SPI, USB 2.0
NVM	300, 500 kByte	300 kByte	300 kByte	500 kByte
RAM	12 kByte	12 kByte	12 kByte	16 kByte
ROM	–	–	–	–
CPU	Dual 16-bit	Dual 16-bit	Dual 16-bit	Dual 16-bit
Crypto coprocessor symmetrical	AES up to 256-bit, DES, 3DES	AES up to 256-bit, DES, 3DES	AES up to 256-bit, DES, 3DES	AES up to 256-bit, DES, 3DES
Crypto coprocessor asymmetrical	ECC up to 521-bit, RSA up to 4096-bit	ECC up to 521-bit, RSA up to 4096-bit	ECC up to 521-bit, RSA up to 4096-bit	ECC up to 521-bit, RSA up to 4096-bit
Ambient temperature	-25°C to +85°C	-25°C to +85°C	-25°C to +85°C	-25°C to +85°C
Delivery forms	Sawn wafer	VQFN-32, sawn wafer	VQFN-32, sawn wafer	VQFN-32, sawn wafer
Certifications	CC EAL6+ high, EMVCo	CC EAL6+ high, EMVCo	CC EAL6+ high, EMVCo	CC EAL6+ high, EMVCo

[3] Please note that xxx in product names stands for NVM size

SLE 78CLUFX5007PH Integrity Guard SOLID FLASH™	SLE 78CLUX5000PH Integrity Guard SOLID FLASH™	SLE 78CLUX5007PH Integrity Guard SOLID FLASH™	SLE 78CUFX5000PH Integrity Guard SOLID FLASH™
Multi-interface USB security cryptocontroller with a contactless interface	Multi-interface USB security cryptocontroller with a contactless interface	Multi-interface USB security cryptocontroller with a contactless interface	Multi-interface USB security cryptocontroller
12 GPIOs, I2C, ISO 14443 A/B, ISO 18092 passive mode, ISO 7816, NRG™ (ISO/IEC 14443-3 type A with CRYPTO1), SPI, USB 2.0, optimized for sub-ID1	12 GPIOs, I2C, ISO 14443 A/B, ISO 18092 passive mode, ISO 7816, NRG™ (ISO/IEC 14443-3 type A with CRYPTO1), SPI, USB 2.0	12 GPIOs, I2C, ISO 14443 A/B, ISO 18092 passive mode, ISO 7816, NRG™ (ISO/IEC 14443-3 type A with CRYPTO1), SPI, USB 2.0, optimized for sub-ID1	12 GPIOs, I2C, ISO 7816, SPI, USB 2.0
500 kByte	500 kByte	500 kByte	500 kByte
16 kByte	16 kByte	16 kByte	16 kByte
–	182 kByte	182 kByte	–
Dual 16-bit	Dual 16-bit	Dual 16-bit	Dual 16-bit
AES up to 256-bit, DES, 3DES	AES up to 256-bit, DES, 3DES	AES up to 256-bit, DES, 3DES	AES up to 256-bit, DES, 3DES
ECC up to 521-bit, RSA up to 4096-bit	ECC up to 521-bit, RSA up to 4096-bit	ECC up to 521-bit, RSA up to 4096-bit	ECC up to 521-bit, RSA up to 4096-bit
-25°C to +85°C	-25°C to +85°C	-25°C to +85°C	-25°C to +85°C
VQFN-32, sawn wafer	VQFN32, sawn wafer	VQFN-32, sawn wafer	VQFN-32, sawn wafer
CC EAL6+ high, EMVCo	CC EAL6+ high, EMVCo	CC EAL6+ high, EMVCo	CC EAL6+ high, EMVCo

USB Tokens

	USB tokens (32-bit)			
Product name [3]	**SLE 97CUFX500FPH** SOLID FLASH™	**SLE 97CUFX5000PH** SOLID FLASH™	**SLE 97CUSIFX1M00PH** SOLID FLASH™ Mega Memory	**SLE 97CUNSIFX1M00PH** SOLID FLASH™
Product description	USB security cryptocontroller for use in chipcard form factor	USB security cryptocontroller	Multi-interface USB security cryptocontroller	Multi-interface USB security cryptocontroller for industrial use
Interfaces	ISO 7816, USB 2.0	ISO 7816, USB 2.0	4 GPIOs, I2C, ISO 7816, SPI, USB 2.0	I2C, SPI, USB 2.0, SWP
NVM	504 kByte	504 kByte	1 MByte	1 MByte
RAM	20 kByte	20 kByte	32 kByte	32 kByte
CPU	32-bit	32-bit	32-bit	32-bit
Crypto coprocessor symmetrical	AES up to 256-bit, DES, 3DES	AES up to 256-bit, DES, 3DES	AES up to 256-bit, DES, 3DES	AES up to 256-bit, DES, 3DES
Crypto coprocessor asymmetrical	ECC up to 521-bit, RSA up to 4096-bit	ECC up to 521-bit, RSA up to 4096-bit	ECC up to 521-bit, RSA up to 4096-bit	ECC up to 521-bit, RSA up to 4096-bit
Ambient temperature	-25°C to +85°C	-25°C to +85°C	-25°C to +85°C	-25°C to +85°C
Delivery forms	Sawn wafer	Sawn wafer, VQFN-32, VQFN-8, USON 8	VQFN-32, sawn wafer	VQFN-32, sawn wafer
Certifications	CC EAL5+ high, EMVCo	CC EAL5+ high, EMVCo	CC EAL5+ high, EMVCo	CC EAL5+ high, EMVCo

[3] Please note that xxx in product names stands for NVM size

SLM 97CUSIFX1M00PH SOLID FLASH™ Mega Memory	SLM 97CUNSIFX1M00PH SOLID FLASH™ Mega Memory	SLE 97CUSIFXxxx0PH SOLID FLASH™	SLM 97CUSIFXxxx0PH SOLID FLASH™
Multi-interface USB security cryptocontroller for industrial use	Multi-interface USB security cryptocontroller for industrial use	Multi-interface USB security cryptocontroller	Multi-interface USB security cryptocontroller for industrial use
4 GPIOs, I2C, ISO 7816, SPI, USB 2.0	I2C, SPI, USB 2.0, SWP	4 GPIOs, I2C, ISO 7816, SPI, USB 2.0	4 GPIOs, I2C, ISO 7816, SPI, USB 2.0
1 MByte	1 MByte	504, 792 kByte	504, 792 kByte
32 kByte	32 kByte	24 kByte	24 kByte
32-bit	32-bit	32-bit	32-bit
AES up to 256-bit, DES, 3DES	AES up to 256-bit, DES, 3DES	AES up to 256-bit, DES, 3DES	AES up to 256-bit, DES, 3DES
ECC up to 521-bit, RSA up to 4096-bit	ECC up to 521-bit, RSA up to 4096-bit	ECC up to 521-bit, RSA up to 4096-bit	ECC up to 521-bit, RSA up to 4096-bit
-40°C to +105°C	-40°C to +105°C	-25°C to +85°C	-40°C to +105°C
VQFN-32, sawn wafer	VQFN-32, sawn wafer	VQFN-32, sawn wafer	VQFN-32, sawn wafer
CC EAL5+ high, EMVCo	CC EAL5+ high, EMVCo	CC EAL5+ high, EMVCo	CC EAL5+ high, EMVCo

Transport Ticketing

	Security products with integrated CIPURSE™ functionality		
Product name [5]	**SLM 10TLC002L**	**SLS 32TLCxxxS(M)**	**SLS 32TLC100(M)**
Product description	CIPURSE™move	CIPURSE™4move	CIPURSE™Security controller
Interfaces	ISO 14443 A, NFC Forum Type 4 Tag configurable	ISO 14443 A, NRG™ (ISO/IEC 14443-3 type A with CRYPTO1) optional, NFC Forum Type 4 Tag configurable	ISO 14443 A, NRG™ (ISO/IEC 14443-3 type A with CRYPTO1) optional, NFC Forum Type 4 Tag configurable
Integrated CIPURSE™ functionality	Security architecture of CIPURSE™, built-in command set based on ISO 7816-4/-9, fully configurable file system based on ISO/ IEC 7816-4	Security architecture of CIPURSE™, built-in command set based on ISO 7816-4/-9, fully configurable file system based on ISO/ IEC 7816-4	Security architecture of CIPURSE™, built-in command set based on ISO 7816-4/-9, fully configurable file system based on ISO/ IEC 7816-4
Supported profiles	CIPURSE™L profile	CIPURSE™S profile	CIPURSE™T profile
Capabilities	1 CIPURSE™ application	Up to 8 CIPURSE™ applications configurable	Up to 8/16 CIPURSE™ applications configurable
EEPROM	304 Byte	1, 2, 4 kByte	8 kByte
Cryptography	AES 128-bit	AES 128-bit	AES 128-bit
Delivery forms	MCC8, NiAu-bump, sawn wafer	MCC8, NiAu-bump, sawn wafer	MCC8, NiAu-bump, sawn wafer
Tools	CIPURSE™ development kit	CIPURSE™ development kit	CIPURSE™ development kit
Typical applications	Public transport, ticketing, access management, micropayment	Public transport, ticketing, access management, micropayment	Public transport, ticketing, access management, micropayment
Certifications	CIPURSE™, NFC Forum Type 4 Tag	CC EAL5+ high, CIPURSE™, NFC Forum Type 4 Tag	CC EAL5+ high, CIPURSE™, NFC Forum Type 4 Tag

[5] Please note that xxx in product names stands for EEPROM size

	Contactless security controllers	Dual-interface security controllers		
Product name [3]	**SLE 77CLFxxx1P(M)** SOLID FLASH™	**SLE 77CLFXxxxP(M)** new SOLID FLASH™ Coil on Module	**SLC32TDzxxx** new SOLID FLASH™ Coil on Module Integrity Guard	**SLC36TDzxxx** new SOLID FLASH™ Coil on Module
Product description	Contactless security controller	Dual-interface security cryptocontroller for traditional transport use cases	Dual-interface security cryptocontroller for traditional transport use cases	Dual-interface security cryptocontroller for traditional transport use cases
Interfaces	ISO 14443 A/B, ISO 18092 passive mode, NRG™ (ISO/IEC 14443-3 type A with CRYPTO1)	ISO 7816, ISO 14443 A/B, ISO 18092 passive mode, optimized for small antenna sizes, optional NRG™ (ISO/IEC 14443-3 type A with CRYPTO1)	ISO 7816, ISO 14443 A/B, ISO 18092 passive mode, optimized for small antenna sizes, optional NRG™ (ISO/IEC 14443-3 type A with CRYPTO1)	ISO 7816 / I2C, ISO 14443 A/B, ISO 18092 passive mode, optimized for small antenna sizes, optional NRG™ (ISO/IEC 14443-3 type A with CRYPTO1)
NVM	60, 100 kByte	136, 156, 184, 200, 240 kByte	180, 212, 228, 268, 300, 348 kByte	352, 280 kByte
RAM	4 kByte	6 kByte	10 kByte	12 kByte
CPU	16-bit	16-bit	16-bit	32-bit Arm® SecurCore® SC300
Symmetrical cryptography	AES up to 256-bit, DES, 3DES	AES up to 256-bit, DES, 3DES	AES up to 256-bit, DES, 3DES	AES up to 256-bit, DES, 3DES
Asymmetrical cryptography		ECC up to 521-bit, RSA up to 4096-bit	ECC up to 521-bit, RSA up to 4096-bit	ECC up to 521-bit, RSA up to 4096-bit
Ambient temperature	-25°C to +85°C	-25°C to +85°C	-25°C to +85°C	-25°C to +85°C
Delivery forms	MCC8, NiAu-bump, sawn wafer	Coil on Module, MCC8, sawn wafer, 6/8 pin dual-interface modules and contactless modules	Coil on Module, MCC8, sawn wafer, 6/8 pin dual-interface modules and contactless modules	Coil on Module, sawn wafer, bumped wafer, 6/8 pin dual- interface modules and contactless modules
Typical applications	Public transport, ticketing	Public transport, ticketing	Public transport, ticketing	Public transport, ticketing
Certifications	CC EAL5+ high	CC EAL5+ high, CUP, EMVCo	CC EAL6+ high, CUP, EMVCo	CC EAL6+ high, EMVCo

[3] Please note that xxx in product names stands for NVM size, y – input capacity of derivatives, z – different interfaces

Transport Ticketing

	Contactless memory-based card and ticket products		
Product name	**NRG™ SLE 66R35**	**SLE 66R01L**	**SLE 66R01P**
Product description	(E7) = Supporting 7-byte UID, (I) = Supporting 4-byte fixed number, non-unique ID, (R) = Supporting 4-byte reused ID, Intelligent 1 kByte EEPROM	my-d™ move lean	my-d™ move
Interface	ISO/IEC 14443-3 Type A	ISO/IEC 14443-3 Type A, NFC Forum Type 2 Tag operation	ISO/IEC 14443-3 Type A, NFC Forum Type 2 Tag operation
Memory organization	16 fixed sectors	1 fixed sector	1 fixed sector
Counter	–	–	16-bit counter, anti-tearing support
EEPROM	768 Byte (user), 256 Byte (admin)	48 Byte (user), 16 Byte (admin)	128 Byte (user), 24 Byte (admin)
Security features	Mutual three-pass authentication with 48-bit keys, transport key	Block locking, individual page locking, unique serial number	32-bit password protection for read and/or write access, block locking, individual page locking, password retry counter, unique serial number
Distance (read/write)	Typically up to 10 cm and above	Typically up to 10 cm and above	Typically up to 10 cm and above
Data rate	106 kbit/s to card, 106 kbit/s to reader	106 kbit/s to card, 106 kbit/s to reader	106 kbit/s to card, 106 kbit/s to reader
Endurance	100000	10000	10000
Retention time, minimum	>10 years	>5 years	>5 years
Delivery forms	MCC2, MCC8, NiAu-bump, sawn wafer	NiAu-bump, sawn wafer	NiAu-bump, sawn wafer
Tools	Evaluation kit contactless	Evaluation kit contactless	Evaluation kit contactless
Typical applications	Transport ticketing, access management	Transport ticketing, access management	Transport ticketing, access management
Certifications	–	NFC Forum Type 2 Tag	NFC Forum Type 2 Tag

	CIPURSE™ components for terminals
Product name	**CIPURSE™SAM (Secure Access Module)** **SLF 9630**
Product description	CIPURSE™ secure access module with NRG™ (ISO/IEC 14443-3 type A with CRYPTO1) interface. Enables secured authentication between the reader and CIPURSE™ chip cards or cards using NRG™ (ISO/IEC 14443-3 type A with CRYPTO1) technology and AES128-based authentication schemes. It features a dedicated key management system including key derivation and key upload.
Interface	ISO 7816
Memory organization	Fully configurable, multi-application file system
Security features	3DES, AES128, AES192, AES256, CIPURSE™ and NRG™ (ISO/IEC 14443-3 type A with CRYPTO1) encryption, online and offline mode, secured key loading
Data rate	Subject to the active interface
Delivery forms	ID-1/ID-000 card (SIM format), VQFN-8
Tools	CIPURSE™ development kit
Typical applications	Access control, authentication, micropayment, transport ticketing
Certifications	CC EAL6+ high for HW, CIPURSE™

Authentication

	Turnkey solutions			
Product name	**OPTIGA™ TRUST B SLE 95250**	**OPTIGA™ TRUST E SLS 32AIA** SOLID FLASH™	**OPTIGA™ Trust X SLS 32AIA**	**OPTIGA™ TRUST M SLS 32AIA**
Product description	Product authentication and brand protection solution	Enhanced authentication solution for high-value goods	Enhanced device security solution	Enhanced device security solution
Interfaces	SWI	I2C	I2C	I2C (shielded connection)
EEPROM	512 bit	–	–	–
NVM	–	3 kByte	10 kByte	10 kByte
RAM	–	–	–	–
CPU	State machine	16-bit	16-bit	16-bit
Symmetrical cryptography	–	–	–	–
Asymmetrical cryptography	ECC 131-bit	ECC 256-bit	ECC 256-bit	ECC 256-bit, ECC 384-bit, RSA 1024-bit, RSA 2048-bit
Ambient temperature	-40°C to +85°C	-40°C to +85°C	SLS32AIA020X4 standard: -25 to +85°C SLS32AIA020X2 extended: -40 to +105°C	SLS32AIA010MS standard: -25 to +85°C ; SLS32AIA010MH extended: -40 to +105°C
Delivery forms	TSNP-6	USON-10-2	USON-10-2	USON-10
Typical applications	Authentication of consumer electronics, accessories, original replacement parts	PKI networks, consumer electronics, smart home, industrial automation, Internet of Things (IoT), authentication of system services and accessories, original replacement parts, smart metering, system configuration management, IP/software protection	Internet of Things (IoT), smart home, industrial automation, consumer electronics, smart metering, authentication of system services and accessories, original replacement parts, secure communication, IP/software protection	Mutual authentication, secured communication, secured updates, key provisioning, life-cycle management, data store protection, power management, platform integrity protection
Certifications	–	–	CC EAL 6+ (high) for the HW	CC EAL6+ (high) for HW

	Contact-based security controllers	
Product name	**SLE 97CIFX1M00PE** SOLID FLASH™	**SLE 97CSFX1M00PE** SOLID FLASH™
Product description	Security cryptocontroller	Security cryptocontroller
Interfaces	I2C, ISO 7816	ISO 7816, SPI
EEPROM	–	–
NVM	1 MByte	1 MByte
RAM	32 kByte	32 kByte
CPU	32-bit	32-bit
Symmetrical cryptography	AES up to 256-bit, DES, 3DES	AES up to 256-bit, DES, 3DES
Asymmetrical cryptography	ECC up to 521-bit, RSA up to 4096-bit	ECC up to 521-bit, RSA up to 4096-bit
Ambient temperature	-25°C to +85°C	-25°C to +85°C
Delivery forms	SMD, sawn wafer	SMD, sawn wafer
Typical applications	Authentication of system services, printers, system configuration management	Authentication of system services, printers, system configuration management
Certifications	CC EAL5+ high	CC EAL5+ high

Authentication

	Pay TV		
Product name	**SLE 79CFXXXP** SOLID FLASH™	**SLC58VCAxxx** new SOLID FLASH™	**SLC58VCAxxxR8** new SOLID FLASH™
Product description	Security controller	Security controller	Security controller
Interfaces	ISO 7816	ISO 7816, I2C	ISO 7816, I2C
EEPROM	–	–	–
NVM	up to 500 kByte	up to 352 kByte	up to 200 kByte
RAM	8 kByte	12 kByte	8 kByte
CPU	Dual 16-bit	Dual 16-bit	Dual 16-bit
Symmetrical cryptography	AES up to 256-bit, DES, 3DES	AES up to 256-bit, DES, 3DES	AES up to 256-bit, DES, 3DES
Asymmetrical cryptography	ECC up to 521-bit, RSA up to 4096-bit	ECC up to 521-bit, RSA up to 4096-bit	ECC up to 521-bit, RSA up to 4096-bit
Ambient temperature	-25°C to +85°C	-25°C to +85°C	-25°C to +85°C
Delivery forms	FCOS™ module, VQFN-8, sawn wafer, wire bond module	Sawn wafer, USON-10, wire bond module	Sawn wafer, USON-10, wire bond module
Typical applications	Conditional access	Conditional access	Conditional access
Certifications	CC EAL5+ high	CC EAL5+ high	CC EAL5+ high

[3] Please note that xxx in product names stands for NVM size

Trusted Computing

	OPTIGA™ TPM (Trusted Platform Module)			
Product name	**OPTIGA™ TPM SLB 9645TT1.2**	**OPTIGA™ TPM SLB 9645XT1.2**	**OPTIGA™ TPM SLB 9645VQ1.2**	**OPTIGA™ TPM SLB 9645XQ1.2**
Product description	The Infineon OPTIGA™ TPM (Trusted Platform Module) is a standardized security controller which provides a wide range of security functions for computing platforms and embedded systems.	The Infineon OPTIGA™ TPM (Trusted Platform Module) is a standardized security controller which provides a wide range of security functions for computing platforms and embedded systems.	The Infineon OPTIGA™ TPM (Trusted Platform Module) is a standardized security controller which provides a wide range of security functions for computing platforms and embedded systems.	The Infineon OPTIGA™ TPM (Trusted Platform Module) is a standardized security controller which provides a wide range of security functions for computing platforms and embedded systems.
Interfaces	I2C	I2C	I2C	I2C
Symmetrical cryptography	AES, HMAC, SHA-1	AES, HMAC, SHA-1	AES, HMAC, SHA-1	AES, HMAC, SHA-1
Asymmetrical cryptography	RSA1024, RSA2048	RSA1024, RSA2048	RSA1024, RSA2048	RSA1024, RSA2048
Ambient temperature	-20°C to +85°C	-40°C to +85°C	-20°C to +85°C	-40°C to +85°C
Package	TSSOP-28	TSSOP-28	VQFN-32	VQFN-32
Typical applications	PC and mobile computing on non-x86 platforms; embedded devices e.g.communication, gateways, printer, PoS systems, networking, ATMs	PC and mobile computing on non-x86 platforms; embedded devices e.g. communication, gateways, printer, PoS systems, networking, ATMs	PC and mobile computing on non-x86 platforms; embedded devices e.g. communication, gateways, printer, PoS systems, networking, ATMs	PC and mobile computing on non-x86 platforms; embedded Devices e.g. communication, gateways, printer, PoS systems, networking, ATMs
Certifications	based on CC EAL4+ certified HW	based on CC EAL4+ certified HW	based on CC EAL4+ certified HW	based on CC EAL4+ certified HW
Standard	Version 1.2 Rev. 116	Version 1.2 Rev. 116	Version 1.2 Rev. 116	Version 1.2 Rev. 116

OPTIGA™ TPM SLB 9660TT1.2	OPTIGA™ TPM SLB 9660XT1.2	OPTIGA™ TPM SLB 9660VQ1.2	OPTIGA™ TPM SLB 9660XQ1.2	OPTIGA™ TPM SLB 9665TT2.0
The Infineon OPTIGA™ TPM (Trusted Platform Module) is a standardized security controller which provides a wide range of security functions for computing platforms and embedded systems.	The Infineon OPTIGA™ TPM (Trusted Platform Module) is a standardized security controller which provides a wide range of security functions for computing platforms and embedded systems.	The Infineon OPTIGA™ TPM (Trusted Platform Module) is a standardized security controller which provides a wide range of security functions for computing platforms and embedded systems.	The Infineon OPTIGA™ TPM (Trusted Platform Module) is a standardized security controller which provides a wide range of security functions for computing platforms and embedded systems.	The Infineon OPTIGA™ TPM (Trusted Platform Module) is a standardized security controller which provides a wide range of security functions for computing platforms and embedded systems.
LPC	LPC	LPC	LPC	LPC
AES, HMAC, SHA-1	AES, HMAC, SHA-1	AES, HMAC, SHA-1	AES, HMAC, SHA-1	AES, HMAC, SHA-1, SHA-256
RSA1024, RSA2048	RSA1024, RSA2048	RSA1024, RSA2048	RSA1024, RSA2048	ECC, ECC BN-256, ECC NIST P-256, ECC256, ECDH, RSA1024, RSA2048
-20°C to +85°C	-40°C to +85°C	-20°C to +85°C	-40°C to +85°C	-20°C to +85°C
TSSOP-28	TSSOP-28	VQFN-32	VQFN-32	TSSOP-28
PC and mobile computing with Intel x86, ARM platforms and others; embedded devices e.g. communication, gateways, printer, PoS systems, networking, ATMs	PC and mobile computing with Intel x86, ARM platforms and others; embedded devices e.g. communication, gateways, printer, PoS systems, networking, ATMs	PC and mobile computing with Intel x86, ARM platforms and others; embedded devices e.g. communication, gateways, printer, PoS systems, networking, ATMs	PC and mobile computing with Intel x86, ARM platforms and others; embedded devices e.g. communication, gateways, printer, PoS systems, networking, ATMs	PC and mobile computing with Intel x86, ARM platforms and others; embedded devices e.g. communication, gateways, printer, PoS systems, networking, ATMs
CC EAL4+, FIPS 140-2 level 2 (with FW update)	CC EAL4+, FIPS 140-2 level 2 (with FW update)	CC EAL4+, FIPS 140-2 level 2 (with FW update)	CC EAL4+, FIPS 140-2 level 2 (with FW update)	CC EAL4+, FIPS 140-2 level 2 (with FW update)
Version 1.2 Rev. 116	Version 1.2 Rev. 116	Version 1.2 Rev. 116	Version 1.2 Rev. 116	Version 2.0 Rev. 01.16

Trusted Computing

	OPTIGA™ TPM (Trusted Platform Module)			
Product name	**OPTIGA™ TPM SLB 9665XT2.0**	**OPTIGA™ TPM SLB 9665VQ2.0**	**OPTIGA™ TPM SLB 9665XQ2.0**	**OPTIGA™ TPM SLB 9670VQ1.2**
Product description	The Infineon OPTIGA™ TPM (Trusted Platform Module) is a standardized security controller which provides a wide range of security functions for computing platforms and embedded systems.	The Infineon OPTIGA™ TPM (Trusted Platform Module) is a standardized security controller which provides a wide range of security functions for computing platforms and embedded systems.	The Infineon OPTIGA™ TPM (Trusted Platform Module) is a standardized security controller which provides a wide range of security functions for computing platforms and embedded systems.	The Infineon OPTIGA™ TPM (Trusted Platform Module) is a standardized security controller which provides a wide range of security functions for computing platforms and embedded systems.
Interfaces	LPC	LPC	LPC	SPI
Symmetrical cryptography	AES, HMAC, SHA-1, SHA-256	AES, HMAC, SHA-1, SHA-256	AES, HMAC, SHA-1, SHA-256	AES, HMAC, SHA-1
Asymmetrical cryptography	ECC, ECC BN-256, ECC NIST P-256, ECC256, ECDH, RSA1024, RSA2048	ECC, ECC BN-256, ECC NIST P-256, ECC256, ECDH, RSA1024, RSA2048	ECC, ECC BN-256, ECC NIST P-256, ECC256, ECDH, RSA1024, RSA2048	RSA1024, RSA2048
Ambient temperature	-40°C to +85°C	-20°C to +85°C	-40°C to +85°C	-20°C to +85°C
Package	TSSOP-28	VQFN-32	VQFN-32	VQFN-32
Typical applications	PC and mobile computing with Intel x86, ARM platforms and others; embedded devices e.g. communication, gateways, printer, PoS systems, networking, ATMs	PC and mobile computing with Intel x86, ARM platforms and others; embedded devices e.g. communication, gateways, printer, PoS systems, networking, ATMs	PC and mobile computing with Intel x86, ARM platforms and others; embedded devices e.g. communication, gateways, printer, PoS systems, networking, ATMs	PC and mobile computing with Intel x86, ARM platforms and others; embedded devices e.g. communication, gateways, printer, PoS systems, networking, ATMs
Certifications	CC EAL4+, FIPS 140-2 level 2 (with FW update)	CC EAL4+, FIPS 140-2 level 2 (with FW update)	CC EAL4+, FIPS 140-2 level 2 (with FW update)	CC EAL4+, FIPS 140-2 level 2 (with FW update)
Standard	Version 2.0 Rev. 01.16	Version 2.0 Rev. 01.16	Version 2.0 Rev. 01.16	Version 1.2 Rev. 116
Qualification	–	–	–	–

		OPTIGA™ TPM Industrial	OPTIGA™ TPM Automotive
OPTIGA™ TPM SLB 9670XQ1.2	**OPTIGA™ TPM SLB 9670VQ2.0**	**OPTIGA™ TPM SLM 9670**	**OPTIGA™ TPM SLI 9670**
The Infineon OPTIGA™ TPM (Trusted Platform Module) is a standardized security controller which provides a wide range of security functions for computing platforms and embedded systems.	The Infineon OPTIGA™ TPM (Trusted Platform Module) is a standardized security controller which provides a wide range of security functions for computing platforms and embedded systems.	The Infineon OPTIGA™ TPM (Trusted Platform Module) SLM 9670 is a special model of OPTIGA™ TPM that meets the requirements of industrial and other demanding applications, where key requirements include an extended temperature range (-40 to +105°C), extended lifetime, long-lasting supply availability in combination with industrial quality grade.	The Infineon OPTIGA™ TPM is a standardized security controller which provides a wide range of security functions for automotive use cases. SLI9670 is AEC-Q100 qualified and does meet automotive requirements for robustness.
SPI	SPI	SPI	SPI
AES, HMAC, SHA-1	AES, HMAC, SHA-1, SHA-256	HMAC, SHA-1, SHA-256	HMAC, SHA-1, SHA-256
RSA1024, RSA2048	ECC, ECC BN-256, ECC NIST P-256, ECC256, ECDH, RSA1024, RSA2048	ECC, ECC BN-256, ECC NIST P-256, ECC256, ECDH, RSA1024, RSA2048	ECC, ECC BN-256, ECC NIST P-256, ECC256, ECDH, RSA1024, RSA2048
-40°C to +85°C	-20°C to +85°C	-40°C to +105°C	-40°C to +105°C
VQFN-32	VQFN-32	VQFN-32	VQFN-32
PC and mobile computing with Intel x86, ARM platforms and others; embedded devices e.g. communication, gateways, printer, PoS systems, networking, ATMs	PC and mobile computing with Intel x86, ARM platforms and others; embedded devices e.g. communication, gateways, printer, PoS systems, networking, ATMs	Industrial computing, industrial PCs, servers, tablets, single-board computers, programmable logic controllers (PLCs), industrial networking infrastructure & equipment, industrial servers, gateways, routers, switches	Enhance security in critical automotive applications such as gateway, telematics or multimedia headunits with tamper resist & secure key-storage, -generation & -management and authentication
CC EAL4+, FIPS 140-2 level 2 (with FW update)	CC EAL4+ & FIPS 140-2 level 2 combined certification	CC EAL4+, FIPS 140-2	CC EAL4+, FIPS 140-2
Version 1.2 Rev. 116	Version 2.0 Rev. 01.38	Version 2.0 Rev. 1.38	Version 2.0 Rev. 1.38
–	–	–	AEC-Q100

Object Identification

	my-d™ vicinity plain			
Product name	**SRF 55V02P**	**SRF 55V02P HC**	**SRF 55V10P**	**SRF 55V10P HC**
Product description	my-d™ vicinity Plain mode with open memory access, NFC Forum Type 5 Tag certified	my-d™ vicinity, 97pF high capacitance Plain mode with open memory access, NFC Forum Type 5 Tag certified	my-d™ vicinity Plain mode with open memory access, NFC Forum Type 5 Tag certified	my-d™ vicinity, 97pF high capacitance Plain mode with open memory access, NFC Forum Type 5 Tag certified
Interface	ISO/IEC 15693, ISO/IEC 18000-3 mode 1	ISO/IEC 15693, ISO/IEC 18000-3 mode 1	ISO/IEC 15693, ISO/IEC 18000-3 mode 1	ISO/IEC 15693, ISO/IEC 18000-3 mode 1
Memory organization	1 fixed sector	1 fixed sector	1 fixed sector	1 fixed sector
Counter	Anti-tearing support, up to 65, 536 units	Anti-tearing support, up to 65, 536 units	Anti-tearing support, up to 65, 536 units	Anti-tearing support, up to 65, 536 units
EEPROM	232 Byte (user), 64 Byte (admin)	232 Byte (user), 64 Byte (admin)	1000 Byte (user), 256 Byte (admin)	1000 Byte (user), 256 Byte (admin)
Security features	Individual page locking, unique serial number	Individual page locking, unique serial number	Individual page locking, unique serial number	Individual page locking, unique serial number
Distance (read/write)	Typically up to 1.5 m	Typically up to 1.5 m	Typically up to 1.5 m	Typically up to 1.5 m
Data rate	26.48 kbit/s	26.48 kbit/s	26.48 kbit/s	26.48 kbit/s
Endurance	100000	100000	100000	100000
Retention time, minimum	>10 years	>10 years	>10 years	>10 years
Delivery forms	MCC2, MCC8, NiAu-bump, sawn wafer	MCC2, MCC8, NiAu-bump, sawn wafer	MCC2, MCC8, NiAu-bump, sawn wafer	MCC2, MCC8, NiAu-bump, sawn wafer
Tools	Evaluation kit contactless	Evaluation kit contactless	Evaluation kit contactless	Evaluation kit contactless
Typical applications	Supply chain management, library management, health-care, pharma-ceutical, product authentication, amusement ticketing	Laundry automation, supply chain management, library management, health-care, pharmaceutical, product authentication amusement ticketing	Supply chain management, library management, health-care, pharma-ceutical, product authentication, amusement ticketing	Supply chain management, library management, health-care, pharma-ceutical, product authentication, amusement ticketing
Certifications	NFC Forum Type 5 Tag	NFC Forum Type 5 Tag	NFC Forum Type 5 Tag	NFC Forum Type 5 Tag

my-d™ vicinity secure			
SRF 55V02S	**SRF 55V02S HC**	**SRF 55V10S**	**SRF 55V10S HC**
my-d™ vicinity secure Security memory with security logic for memory access controlled by authentication procedures	my-d™ vicinity secure Security memory with security logic for memory access controlled by authentication procedures. 97pF high capacitance	my-d™ vicinity secure Security memory with security logic for memory access controlled by authentication procedures	my-d™ vicinity secure Security memory with security logic for memory access controlled by authentication procedures. 97pF high capacitance
ISO/IEC 15693, ISO/IEC 18000-3 mode 1	ISO/IEC 15693, ISO/IEC 18000-3 mode 1	ISO/IEC 15693, ISO/IEC 18000-3 mode 1	ISO/IEC 15693, ISO/IEC 18000-3 mode 1
Fully configurable, up to 15 sectors (14 secure, 1 plain)	Fully configurable, up to 15 sectors (14 secure, 1 plain)	Fully configurable, up to 15 sectors (14 secure, 1 plain)	Fully configurable, up to 15 sectors (14 secure, 1 plain)
Anti-tearing support, up to 65, 536 units	Anti-tearing support, up to 65, 536 units	Anti-tearing support, up to 65, 536 units	Anti-tearing support, up to 65, 536 units
224 Byte (user), 64 Byte (admin)	224 Byte (user), 64 Byte (admin)	992 Byte (user), 256 Byte (admin)	992 Byte (user), 256 Byte (admin)
2-way mutual authentication with 64-bit secret key between reader and card for basic security. 64-bit keys for each sector enable hierarchical key management multi-application functionality transport key, unique serial number	2-way mutual authentication with 64-bit secret key between reader and card for basic security. 64-bit keys for each sector enable hierarchical key management multi-application functionality transport key, unique serial number	2-way mutual authentication with 64-bit secret key between reader and card for basic security. 64-bit keys for each sector enable hierarchical key management multi-application functionality transport key, unique serial number	2-way mutual authentication with 64-bit secret key between reader and card for basic security. 64-bit keys for each sector enable hierarchical key management multi-application functionality transport key, unique serial number
Typically up to 1.5 m	Typically up to 1.5 m	Typically up to 1.5 m	Typically up to 1.5 m
26.48 kbit/s	26.48 kbit/s	26.48 kbit/s	26.48 kbit/s
100000	100000	100000	100000
>10 years	>10 years	>10 years	>10 years
MCC2, MCC8, NiAu-bump, sawn wafer	MCC2, MCC8, NiAu-bump, sawn wafer	MCC2, MCC8, NiAu-bump, sawn wafer	MCC2, MCC8, NiAu-bump, sawn wafer
Evaluation kit contactless	Evaluation kit contactless	Evaluation kit contactless	Evaluation kit contactless
Supply chain management, library management, health-care, pharmaceutical, product authentication, amusement ticketing, access control	Supply chain management, library management, health-care, pharmaceutical, product authentication, amusement ticketing, access control	Supply chain management, library management, health-care, pharmaceutical, product authentication, amusement ticketing, access control	Inventory control, library management, health-care, pharmaceutical, product authentication, amusement ticketing, access control

Object Identification

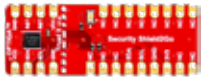
	my-d™ NFC			
Product name	**SLE 66R08P** new	**SLE 66R16P** new	**SLE 66R32P** new	**SLE 66R64P** new
Product description	my-d™ NFC, plain mode with open memory access	my-d™ NFC, plain mode with open memory access, support of NFC Forum Type 2 Tag Operation	my-d™ NFC, plain mode with open memory access , support of NFC Forum Type 2 Tag Operation	my-d™ NFC, plain mode with open memory access, support of NFC Forum Type 2 Tag Operation
Interface	ISO/IEC 14443 Type A	ISO/IEC 14443 Type A	ISO/IEC 14443 Type A	ISO/IEC 14443 Type A
Memory organization	1 fixed sector	1 fixed sector , nFC Forum Type 2 Tag up to 1024 Byte	1 fixed sector, NFC Forum Type 2 Tag up to 2048 Byte	1 fixed sector, NFC Forum Type 2 Tag up to 4096 Byte
Counter	Anti-tearing support, up to 65, 536 units	Anti-tearing support, up to 65, 536 units	Anti-tearing support, up to 65, 536 units	Anti-tearing support, up to 65, 536 units
EEPROM	1000 Byte (user), 280 Byte (admin)	2024 Byte (user), 536 Byte (admin)	4072 Byte (user), 1048 Byte (admin)	8168 Byte (user), 2072 Byte (admin)
Security features	Individual page locking, unique serial number	Individual page locking, unique serial number	Individual page locking, unique serial number	Individual page locking, unique serial number
Distance (read/write)	Typically up to 10 cm and above	Typically up to 10 cm and above	Typically up to 10 cm and above	Typically up to 10 cm and above
Data rate	106 kbit/s to card, 848 kbit/s to reader	106 kbit/s to card, 848 kbit/s to reader	106 kbit/s to card, 848 kbit/s to reader	106 kbit/s to card, 848 kbit/s to reader
Endurance	100000	100000	100000	100000
Retention time, minimum	>10 years	>10 years	>10 years	>10 years
Delivery forms	MCC2, MCC8, NiAu-bump, sawn wafer	MCC2, MCC8, NiAu-bump, sawn wafer	MCC2, MCC8, NiAu-bump, sawn wafer	MCC2, MCC8, NiAu-bump, sawn wafer
Tools	Evaluation kit contactless	Evaluation kit contactless	Evaluation kit contactless	Evaluation kit contactless
Typical applications	NFC Device pairing, smart posters, consumer goods information, data logging	NFC Device pairing, smart posters, consumer goods information, data logging	NFC Device pairing, smart posters, consumer goods information, data logging	NFC Device pairing, smart posters, consumer goods information, data logging

my-d™ proximity 2			
SLE 66R08S new	**SLE 66R16S** new	**SLE 66R32S** new	**SLE 66R64S** new
my-d™ proximity 2, security memory with security logic for memory access controlled by authentication procedures	my-d™ proximity 2, security memory with security logic for memory access controlled by authentication procedures	my-d™ proximity 2, security memory with security logic for memory access controlled by authentication procedures	my-d™ proximity 2, security memory with security logic for memory access controlled by authentication procedures
ISO/IEC 14443 Type A	ISO/IEC 14443 Type A	ISO/IEC 14443 Type A	ISO/IEC 14443 Type A
Fully configurable, up to 15 sectors (14 secure, 1 plain)	Fully configurable, up to 15 sectors (14 secure, 1 plain)	Fully configurable, up to 15 sectors (14 secure, 1 plain)	Fully configurable, up to 15 sectors (14 secure, 1 plain)
Anti-tearing support, up to 65, 536 units	Anti-tearing support, up to 65, 536 units	Anti-tearing support, up to 65, 536 units	Anti-tearing support, up to 65, 536 units
984 Byte (user), 296 Byte (admin)	2008 Byte (user), 552 Byte (admin)	4056 Byte (user), 1064 Byte (admin)	8152 Byte (user), 2088 Byte (admin)
2-way mutual authentication with 64-bit secret key between reader and card for basic security. 64-bit keys for each sector enable hierarchical key management, multi-application, functionality transport key, unique serial number	2-way mutual authentication with 64-bit secret key between reader and card for basic security. 64-bit keys for each sector enable hierarchical key management, multi-application, functionality transport key, unique serial number	2-way mutual authentication with 64-bit secret key between reader and card for basic security. 64-bit keys for each sector enable hierarchical key management, multi-application, functionality transport key, unique serial number	2-way mutual authentication with 64-bit secret key between reader and card for basic security. 64-bit keys for each sector enable hierarchical key management, multi-application, functionality transport key, unique serial number
Typically up to 10 cm and above	Typically up to 10 cm and above	Typically up to 10 cm and above	Typically up to 10 cm and above
106 kbit/s to card, 848 kbit/s to reader	106 kbit/s to card, 848 kbit/s to reader	106 kbit/s to card, 848 kbit/s to reader	106 kbit/s to card, 848 kbit/s to reader
100000	100000	100000	100000
>10 years	>10 years	>10 years	>10 years
MCC2, MCC8, NiAu-bump, sawn wafer	MCC2, MCC8, NiAu-bump, sawn wafer	MCC2, MCC8, NiAu-bump, sawn wafer	MCC2, MCC8, NiAu-bump, sawn wafer
Evaluation kit contactless	Evaluation kit contactless	Evaluation kit contactless	Evaluation kit contactless
Ticketing, consumer goods information, data logging, product authentication, access control	Ticketing, consumer goods information, data logging, product authentication, access control	Ticketing, consumer goods information, data logging, product authentication, access control	Ticketing, consumer goods information, data logging, product authentication, access control

Object Identification

	my-d™ components for terminals
Product name	**EasySAM (Secure Access Module) SLF 9620**
Product description	Secure access module for NRG™ (ISO/ IEC 14443-3 type A with CRYPTO1), interface, my-d™ algorithm, 3DES and AES128. Enables secured authentication between the reader and my-d™ chip cards or cards using NRG™(TM) (ISO/IEC 14443-3 type A with CRYPTO1) technology.
Interface	ISO 7816-3 T=1
Memory organization	Fixed pre-defined file system
Security features	NRG™ (ISO/IEC 14443-3 type A with CRYPTO1) encryption, my-d™ encryption schemes, 3DES and AES128, online and offline modes, secured key loading
Data rate	Subject to the active interface
Delivery forms	ID-1/ID-000 card (SIM format), VQFN-8
Tools	Evaluation kit contactless
Typical applications	Security applications with key-based authentication, transport ticketing, access management
Certifications	CC EAL5+ high for HW

Evaluation Boards

	OPTIGA™ Trust Shield2Go			
Product name	**S2Go Security OPTIGA™ Trust E**	**S2Go Security OPTIGA™ Trust X**	**S2Go Security OPTIGA™ Trust M** new	**MY IOT ADAPTER**
Picture				
Product description	This Shield2Go board is equipped with one OPTIGA™ Trust E security chip and comes with a ready-to-use Arduino library. By combining Shield2Go boards with Infineon MyIoT adapters, customized system solutions can be developed.	This Shield2Go board is equipped with one OPTIGA™ Trust X security chip and comes with a ready-to-use Arduino library. By combining Shield2Go boards with Infineon MyIoT adapters, customized system solutions can be developed.	This Shield2Go board is equipped with one OPTIGA™ Trust M security chip and comes with a ready-to-use Arduino library. By combining Shield2Go boards with Infineon MyIoT adapters, customized system solutions can be developed.	By combining Shield2Go boards with the Infineon My IoT adapter, customized system solutions can be developed and evaluated.
Configuration	–	–	–	Infineon Shield2Go boards
Typical applications	Device authentication, embedded systems networked over the IoT, industrial control and automation, medical devices, consumer electronics, smart home, PKI networks	Embedded systems networked over the IoT, industrial control and automation, medical devices, consumer electronics, smart home, PKI networks	Embedded systems networked over the IoT, industrial control and automation, medical devices, consumer electronics, smart home, PKI networks	Device authentication, embedded systems networked over the IoT, industrial control and automation, medical devices, consumer electronics, smart home, PKI networks
Qualification	Consumer, industrial	Consumer, industrial	Consumer, industrial	Consumer, industrial
Input type	DC	DC	DC	DC
Supply voltage min	3.13 V	3.13 V	3.13 V	3.15 V
Supply voltage max	3.63 V	3.63 V	3.63 V	5 V
Supply voltage	–	–	–	–

OPTIGA™ Trust Evaluation Kits				OPTIGA™ TPM MCU board
OPTIGA™ Trust B EVAL KIT	**OPTIGA™ Trust X EVAL KIT**	**OPTIGA™ Trust E EVAL KIT**	**OPTIGA™ Trust M EVAL KIT** new	**A-TPM BOARD SLI 9670** new
				
The OPTIGA™ Trust B SLE95250 evaluation and demonstration kit is an easy way of getting started with counterfeit protection. It can be used to demonstrate an authentication flow and to check how to read and write on the storage. The software GUI can be downloaded from the Infineon portal myICP for installation on a PC.	With the XMC4500 controller as the host on the evaluation kit allows users to connect to the OPTIGA™ Trust X (SLS 32AIA) through the I2C interface. Customers can use this evaluation kit to either debug the host lib code or demonstrate major features of the OPTIGA™ Trust X through an intuitive PC GUI.	With the XMC4500 controller as the host on the evaluation kit allows users to connect to the OPTIGA™ Trust E (SLS 32AIA) through the I2C interface. Customers can use this evaluation kit to either debug the host lib code or demonstrate major features of the OPTIGA™ Trust E through an intuitive PC GUI.	With the XMC4800 controller as the host on the evaluation kit allows users to connect to the OPTIGA™ Trust M (SLS 32AIA) through the I2C interface. Customers can use this evaluation kit to either debug the host lib code or demonstrate major features of the OPTIGA™ Trust M.	Infineon A-TPM BOARD is featuring the automotive qualified TPM SLI 9670. It is an add-on board for the Infineon AURIX™ TC3 host, supported by TPM Software Stack (TSS).
SLE95250 for XMC4500	–	–	–	SLI 9670 TPM 2.0 for AURIX™ TriBoard TC389 EVB
Battery authentication, IoT edge devices, consumer accessories, IP	Device authentication, embedded systems networked over the IoT, industrial control and automation, medical devices, consumer electronics, smart home,	Device authentication, embedded systems networked over the IoT, industrial control and automation, medical devices, consumer electronics, smart home, PKI networks	Device authentication, embedded systems networked over the IoT, industrial control and automation, medical devices, consumer electronics, smart home	Automotive security
Consumer, industrial	Consumer, industrial	Consumer, industrial	Consumer, industrial	Automotive (AEC-Q100)
DC	DC	DC	DC	DC
4.2 V	3.13 V	3.13 V	3.13 V	1.65 V
5 V	3.63 V	3.63 V	3.63 V	3.6 V
4.4 V	3.3 V	3.3 V	3.3 V	3.3 V

Evaluation Boards

	OPTIGA™ TPM Iridiumboards			
Product name	**TPM SLB 9645 IRIDIUMBOARD**	**IRIDIUM9670 TPM1.2 LINUX**	**IRIDIUM9670 TPM2.0 LINUX**	**IRIDIUM SLI9670 TPM2.0 LINUX**
Picture				
Product description	Infineon TPM SLB 9645 Iridium add-on board for Raspberry Pi and BeagleBoard xM. For integration into the corresponding platform OS (Linux, Win 10 IoT, etc.).	Infineon TPM SLB 9670 Iridium add-on board for Raspberry Pi. For integration into the corresponding platform OS (Linux, Win 10 IoT, etc.).	Infineon TPM SLB 9670 Iridium add-on board for Raspberry Pi. For integration into the corresponding platform OS (Linux, Win 10 IoT, etc.).	Infineon TPM SLI 9670 Iridium add-on board for Raspberry Pi. For integration into the corresponding platform OS (Linux etc.).
Configuration	SLB 9645 TPM 1.2 for Raspberry Pi	SLB 9670 TPM 1.2 for Raspberry Pi	SLB 9670 TPM 2.0 for Raspberry Pi	SLI 9670 TPM 2.0 for Raspberry Pi
Typical applications	Embedded computing, trusted computing	Embedded computing, trusted computing	Embedded computing, trusted computing	Automotive security
Qualification	Consumer, industrial	Consumer, industrial	Consumer, industrial	Automotive (AEC-Q100)
Input type	DC	DC	DC	DC
Supply voltage min	1.65 V	1.65 V	1.65 V	1.65 V
Supply voltage max	3.6 V	3.6 V	3.6 V	3.6 V
Supply voltage	3.3 V	3.3 V	3.3 V	3.3 V

	OPTIGA™ TPM Xenonboards		
IRIDIUM SLM9670 TPM2.0 LINUX	**TPM 70 1.2 XENONBOARD**	**TPM 65 XENONBOARD**	**TPM 70 2.0 XENONBOARD**
			
Infineon TPM SLM 9670 Iridium add-on board for Raspberry Pi. For integration into the corresponding platform OS (Linux, Win 10 IoT, etc.).	Infineon TPM SLB 9670 Xenon is an add-on board for the PC platform. For integration into the corresponding platform OS (Windows, Linux, Win 10 IoT, etc.).	Infineon TPM SLB 9665 Xenon is an add-on board for a PC platform. For integration into the corresponding platform OS (Windows, Linux, Win 10 IoT, etc.).	Infineon TPM SLB 9670 Xenon is an add-on board for the PC platform. For integration into the corresponding platform OS (Windows, Linux, Win 10 IoT, etc.).
SLM 9670 TPM 2.0 for Raspberry Pi	SLB 9670 TPM 1.2 for a PC platform	SLB 9665 TPM 2.0 for a PC platform	SLB 9670 TPM 2.0 for a PC platform
Industrial computing, industrial PCs, servers, tablets, single-board computers, Programmable Logic Controllers (PLCs), industrial networking infrastructure & equipment, industrial servers, gateways, routers, switches	Embedded computing, trusted computing	Embedded computing, trusted computing	Embedded computing, trusted computing
–	–	–	–
DC	DC	DC	DC
1.65 V	1.65 V	3 V	1.65 V
3.6 V	3.6 V	3.6 V	3.6 V
3.3 V	3.3 V	3.3 V	3.3 V

Modules

	Contactless controller & memory modules			Contact-based controller modules
Product name	**P-MCS8-2-1**	**P-MCC8-2-6**	**P-MCC2-2-1**	**S-MID4.8**
Picture				
Product description	Thin contactless module, mold	Standard contactless module, mold	Contactless module, mold	Contact-based module for highly demanding applications
Pitch	9.5 mm	9.5 mm	4.75 mm	14.25 mm
Dimensions	8.1 x 5.15 mm	8.1 x 5.15 mm	10.3 x 2.9 mm	13 x 11.8 mm
Thickness	max. 250 µm	max. 340 µm	max. 330 µm	max. 420 µm
Contact surface	Ag	Ag	Ag	NiAu
ISO reference	ISO 7816-1, ISO 10373-1/-3, ISO 7810, ISO 14443	ISO 7816-1, ISO 10373-1/-3, ISO 7810, ISO 14443	ISO 7816-1, ISO 10373-1/-3, ISO 7810, ISO 14443	ISO 7816-1, ISO 10373-1/-3, ISO 7810
Derivatives	–	–	–	Au surface, Pd surface
Delivery form	Tape on Reel	Tape on Reel	Tape on Reel	Tape on Reel
Main applications	Payment, government identification	Payment, government identification, transport ticketing	Access control, transport ticketing	Authentication, government identification

S-MFC6.8	S-MFC6.6	P-M2M4.7	P-M4.8	T-M4.8
				
Contact-based module, 8 contacts	Contact-based module, 6 contacts	Contact-based module, 8 contacts, epoxy tape, mold, wire bond	Contact-based module, 8 contacts, epoxy tape, mold, wire bond	Contact-based module, 8 contacts, epoxy tape, wire bond globe top
14.25 mm	9.5 mm	14.25 mm	14.25 mm	14.25 mm
13 x 11.8 mm	11 x 8.3 mm	12.8 x 10.8 mm	13 x 11.8 mm	13 x 11.8 mm
max. 420 µm	max. 420 µm	max. 600 µm	max. 600 µm	max. 580 µm
NiAu	NiAu	NiAu	NiAu	NiAu
ISO 7816-1, ISO 10373-1/-3, ISO 7810	ISO 7816-1, ISO 10373-1/-3, ISO 7810	ISO 7816-1, ISO 10373-1/-3, ISO 7810	ISO 7816-1, ISO 10373-1/-3, ISO 7810	ISO 7816-1, ISO 10373-1/-3, ISO 7810
Au surface, Pd surface	Au surface, Pd surface	Au surface	Au surface, Pd surface	Au surface, Pd surface
Tape on Reel	Tape on Reel	Tape on Reel	Tape on Reel	Tape on Reel
Payment, government identification	Payment, government identification	M2M	Payment, government identification	Payment, government identification, Pay TV

Modules

	Dual-interface modules			
Product name	**S-COM10.6** Coil on Module	**S-COM8.6** Coil on Module	**S-COM8.4** Coil on Module	**S-COMCL1-0-1** Coil on Module
Picture				
Product description	Dual-interface module with inductive coupling for highly demanding applications	Dual-interface module, 6 CB contacts, inductive coupling	Dual-interface module, 6 CB contacts, inductive coupling	Ultra-thin contactless module, with inductive coupling
Pitch	14.25 mm	14.25 mm	9.5 mm	9.5 mm
Dimensions	13 x 11.8 mm	13 x 11.8 mm	11 x 8.3 mm	8 x 8 mm
Thickness	max. 420 µm	max. 420 µm	max. 320 µm	max. 125 µm
Contact surface	NiAu	NiAu	NiAu	Inductive coupling
ISO reference	ISO 7816-1, ISO 10373-1/-3, ISO 7810, ISO 14443	ISO 7816-1, ISO 10373-1/-3, ISO 7810, ISO 14443	ISO 7816-1, ISO 10373-1/-3, ISO 7810, ISO 14443	ISO 7816-1, ISO 10373-1/-3, ISO 7810, ISO 14443
Derivatives	Au surface, Pd surface	Au surface, Pd surface	Au surface, Pd surface	-
Delivery form	Tape on Reel	Tape on Reel	Tape on Reel	Tape on Reel
Main applications	Authentication, government identification, payment	Payment, government identification	Payment, government identification	Government identification

T-M8.8	P-M8.4	T-M8.6	S-SPA1.x	S-COM10.8 new Coil on Module
				
Standard dual-interface module, 2 antenna contacts, 8 CB contacts	Dual-interface module, mold, 2 antenna contacts, 8 CB contacts, epoxy tape, wire bond	Standard dual-interface module, 2 antenna contacts, 6 CB contacts	Smart Payment Accessory - the ready-to-use solution for wearables and stickers	Dual-interface module with inductive coupling for highly demanding applications
14.25 mm	14.25 mm	9.25 mm	19.00 mm	14.25 mm
13 x 11.8 mm	13 x 11.8 mm	11 x 8.3 mm	27.2 x 17.5 mm	13 x 11.8 mm
max. 580 µm	max. 620 µm	max. 580 µm	max. 300 µm	max. 420 µm
NiAu	NiAu	NiAu	n.a.	NiAu
ISO 7816-1, ISO 10373-1/-3, ISO 7810, ISO 14443	ISO 7816-1, ISO 10373-1/-3, ISO 7810, ISO 14443	ISO 7816-1, ISO 10373-1/-3, ISO 7810, ISO 14443	EMVCo	ISO 7816-1, ISO 10373-1/-3, ISO 7810, ISO 14443
Au surface, Pd surface	Au surface, Pd surface	Au surface, Pd surface	n.a.	Au surface, Pd surface
Tape on Reel	Tape on Reel	Tape on Reel	Tape on Reel	Tape on Reel
Payment, government identification	Payment, government identification	Payment, government identification	Payment	Authentication, government identification

SMD

	SMD packages			
Product name	**TSNP-6-9**	**TSSOP-28-2**	**VQFN-8-1, -2, -4, -6/MFF2**	**VQFN-10-2**
Picture				
Product description	Thin Small Non-leaded Package	Thin shrink small outline, gull-wing lead	Small outline no leads, exposed pad	Small outline no leads, exposed pads
Pitch	0.5 mm	0.65 mm	1.27 mm	1.27 mm
Dimensions	1.1 x 1.5 mm	9.7 x 4.4 mm	5 x 6 mm	6 x 5 mm
Thickness	0.375 mm	max. 1.1 mm	max. 900 µm	max. 900 µm
Contact surface	Sn	Sn	NiPd-AuAg	NiPd-AuAg
ISO reference	–	–	–	–
Derivatives	–	–	–	–
Delivery form	Tape & Reel	Tape & Reel	Tape & Reel	Tape & Reel
Main applications	Authentication	Trusted Computing	Automotive M2M, industrial M2M, consumer M2M, authentication	Authentication, Pay TV

VQFN-32-13, -20	USON-8-1, -4	USON-8-3	USON-10-1	USON-10-2, -4
				
Quad flat no leads, exposed pad	Small outline no leads, exposed bar pad	Small outline no-leads, exposed pad	Small outline no leads, exposed bar pad	Small outline no leads, exposed pad
0.5 mm	0.5 mm	1.0 mm	0.5 mm	0.5 mm
5 x 5 mm	2.5 x 2.5 mm	4.2 x 4.0 mm	3 x 3 mm	3 x 3 mm
max. 900 µm	max. 600 µm	max. 600 µm	max. 600 µm	max. 600 µm
NiPd-AuAg	NiPd-AuAg	NiPd-AuAg	NiPd-AuAg	NiPd-AuAg
–	–	–	–	–
–	–	–	–	–
Tape & Reel	Tape & Reel	Tape & Reel	Tape & Reel	Tape & Reel
Embedded secure element, Trusted Computing, USB tokens	Authentication	Authentication	Authentication	Authentication

SMD

	SMD packages			
Product name	**X2QFN-24-1** new	**USON-8-5** new	**USON-8-6** new	**USON-6-2** new
Picture				
Product description	Small outline no leads, exposed pad	Small outline no leads, exposed pad	Small outline no leads, exposed pad	Small outline no leads, exposed pad
Pitch	0.5 mm	0.5 mm	0.5 mm	0.5 mm
Dimensions	4 x 4 mm	2 x 2 mm	2 x 2 mm	3 x 2.3 mm
Thickness	max. 330 µm	max. 600 µm	max. 600 µm	max. 600 µm
Contact surface	NiPd-AuAg	NiPd-AuAg	NiPd-AuAg	NiPd-AuAg
ISO reference	–	–	–	–
Derivatives	–	–	–	–
Delivery form	Tape & Reel	Tape & Reel	Tape & Reel	Tape & Reel
Main applications	–	–	–	–

TSNP-6-12 new	VQFN-32-19 new from April 2021
	
Thin Small Non-leaded Package	Small outline no leads, exposed pad
0.5 mm	0.4 mm
1,5 x 1,5 mm	4 x 4 mm
max. 400 µm	max. 900 µm
Sn	NiPd-AuAg
–	–
–	–
Tape & Reel	Tape & Reel
–	–

SMD

	SMD packages			
Product name	**SG-WFWLB-16-3** new	**SG-XFWLB-25-3** new	**SG-XFWLB-6-2** new	**SG-XFWLB-6-3** new
Picture				
Product description	Chip scale package, solder ball array	Chip scale package, solder ball array	Chip scale package, solder ball array	Chip scale package, solder ball array
Pitch	0.5 mm	0.4mm	0.4mm	0.4mm
Dimensions	2.72 x 2.55 mm	2.926 x 2.554 mm	1.278 x 1.256 mm	0.946 x 1.17 mm
Thickness	max. 700 µm	max. 430 µm	max. 430 µm	max. 430 µm
Contact surface	SnAgCu	SnAgCu	SnAgCu	SnAgCu
ISO reference	–	–	–	–
Derivatives	–	–	–	–
Delivery form	Tape & Reel	Tape & Reel	Tape & Reel	Tape & Reel
Main applications	Near-field communication, embedded secure element, authentication	–	–	–

Wafer delivery forms

	Wafer delivery forms		
Product name	**Bumping NiAu**	**Stud Bump**	**Wafer Thinning and Dicing**
Picture			
Product description	NiAu bump on the pad	Gold bump on the pad	Bare die delivery on UV foil in wafer frame
Thickness	–	–	55 µm, 150 µm other thicknesses on request
Mapping	Based on SEMI	Based on SEMI	Based on SEMI
Delivery form	Sawn wafer on UV foil	Sawn wafer on UV foil	Sawn wafer on UV foil
Documents	Specification NiAu bumping, chip delivery specification for 8” wafer, general and product-specific issues	Specification stud bumping, chip delivery specification for 8”/12” wafer, general and product-specific issues	Chip delivery specification for 8”/12” wafer, general and product-specific issues

Notes

Service Hotline

Infineon offers its toll-free 0800/4001 service hotline as one central number, available 24/7 in English, Mandarin and German.

- Germany ..... 0800 951 951 951 (German/English)
- China, mainland ..... 4001 200 951 (Mandarin/English)
- India ..... 000 800 4402 951 (English)
- USA ..... 1-866 951 9519 (English/German)
- Other countries ..... 00* 800 951 951 951 (English/German)
- Direct access ..... +49 89 234-0 (interconnection fee, German/English)

* Please note: Some countries may require you to dial a code other than "00" to access this international number. Please visit www.infineon.com/service for your country!

Where to Buy

Infineon Distribution Partners and Sales Offices:
www.infineon.com/WhereToBuy

Mobile Product Catalog

Mobile app for iOS and Android.

More information:

www.infineon.com/security

Published by
Infineon Technologies AG
81726 Munich, Germany

Document number: B180-I0041-V6-7600-EU-EC
Date: 02/2020

Please note!
This Document is for information purposes only and any information given herein shall in no event be regarded as a warranty, guarantee or description of any functionality, conditions and/or quality of our products or any suitability for a particular purpose. With regard to the technical specifications of our products, we kindly ask you to refer to the relevant product data sheets provided by us. Our customers and their technical departments are required to evaluate the suitability of our products for the intended application.

We reserve the right to change this document and/or the information given herein at any time.

Additional information
For further information on technologies, our products, the application of our products, delivery terms and conditions and/or prices, please contact your nearest Infineon Technologies office (www.infineon.com).

Warnings
Due to technical requirements, our products may contain dangerous substances. For information on the types in question, please contact your nearest Infineon Technologies office.

Except as otherwise explicitly approved by us in a written document signed by authorized representatives of Infineon Technologies, our products may not be used in any life-endangering applications, including but not limited to medical, nuclear, military, life-critical or any other applications where a failure of the product or any consequences of the use thereof can result in personal injury.