

# INFINEON CHIP CARD IC PORTFOLIO

Proven security you can trust



[www.infineon.com/security](http://www.infineon.com/security)



Never stop thinking

## Contactless memories

	my-d® light	my-d® vicinity								PJM ItemTag® and PJM StackTag®
Product name	SRF 55Vo1P	SRF 55Vo2P	SRF 55Vo2P HC	SRF 55Vo1P	SRF 55Vo1P HC <span style="border: 1px solid black; padding: 2px;">new</span>	SRF 55Vo2S	SRF 55Vo1S	SRF 66Vo1T	SRF 66Vo1 ST	
<b>Product description</b>	Plain memory, 576-bit EEPROM	Plain memory, 2.5 kbit EEPROM	Plain memory, 2.5 kbit EEPROM	Plain memory, 10 kbit EEPROM	Plain memory, 10 kbit EEPROM	Security memory with authentication, 2.5 kbit EEPROM	Security memory with authentication, 10 kbit EEPROM	Plain memory, 10 kbit EEPROM	Plain memory, zero separation stackability, 10 kbit EEPROM	
<b>Interface</b>	ISO/IEC 18000-3 mode 1	ISO/IEC 18000-3 mode 1	ISO/IEC 18000-3 mode 1	ISO/IEC 18000-3 mode 1	ISO/IEC 18000-3 mode 1	ISO/IEC 18000-3 mode 1	ISO/IEC 18000-3 mode 1	ISO/IEC 18000-3 mode 2	ISO/IEC 18000-3 mode 2	
<b>Memory organization</b>	1 fixed sector	1 fixed sector	1 fixed sector	1 fixed sector	1 fixed sector	Up to 15 sectors fully configurable (14 secure, 1 plain)	Up to 15 sectors fully configurable (14 secure, 1 plain)	1 fixed sector	1 fixed sector	
<b>Counter</b>	–	Up to 65,536 units, support of anti-tearing	Up to 65,536 units, support of anti-tearing	Up to 65,536 units, support of anti-tearing	Up to 65,536 units, support of anti-tearing	Up to 65,536 units, support of anti-tearing	Up to 65,536 units, support of anti-tearing	–	–	
<b>Operating frequency</b>	13.56 MHz	13.56 MHz	13.56 MHz	13.56 MHz	13.56 MHz	13.56 MHz	13.56 MHz	13.56 MHz	13.56 MHz	
<b>EEPROM – user</b>	52 Byte	224 Byte	224 Byte	992 Byte	992 Byte	224 Byte	992 Byte	1,016 Byte	1,016 Byte	
<b>EEPROM – administration</b>	20 Byte	64 Byte	64 Byte	256 Byte	256 Byte	64 Byte	256 Byte	14 Byte	14 Byte	
<b>Security features</b>	Unique serial number, individual page locking	Unique serial number, individual page locking	Unique serial number, individual page locking	Unique serial number, individual page locking	Unique serial number, individual page locking	Transport key, unique serial number, mutual authentication with 64-bit keys, hierarchical key management	Transport key, unique serial number, mutual authentication with 64-bit keys, hierarchical key management	Unique serial number, lock pointer, 48-bit write password	Unique serial number, lock pointer, 48-bit write password	
<b>Distance (read/write)</b>	Typically up to 1,5 m <sup>1)</sup>	Typically up to 1,5 m <sup>1)</sup>	Typically up to 1,5 m <sup>1)</sup>	Typically up to 1,5 m <sup>1)</sup>	Typically up to 1,5 m <sup>1)</sup>	Typically up to 1,5 m <sup>1)</sup>	Typically up to 1,5 m <sup>1)</sup>	Typically up to 1 m <sup>1)</sup>	Typically up to 1 m <sup>1)</sup>	
<b>Data rate</b>	26.48 kbit/s	26.48 kbit/s	26.48 kbit/s	26.48 kbit/s	26.48 kbit/s	26.48 kbit/s	26.48 kbit/s	423.75 kbit/s to card, 105.94 kbit/s to reader @ 8 channels	423.75 kbit/s to card, 105.94 kbit/s to reader @ 8 channels	
<b>Anticollision</b>	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	
<b>Ambient temperature</b>	-25 to +70°	-25 to +70°	-25 to +70°	-25 to +70°	-25 to +70°	-25 to +70°	-25 to +70°	-25 to +70°	-25 to +70°	
<b>Endurance</b>	100,000	100,000	100,000	100,000	100,000	100,000	100,000	100,000	100,000	
<b>Retention time, minimum</b>	10 years	10 years	10 years	10 years	10 years	10 years	10 years	10 years	10 years	
<b>Delivery forms</b>	Wafer, NiAu-bump	Wafer, NiAu-bump, module MCC2	Wafer, NiAu-bump, module MCC2	Wafer, NiAu-bump, module MCC2	Wafer, NiAu-bump, module MCC2	Wafer, NiAu-bump, module MCC2	Wafer, NiAu-bump, module MCC2	Wafer, NiAu-bump	Wafer, NiAu-bump	
<b>Tools</b>	Evaluation Kit my-d®	Evaluation Kit my-d®	Evaluation Kit my-d®	Evaluation Kit my-d®	Evaluation Kit my-d®	Evaluation Kit my-d®	Evaluation Kit my-d®	Evaluation Kit PJM®	Evaluation Kit PJM®	
<b>Typical applications</b>	Libraries, Supply Chain Management	Libraries, Inventory Control	Laundry, CD Inlays	Libraries, Inventory Control	Factory Automation, Inventory Control	Ticketing, Brand Protection	Ticketing, Brand Protection	Factory Automation, Production Control	Pharmaceuticals, Document Management	

<sup>1)</sup> Depending on reader system and tag antenna configuration

<sup>2)</sup> NFC compatible. This product is compliant to ISO/IEC and ECMA standards as stated in the respective product specifications, allowing for building NFC devices as defined by the NFC Forum.

Mifare® is a registered trademark of NXP Semiconductors

PJM StackTag® and PJM ItemTag® are registered trademarks of Magellan Technology Pty Ltd. Corp.

## Contactless memories

	my-d® proximity 2 <sup>1)</sup>	my-d® proximity 2 <sup>1)</sup>	my-d® proximity 2 <sup>1)</sup>	my-d® proximity 2 <sup>1)</sup>	my-d® proximity 2 <sup>1)</sup>	my-d® proximity 2 <sup>1)</sup>	Mifare® SLE 66R35 <sup>2)</sup>
<b>Product name</b>	<b>SLE 55R04</b>	<b>SLE 55R16</b>	<b>SLE 66R04P</b>	<b>SLE 66R16P</b>	<b>SLE 66R04S</b>	<b>SLE 66R16S</b>	<b>SLE 66R35</b>
<b>Product description</b>	Security memory with authentication, 770 Byte EEPROM	Security memory with authentication, 2,560 Byte EEPROM	Plain memory, 770 Byte EEPROM	Plain memory, 2,560 Byte EEPROM	Security memory with authentication, 770 Byte EEPROM	Security memory with authentication, 2,560 Byte EEPROM	Intelligent 1 kByte EEPROM with Mifare algorithm
<b>Interface</b>	ISO/IEC 14443 (type A)	ISO/IEC 14443 (type A)	ISO/IEC 14443 (type A)	ISO/IEC 14443 (type A)	ISO/IEC 14443 (type A)	ISO/IEC 14443 (type A)	ISO/IEC 14443 (type A)
<b>Memory organization</b>	Up to 15 sectors fully configurable (14 secure, 1 plain)	Up to 15 sectors fully configurable (14 secure, 1 plain)	1 fixed sector	1 fixed sector	Up to 15 sectors fully configurable (14 secure, 1 plain)	Up to 15 sectors fully configurable (14 secure, 1 plain)	16 fixed sectors
<b>Counter</b>	Up to 65,536 units, support of anti-tearing	Up to 65,536 units, support of anti-tearing	Up to 65,536 units, support of anti-tearing	Up to 65,536 units, support of anti-tearing	Up to 65,536 units, support of anti-tearing	Up to 65,536 units, support of anti-tearing	–
<b>Operating frequency</b>	13.56 MHz	13.56 MHz	13.56 MHz	13.56 MHz	13.56 MHz	13.56 MHz	13.56 MHz
<b>EEPROM – user</b>	616 Byte	2,048 Byte	616 Byte	2,048 Byte	616 Byte	2,048 Byte	768 Byte
<b>EEPROM – administration</b>	154 Byte	512 Byte	154 Byte	512 Byte	154 Byte	512 Byte	256 Byte
<b>Security features</b>	Transport key, unique serial number, mutual authentication with 64-bit keys, hierarchical key management	Transport key, unique serial number, mutual authentication with 64-bit keys, hierarchical key management	Unique serial number, individual page locking	Unique serial number, individual page locking	Transport key, unique serial number, mutual authentication with 64-bit keys, hierarchical key management	Transport key, unique serial number, mutual authentication with 64-bit keys, hierarchical key management	Transport code, unique serial number, mutual three pass authentication with 48-bit keys
<b>Distance (read/write)</b>	Typically up to 10 cm and above <sup>3)</sup>	Typically up to 10 cm and above <sup>3)</sup>	Typically up to 10 cm and above <sup>3)</sup>	Typically up to 10 cm and above <sup>3)</sup>	Typically up to 10 cm and above <sup>3)</sup>	Typically up to 10 cm and above <sup>3)</sup>	Typically up to 10 cm and above <sup>3)</sup>
<b>Data rate</b>	105,94 kbit/s	105,94 kbit/s	105,94 kbit/s	105,94 kbit/s	105,94 kbit/s	105,94 kbit/s	105,94 kbit/s
<b>Anticollision</b>	Yes	Yes	Yes	Yes	Yes	Yes	Yes
<b>Ambient temperature</b>	-25 to +70°	-25 to +70°	-25 to +70°	-25 to +70°	-25 to +70°	-25 to +70°	-25 to +70°
<b>Endurance</b>	100,000	100,000	100,000	100,000	100,000	100,000	100,000
<b>Retention time, minimum</b>	10 years	10 years	10 years	10 years	10 years	10 years	10 years
<b>Delivery forms</b>	Wafer, NiAu-bump, module MCC2	Wafer, NiAu-bump, module MCC2	Wafer, NiAu-bump, module MCC2	Wafer, NiAu-bump, module MCC2	Wafer, NiAu-bump, module MCC2	Wafer, NiAu-bump, module MCC2	Wafer, NiAu-bump, module MCCB, MCC2
<b>Tools</b>	Evaluation Kit my-d®	Evaluation Kit my-d®	Evaluation Kit my-d®	Evaluation Kit my-d®	Evaluation Kit my-d®	Evaluation Kit my-d®	Evaluation Kit proximity
<b>Typical applications</b>	Access, Entertainment	Access, Entertainment	Ticketing, Customer Loyalty Schemes	Ticketing, Customer Loyalty Schemes	Access, Entertainment	Access, Entertainment	Transport, Access

<sup>1)</sup> Depending on reader system and tag antenna configuration

<sup>2)</sup> NFC compatible. This product is compliant to ISO/IEC and ECMA standards as stated in the respective product specifications, allowing for building NFC devices as defined by the NFC Forum.

Mifare® is a registered trademark of NXP Semiconductors

## Dual-interface/ contactless Controller

	SLE 66CLxxxxP				SLE 66CLxxxxPE			
Product name	SLE 66CL320P	SLE 66CL321P	SLE 66CL640P	SLE 66CL641P	SLE 66CL41PE	SLE 66CL80PE (M/S)	SLE 66CL81PE (M)	
<b>Product description</b>	Dual-interface security cryptocontroller	Pure contactless security cryptocontroller	Dual-interface security cryptocontroller	Pure contactless security cryptocontroller	Pure contactless security cryptocontroller	Dual-interface security controller	Pure contactless security controller	
<b>RF Interface</b>	ISO/IEC 14443 B & A	ISO/IEC 14443 B & A	ISO/IEC 14443 B & A	ISO/IEC 14443 B & A	ISO/IEC 14443 B & A	ISO/IEC 14443 type B & A ISO/IEC 18092 passive mode Mifare® emulation	ISO/IEC 14443 type B & A Mifare® emulation	
<b>Baudrate (kbit/s)</b>	up to 424 kbit/s	up to 424 kbit/s	up to 424 kbit/s	up to 424 kbit/s	up to 848 kbit/s	up to 848 kbit/s	up to 848 kbit/s	
<b>User-ROM</b>	136 kByte	136 kByte	134 kByte	134 kByte	92 kByte	92 kByte (88 kByte) <sup>1)</sup>	92 kByte (88 kByte) <sup>1)</sup>	
<b>EEPROM</b>	32 kByte	32 kByte	64 kByte	64 kByte	4 kByte	8 kByte (+ 1 kByte for M) <sup>1)</sup>	8 kByte (+ 1 kByte for M) <sup>1)</sup>	
<b>RAM</b>	4,352 + 700 Byte crypto	4,352 + 700 Byte crypto	4,352 + 700 Byte crypto	4,352 + 700 Byte crypto	2 kByte XRAM, 256 Byte IRAM	2 kByte XRAM, 256 Byte IRAM	2 kByte XRAM, 256 Byte IRAM	
<b>CPU</b>	8-bit/16-bit	8-bit/16-bit	8-bit/16-bit	8-bit/16-bit	8-bit/16-bit	8-bit/16-bit	8-bit/16-bit	
<b>Crypto coprocessor</b>	1,100-bit arithmetic	1,100-bit arithmetic	1,100-bit arithmetic	1,100-bit arithmetic	–	–	–	
<b>Hardware triple DES</b>	Yes	Yes	Yes	Yes	Yes	Yes	Yes	
<b>Clock (int.)</b>	1 – 15 MHz	1 – 15 MHz	1 – 15 MHz	1 – 15 MHz	1 – 30 MHz	1 – 30 MHz	1 – 30 MHz	
<b>Clock (ext.)</b>	1 – 5 MHz	–	1 – 5 MHz	–	–	1 – 7.5 MHz	–	
<b>Operating voltage</b>	2.7 V – 5.5 V	2.7 V – 5.5 V	2.7 V – 5.5 V	2.7 V – 5.5 V	1.62 V – 5.5 V	1.62 V – 5.5 V	1.62 V – 5.5 V	
<b>Max. sleep mode current (typ.)</b>	100 µA	100 µA	100 µA	100 µA	100 µA	100 µA	100 µA	
<b>Ambient temperature</b>	-25 to +70°	-25 to +70°	-25 to +70°	-25 to +70°	-25 to +70°	-25 to +70°	-25 to +70°	
<b>EEPROM Programming Time @ contactless operation</b>	< 4.0 ms (typ.)	< 4.0 ms (typ.)	< 4.0 ms (typ.)	< 4.0 ms (typ.)	< 2.3 ms (typ.)	< 2.3 ms (typ.)	< 2.3 ms (typ.)	
<b>EEPROM page programming</b>	1 to 256 Byte	1 to 256 Byte	1 to 256 Byte	1 to 256 Byte	1 to 64 Byte	1 to 64 Byte	1 to 64 Byte	
<b>MMU</b>	Yes	Yes	Yes	Yes	Yes	Yes	Yes	
<b>Security features</b>	Tamper-proof design, chip ID, countermeasures against reverse engineering, SPA/DPA, DFA/EMA, memory encryption, sensor concept: voltage-, frequency-, light-, temperature-, glitch sensor, active shield, triple DES in HW, asymmetric algorithms, hardware-supported (e.g. RSA, ECC)	Tamper-proof design, chip ID, countermeasures against reverse engineering, SPA/DPA, DFA/EMA, memory encryption, sensor concept: voltage-, frequency-, light-, temperature-, glitch sensor, active shield, triple DES in HW, asymmetric algorithms, hardware-supported (e.g. RSA, ECC)	Tamper-proof design, chip ID, countermeasures against reverse engineering, SPA/DPA, DFA/EMA, memory encryption, sensor concept: voltage-, frequency-, light-, temperature-, glitch sensor, active shield, triple DES in HW, asymmetric algorithms, hardware-supported (e.g. RSA, ECC)	Tamper-proof design, chip ID, countermeasures against reverse engineering, SPA/DPA, DFA/EMA, memory encryption, sensor concept: voltage-, frequency-, light-, temperature-, glitch sensor, active shield, triple DES in HW, asymmetric algorithms, hardware-supported (e.g. RSA, ECC)	Tamper-proof design, chip ID, countermeasures against reverse engineering, SPA/DPA, DFA/EMA, memory encryption, sensor concept: voltage-, frequency-, light-, temperature-, glitch sensor, active shield, triple DES in HW	Tamper-proof design, chip ID, countermeasures against reverse engineering, SPA/DPA, DFA/EMA, memory encryption, sensor concept: voltage-, frequency-, light-, temperature-, glitch sensor, active shield, triple DES in HW	Tamper-proof design, chip ID, countermeasures against reverse engineering, SPA/DPA, DFA/EMA, memory encryption, sensor concept: voltage-, frequency-, light-, temperature-, glitch sensor, active shield, triple DES in HW	Tamper-proof design, chip ID, countermeasures against reverse engineering, SPA/DPA, DFA/EMA, memory encryption, sensor concept: voltage-, frequency-, light-, temperature-, glitch sensor, active shield, triple DES in HW
<b>Peripherals</b>	2 x 16-bit autoreload timers, PLL, interrupt, CRC, RNG, UART, DES, ACE	2 x 16-bit autoreload timers, PLL, interrupt, CRC, RNG, DES, ACE	2 x 16-bit autoreload timers, PLL, interrupt, CRC, RNG, UART, DES, ACE	2 x 16-bit autoreload timers, PLL, interrupt, CRC, RNG, DES, ACE	2 x 16-bit autoreload timers, PLL, interrupt, CRC, RNG, DES	2 x 16-bit autoreload timers, PLL, interrupt, CRC, UART, RNG, DES	2 x 16-bit autoreload timers, PLL, interrupt, CRC, RNG, DES	
<b>Delivery forms</b>	Module M8.4, die, bumped wafer	Contactless module MCC8, die, bumped wafer	Module M8.4, die, bumped wafer	Module M8.4, die, bumped wafer	Contactless module MCC8, die, bumped wafer	Module M8.4, die, bumped wafer	Contactless module MCC8, die, bumped wafer	
<b>Typical applications</b>	Digital Signature, ID-Card, Open Platform	Digital Signature, ID-Card, Open Platform	Digital Signature, ID-Card, Open Platform	Digital Signature, ID-Card, Open Platform	Payment, EMV SDA, ePurse, Loyalty, Access, Driver Licence, Transport	Payment, EMV SDA, ePurse, Loyalty, Access, Driver Licence, Transport	Payment, EMV SDA, ePurse, Loyalty, Access, Driver Licence, Transport	
<b>Tools</b>	EKP (Evaluation Kit Proximity) ROK (Reader Optimization Kit)	EKP (Evaluation Kit Proximity) ROK (Reader Optimization Kit)	EKP (Evaluation Kit Proximity) ROK (Reader Optimization Kit)	EKP (Evaluation Kit Proximity) ROK (Reader Optimization Kit)	EKP (Evaluation Kit Proximity) ROK (Reader Optimization Kit)	EKP (Evaluation Kit Proximity) ROK (Reader Optimization Kit)	EKP (Evaluation Kit Proximity) ROK (Reader Optimization Kit)	
<b>Certifications</b>	CC EAL5+ high (PP0002), VISA level 3, CAST, VISA® Wave	CC EAL5+ high (PP0002), VISA level 3, CAST	CC EAL5+ high (PP0002), VISA level 3, CAST	CC EAL5+ high (PP0002), VISA level 3, CAST	CC EAL5+ high (PP0002), VISA level 3, CAST, Mastercard PayPass® MS, VISA® MSD	CC EAL5+ high (PP0002), VISA level 3, CAST	CC EAL5+ high (PP0002), VISA level 3, CAST, Mastercard PayPass® MS, VISA® MSD	

<sup>1)</sup> If Mifare® emulation is used  
MasterCard PayPass® is a registered trademark of MasterCard Worldwide. VISA® is a registered trademark of Visa Inc.

## Dual-interface/ contactless Controller

SLE 66CLxxxxPE							
Product name	SLE 66CL180PE (M/S)	SLE 66CLx80PE (M/S) <span style="float: right;">new</span>	SLE 66CLx20PE (M/S) <span style="float: right;">new</span>	SLE 66CL360PE (M/S)	SLE 66CLX800PE (M/S)	SLE 66CLx280PE (M/S) <span style="float: right;">new</span>	SLE 66CLx440PE (M/S) <span style="float: right;">new</span>
<b>Product description</b>	Dual-interface and contactless security controller	Dual-interface and contactless security cryptocontroller	Dual-interface and contactless security cryptocontroller	Dual-interface and contactless security cryptocontroller	Dual-interface and contactless security cryptocontroller	Dual-interface and contactless security cryptocontroller	Dual-interface and contactless security cryptocontroller
<b>RF Interface</b>	ISO/IEC 14443 type B & A ISO/IEC 18092 passive mode Mifare® emulation	ISO/IEC 14443 type B & A ISO/IEC 18092 passive mode Mifare® emulation	ISO/IEC 14443 type B & A ISO/IEC 18092 passive mode Mifare® emulation	ISO/IEC 14443 type B & A ISO/IEC 18092 passive mode Mifare® emulation	ISO/IEC 14443 type B & A ISO/IEC 18092 passive mode Mifare® emulation	ISO/IEC 14443 type B & A ISO/IEC 18092 passive mode Mifare® emulation	ISO/IEC 14443 type B & A ISO/IEC 18092 passive mode Mifare® emulation
<b>Baudrate (kbit/s)</b>	up to 848 kbit/s	up to 848 kbit/s	up to 848 kbit/s	up to 848 kbit/s	up to 848 kbit/s	up to 848 kbit/s	up to 848 kbit/s
<b>User-ROM</b>	92 kByte (88 kByte) <sup>1)</sup>	156 kByte (152 kByte) <sup>1)</sup>	156 kByte (152 kByte) <sup>1)</sup>	240 kByte (236 kByte) <sup>1)</sup>	240 kByte (236 kByte) <sup>1)</sup>	240 kByte (236 kByte) <sup>1)</sup>	240 kByte (236 kByte) <sup>1)</sup>
<b>EEPROM</b>	18 kByte (16 kByte + 1 kByte for M) <sup>1)</sup>	18 kByte (16 kByte + 1 kByte for M) <sup>1)</sup>	12 kByte (10 kByte + 1 kByte for M) <sup>1)</sup>	36 kByte (+ 1 kByte for M) <sup>1)</sup>	80 kByte (78 kByte + 1 kByte for M) <sup>1)</sup>	128 kByte (128 kByte + 1 kByte for M) <sup>1)</sup>	144 kByte (128 kByte + 1 kByte for M) <sup>1)</sup>
<b>RAM</b>	2 kByte XRAM, 256 Byte IRAM	4 kByte XRAM, 700 Byte Crypto, 256 Byte IRAM	4 kByte XRAM, 700 Byte Crypto, 256 Byte IRAM	6 kByte XRAM, 700 Byte Crypto, 256 Byte IRAM	6 kByte XRAM, 700 Byte Crypto, 256 Byte IRAM	6 kByte XRAM, 700 Byte Crypto, 256 Byte IRAM	6 kByte XRAM, 700 Byte Crypto, 256 Byte IRAM
<b>CPU</b>	8-bit/16-bit	8-bit/16-bit	8-bit/16-bit	8-bit/16-bit	8-bit/16-bit	8-bit/16-bit	8-bit/16-bit
<b>Crypto coprocessor</b>	–	1,100-bit arithmetic	1,100-bit arithmetic	1,100-bit arithmetic	1,100-bit arithmetic	1,100-bit arithmetic	1,100-bit arithmetic
<b>Hardware triple DES</b>	Yes	Yes	Yes	Yes	Yes	Yes	Yes
<b>Clock (int.)</b>	1 – 30 MHz	1 – 30 MHz	1 – 30 MHz	1 – 30 MHz	1 – 30 MHz	1 – 30 MHz	1 – 30 MHz
<b>Clock (ext.)</b>	1 – 7.5 MHz	1 – 7.5 MHz	1 – 7.5 MHz	1 – 7.5 MHz	1 – 7.5 MHz	1 – 7.5 MHz	1 – 7.5 MHz
<b>Operating voltage</b>	1.62 V – 5.5 V	1.62 V – 5.5 V	1.62 V – 5.5 V	1.62 V – 5.5 V	1.62 V – 5.5 V	1.62 V – 5.5 V	1.62 V – 5.5 V
<b>Max. sleep mode current (typ.)</b>	100 µA	100 µA	100 µA	100 µA	100 µA	100 µA	100 µA
<b>Ambient temperature</b>	-25 to +70°	-25 to +70°	-25 to +70°	-25 to +70°	-25 to +70°	-25 to +70°	-25 to +70°
<b>EEPROM Programming Time @ contactless operation</b>	< 2.3 ms (typ.)	< 2.3 ms (typ.)	< 2.3 ms (typ.)	< 2.3 ms (typ.)	< 2.3 ms (typ.)	< 2.3 ms (typ.)	< 2.3 ms (typ.)
<b>EEPROM page programming</b>	1 to 64 Byte	1 to 64 Byte	1 to 64 Byte	1 to 64 Byte	1 to 64 Byte	1 to 64 Byte	1 to 64 Byte
<b>MMU</b>	Yes	Yes	Yes	Yes	Yes	Yes	Yes
<b>Security features</b>	Tamper-proof design, chip ID, countermeasures against reverse engineering, SPA/DPA, DFA/EMA, memory encryption, sensor concept: voltage-, frequency-, light-, temperature-, glitch sensor, active shield, triple DES in HW	Tamper-proof design, chip ID, countermeasures against reverse engineering, SPA/DPA, DFA/EMA, memory encryption, sensor concept: voltage-, frequency-, light-, temperature-, glitch sensor, active shield, triple DES in HW, asymmetric algorithms, hardware-supported (e.g. RSA, ECC)	Tamper-proof design, chip ID, countermeasures against reverse engineering, SPA/DPA, DFA/EMA, memory encryption, sensor concept: voltage-, frequency-, light-, temperature-, glitch sensor, active shield, triple DES in HW, asymmetric algorithms, hardware-supported (e.g. RSA, ECC)	Tamper-proof design, chip ID, countermeasures against reverse engineering, SPA/DPA, DFA/EMA, memory encryption, sensor concept: voltage-, frequency-, light-, temperature-, glitch sensor, active shield, triple DES in HW, asymmetric algorithms, hardware-supported (e.g. RSA, ECC)	Tamper-proof design, chip ID, countermeasures against reverse engineering, SPA/DPA, DFA/EMA, memory encryption, sensor concept: voltage-, frequency-, light-, temperature-, glitch sensor, active shield, triple DES in HW, asymmetric algorithms, hardware-supported (e.g. RSA, ECC)	Tamper-proof design, chip ID, countermeasures against reverse engineering, SPA/DPA, DFA/EMA, memory encryption, sensor concept: voltage-, frequency-, light-, temperature-, glitch sensor, active shield, triple DES in HW, asymmetric algorithms, hardware-supported (e.g. RSA, ECC)	Tamper-proof design, chip ID, countermeasures against reverse engineering, SPA/DPA, DFA/EMA, memory encryption, sensor concept: voltage-, frequency-, light-, temperature-, glitch sensor, active shield, triple DES in HW, asymmetric algorithms, hardware-supported (e.g. RSA, ECC)
<b>Peripherals</b>	2 x 16-bit autoreload timers, PLL, interrupt, CRC, UART, RNG, DES	2 x 16-bit autoreload timers, PLL, interrupt, CRC, UART, RNG, DES, ACE	2 x 16-bit autoreload timers, PLL, interrupt, CRC, UART, RNG, DES, ACE	2 x 16-bit autoreload timers, PLL, interrupt, CRC, UART, RNG, DES, ACE	2 x 16-bit autoreload timers, PLL, interrupt, CRC, UART, RNG, DES, ACE	2 x 16-bit autoreload timers, PLL, interrupt, CRC, UART, RNG, DES, ACE	2 x 16-bit autoreload timers, PLL, interrupt, CRC, UART, RNG, DES, ACE
<b>Delivery forms</b>	Module M8.4, contactless module MCC8, die, bumped wafer	Module M8.4, contactless module MCC8, die, bumped wafer	Module M8.4, contactless module MCC8, die, bumped wafer	Module M8.4, contactless module MCC8, die, bumped wafer	Module M8.4, contactless module MCC8, die, bumped wafer	Module M8.4, contactless module MCC8, die, bumped wafer	Module M8.4, contactless module MCC8, die, bumped wafer
<b>Typical applications</b>	Payment, EMV SDA, ePurse, Loyalty, Access, Driver Licence, Transport	Payment, EMV DDA, ePurse, Loyalty, Access, Digital Signature, Open Platform, Transport	Payment, EMV DDA, ePurse, Loyalty, Access, Digital Signature, Open Platform, Transport	Payment, EMV DDA, ePurse, Loyalty, Access, Digital Signature, ePassport, Open Platform, Transport, Dual SIM	Payment, EMV DDA, ePurse, Loyalty, Access, Digital Signature, ePassport, Open Platform, Transport	Payment, EMV DDA, ePurse, Loyalty, Access, Digital Signature, ePassport, Open Platform, Transport	Payment, EMV DDA, ePurse, Loyalty, Access, Digital Signature, ePassport, Open Platform, Transport
<b>Tools</b>	EKP (Evaluation Kit Proximity) ROK (Reader Optimization Kit)	EKP (Evaluation Kit Proximity) ROK (Reader Optimization Kit)	EKP (Evaluation Kit Proximity) ROK (Reader Optimization Kit)	EKP (Evaluation Kit Proximity) ROK (Reader Optimization Kit)	EKP (Evaluation Kit Proximity) ROK (Reader Optimization Kit)	EKP (Evaluation Kit Proximity) ROK (Reader Optimization Kit)	EKP (Evaluation Kit Proximity) ROK (Reader Optimization Kit)
<b>Certifications</b>	CC EAL5+ high (PP0002), VISA level 3, CAST	CC EAL5+ high (PP0002), VISA level 3, CAST, VISA® Wave, Mastercard PayPass® M/chip	CC EAL5+ high (PP0002), VISA level 3, CAST, VISA® Wave, Mastercard PayPass® M/chip	CC EAL5+ high (PP0002), VISA level 3, CAST, VISA® Wave, Mastercard PayPass® M/chip	CC EAL5+ high (PP0002), VISA level 3, CAST, VISA® Wave, Mastercard PayPass® M/chip	CC EAL5+ high (PP0002), VISA level 3, CAST, VISA® Wave, Mastercard PayPass® M/chip	CC EAL5+ high (PP0002), VISA level 3, CAST, VISA® Wave, Mastercard PayPass® M/chip

<sup>1)</sup> If Mifare® emulation is used

## Components for contactless terminals

## Contact-based security memories

	SLF 9xxx
<b>Product name</b>	SLF 9611
<b>Product description</b>	Security access module for SLE 55RXX/SRF 55VXX, Eurochip
<b>Interface</b>	ISO/IEC 7816
<b>Memory organization</b>	Enables high-security authentication between the terminal and the my-d® chip card and handless cards communication with the background system. Furthermore it offers the capability to manage the security mechanism with the background system.
<b>Operating frequency</b>	–
<b>Security features</b>	Evaluation according to ITSEC E3, based on SLE 66CxxxP security controller, my-d® 64-bit cryptographic algorithm, triple DES in HW for key diversification
<b>Data rate</b>	115 kbit/s
<b>Anticollision</b>	–
<b>Ambient temperature</b>	-25 to +75°
<b>Delivery forms</b>	ID-000/ID1
<b>Typical applications</b>	Security applications with key-based authentication, Prepaid Telecom, Security Access, Electronic Ticketing

Product name	SLE 4406SP Classic	SLE 6636 Eurochip 66	SLE 5532 DataCarrier	SLE 5542 DataCarrier	SLE 5552 DataCarrier	SLE 5518 DataCarrier <sup>new</sup>	SLE 5528 DataCarrier <sup>new</sup>	SLE 5538 DataCarrier <sup>new</sup>
<b>Product description</b>	Intelligent 128-bit EEPROM counter with security logic	Intelligent 237-bit EEPROM counter with security logic and high-security authentication	Intelligent 256-Byte EEPROM with Write Protection Function	Intelligent 256-Byte EEPROM with Write Protection Function and Programmable Security Code	Intelligent 256-Byte EEPROM with Write and Read-Out Protection Function and Programmable Security Code	Intelligent 1024-Byte EEPROM with Write Protection Function	Intelligent 1024-Byte EEPROM with Write Protection Function and Programmable Security Code	Intelligent 1024-Byte EEPROM with Write and Read-Out Protection Function and Programmable Security Code
<b>Counter</b>	> 20,000 count units	> 20,000 count units, support of anti-tearing	–	–	–	–	–	–
<b>ROM</b>	24-bit	24-bit	–	–	–	–	–	–
<b>PROM</b>	72-bit	177-bit	32-bit	32-bit	32-bit	1024-bit	1024-bit	1024-bit
<b>EEPROM</b>	32-bit	36-bit	256 Byte	256 Byte	256 Byte	1024 Byte	1024 Byte	1024 Byte
<b>Security features</b>	Security logic, irreversible chip coding, transport code, advanced CMOS security technology	High security authentication with 1 or 2 keys, optional cipher block chaining, security logic, irreversible chip coding, transport code, dedicated advanced CMOS security technology	EEPROM-cells protected by shield, shielding of deeper layers via metal, sensory- and logical security functions, Byte protection, irreversible chip coding, advanced CMOS security technology	EEPROM-cells protected by shield, shielding of deeper layers via metal, sensory- and logical security functions, Programmable Security Code, Byte protection, irreversible chip coding, advanced CMOS security technology	EEPROM-cells protected by shield, shielding of deeper layers via metal, sensory- and logical security functions, Programmable Security Code, Byte protection, irreversible chip coding, advanced CMOS security technology	EEPROM-cells protected by shield, shielding of deeper layers via metal, sensory- and logical security functions, Byte protection, irreversible chip coding, advanced CMOS security technology	EEPROM-cells protected by shield, shielding of deeper layers via metal, sensory- and logical security functions, Programmable Security Code, Byte protection, irreversible chip coding, advanced CMOS security technology	EEPROM-cells protected by shield, shielding of deeper layers via metal, sensory- and logical security functions, Programmable Security Code, Byte protection, irreversible chip coding, advanced CMOS security technology
<b>Min. write/erase time</b>	3 ms / 3 ms	3 ms / 3 ms	2.5 ms / 2.5 ms	2.5 ms / 2.5 ms	2.5 ms / 2.5 ms	5 ms / 5 ms	5 ms / 5 ms	5 ms / 5 ms
<b>Operating voltage</b>	5 V	5 V	5 V	5 V	5 V	5 V	5 V	5 V
<b>Max. supply current</b>	1 mA	1 mA (typ. 400 µA)	3 mA	3 mA	3 mA	1 mA	1 mA	1 mA
<b>Ambient temperature</b>	-40 to +80°	-40 to +80°	-40 to +80°	-40 to +80°	-40 to +80°	-40 to +100°	-40 to +100°	-40 to +100°
<b>Endurance</b>	100,000	100,000	100,000	100,000	100,000	100,000	100,000	100,000
<b>Retention time, minimum</b>	30 years	30 years	10 years	10 years	10 years	10 years	10 years	10 years
<b>Delivery forms</b>	Module M3, MFC 3.1 (FCOS®), die	Module M3, MFC 3.1 (FCOS®), die	Module M3, MFC 3.1 (FCOS®), die	Module M3, MFC 3.1 (FCOS®), die	Module M3, MFC 3.1 (FCOS®), die	Module M3, MFC 3.1 (FCOS®), die	Module M3, MFC 3.1 (FCOS®), die	Module M3, MFC 3.1 (FCOS®), die
<b>Tools</b>	EVA-kit	EVA-kit	EVA-kit	EVA-kit	EVA-kit	EVA-kit	EVA-kit	EVA-kit
<b>Typical applications</b>	Prepaid Phone Card, Vending	Prepaid Phone Card, Vending	Healthcare and Health Insurance Card, Member Card, Electronic Ticketing, Loyalty Card, Access Control	Healthcare and Health Insurance Card, Member Card, Electronic Ticketing, Loyalty Card, Access Control	Healthcare and Health Insurance Card, Member Card, Electronic Ticketing, Loyalty Card, Access Control	Healthcare and Health Insurance Card, Member Card, Electronic Ticketing, Loyalty Card, Access Control	Healthcare and Health Insurance Card, Member Card, Electronic Ticketing, Loyalty Card, Access Control	Healthcare and Health Insurance Card, Member Card, Electronic Ticketing, Loyalty Card, Access Control

## Security controller overview by EEPROM sizes

EEPROM	2 KB	4 KB	8 KB	16 KB	16 KB	16 KB	16 KB
<b>Product name</b>	<b>SLE 66C24PE</b> Secure µSlim EEPROM	<b>SLE 66C44PE</b> Secure µSlim EEPROM	<b>SLE 66C84PE</b> Secure µSlim EEPROM	<b>SLE 66CX80PE</b> Secure µSlim EEPROM	<b>SLE 66C161PE</b> Secure µSlim EEPROM	<b>SLE 66C166PE</b> Secure µSlim EEPROM	<b>SLE 66C168PE</b> Secure µSlim EEPROM
<b>Product description</b>	Security controller	Security controller	Security controller	Security controller	Security controller	Security controller	Security controller
<b>User-ROM</b>	68 kByte	68 kByte	68 kByte	96 kByte	48 kByte	96 kByte	68 kByte
<b>EEPROM</b>	2 kByte	4 kByte	8 kByte	8 kByte	16 kByte	16 kByte	16 kByte
<b>RAM</b>	2,304 Byte	2,304 Byte	2,304 Byte	4,352 Byte + 700 Byte crypto	2,304 Byte	2,304 Byte	2,304 Byte
<b>CPU</b>	8-bit/16-bit	8-bit/16-bit	8-bit/16-bit	8-bit/16-bit	8-bit/16-bit	8-bit/16-bit	8-bit/16-bit
<b>Crypto coprocessor</b>	–	–	–	1,100-bit arithmetic	–	–	–
<b>Hardware triple DES</b>	Yes	Yes	Yes	Yes	No	Yes	Yes
<b>Clock (int.)</b>	1 – 33 MHz	1 – 33 MHz	1 – 33 MHz	1 – 33 MHz	1 – 33 MHz	1 – 33 MHz	1 – 33 MHz
<b>Clock (ext.)</b>	1 – 7.5 MHz	1 – 7.5 MHz	1 – 7.5 MHz	1 – 7.5 MHz	1 – 7.5 MHz	1 – 7.5 MHz	1 – 7.5 MHz
<b>Operating voltage</b>	1.62 V – 5.5 V	1.62 V – 5.5 V	1.62 V – 5.5 V	1.62 V – 5.5 V	1.62 V – 5.5 V	1.62 V – 5.5 V	1.62 V – 5.5 V
<b>Max. supply current (at 5 MHz, 5 V)</b>	10 mA	10 mA	10 mA	10 mA	10 mA	10 mA	10 mA
<b>Max. sleep mode current (typical)</b>	100 µA	100 µA	100 µA	100 µA	100 µA	100 µA	100 µA
<b>Ambient temperature</b>	-25 to +85°	-25 to +85°	-25 to +85°	-25 to +85°	-25 to +85°	-25 to +85°	-25 to +85°
<b>Write/erase time</b>	2 ms (typ.)	2 ms (typ.)	2 ms (typ.)	2 ms (typ.)	2 ms (typ.)	2 ms (typ.)	2 ms (typ.)
<b>EEPROM page programming</b>	1 to 64 Byte	1 to 64 Byte	1 to 64 Byte	1 to 64 Byte	1 to 64 Byte	1 to 64 Byte	1 to 64 Byte
<b>MMU</b>	Yes	Yes	Yes	Yes	Yes	Yes	Yes
<b>Security features</b>	Tamper-proof design, chip ID, countermeasures against SEMA/DEMA, SPA/DPA, DFA and timing attacks, sensor concept: low- and high-voltage sensors, frequency sensors and filters, light-, glitch-, temperature sensors, life test function for sensors, symmetric algorithms (e.g. DES/AES), triple DES in HW, elliptic curves in SW, bus encryption, active shield	Tamper-proof design, chip ID, countermeasures against SEMA/DEMA, SPA/DPA, DFA and timing attacks, sensor concept: low- and high-voltage sensors, frequency sensors and filters, light-, glitch-, temperature sensors, life test function for sensors, symmetric algorithms (e.g. DES/AES), triple DES in HW, elliptic curves in SW, bus encryption, active shield	Tamper-proof design, chip ID, countermeasures against SEMA/DEMA, SPA/DPA, DFA and timing attacks, sensor concept: low- and high-voltage sensors, frequency sensors and filters, light-, glitch-, temperature sensors, life test function for sensors, symmetric algorithms (e.g. DES/AES), triple DES in HW, elliptic curves in SW, bus encryption, active shield	Tamper-proof design, chip ID, countermeasures against SEMA/DEMA, SPA/DPA, DFA and timing attacks, sensor concept: low- and high-voltage sensors, frequency sensors and filters, light-, glitch-, temperature sensors, life test function for sensors, symmetric algorithms (e.g. DES/AES), triple DES in HW, RSA, elliptic curves in HW, active shield, bus encryption	Tamper-proof design, chip ID, countermeasures against SEMA/DEMA, SPA/DPA, DFA and timing attacks, sensor concept: low- and high-voltage sensors, frequency sensors and filters, light-, glitch-, temperature sensors, life test function for sensors, DES in software, bus encryption	Tamper-proof design, chip ID, countermeasures against SEMA/DEMA, SPA/DPA, DFA and timing attacks, sensor concept: low- and high-voltage sensors, frequency sensors and filters, light-, glitch-, temperature sensors, life test function for sensors, symmetric algorithms (e.g. DES/AES), triple DES in HW, elliptic curves in SW, bus encryption, active shield	Tamper-proof design, chip ID, countermeasures against SEMA/DEMA, SPA/DPA, DFA and timing attacks, sensor concept: low- and high-voltage sensors, frequency sensors and filters, light-, glitch-, temperature sensors, life test function for sensors, symmetric algorithms (e.g. DES/AES), triple DES in HW, elliptic curves in SW, bus encryption, active shield
<b>Peripherals</b>	CRC, UART, RNG, 2 x 16-bit autoreload timers, Interrupt, DES, PLL	CRC, UART, RNG, 2 x 16-bit autoreload timers, Interrupt, DES, PLL	CRC, UART, RNG, 2 x 16-bit autoreload timers, Interrupt, DES, PLL	CRC, UART, RNG, 2 x 16-bit autoreload timers, Interrupt, ACE, DES, PLL	CRC, UART, RNG, 2 x 16-bit autoreload timers, Interrupt, PLL	CRC, UART, RNG, 2 x 16-bit autoreload timers, Interrupt, DES, PLL	CRC, UART, RNG, 2 x 16-bit autoreload timers, Interrupt, DES, PLL
<b>Delivery forms</b>	Module M5, MFC5-x, DSO-8, VQFN-8, die	Module M5, MFC5-x, DSO-8, VQFN-8, die	Module M5, MFC5-x, DSO-8, VQFN-8, die	Module M5, MFC5-x, DSO-8, VQFN-8, die	Module M4.8, M5.1, MFC5-x, DSO-8, VQFN-8, die	Module M5, MFC5-x, DSO-8, VQFN-8, die	Module M5, MFC5-x, DSO-8, VQFN-8, die
<b>Typical applications</b>	Payment, EMV SDA, ePurse, Loyalty, Access, Driver Licence	Payment, EMV SDA, ePurse, Loyalty, Access, Driver Licence	Payment, EMV SDA, ePurse, Loyalty, Access, Driver Licence	Payment, EMV DDA, ePurse, Loyalty, Access, Pay-TV	16k SIM, Native GSM	Payment, EMV SDA, ePurse, Loyalty, Access, Health/Social Security	Payment, EMV SDA, ePurse, Loyalty, Access, Health/Social Security, Pay-TV
<b>Certifications</b>	CC EAL5+ high (PP0002), VISA, CAST	CC EAL5+ high (PP0002), VISA, CAST	CC EAL5+ high (PP0002), VISA, CAST	CC EAL5+ high (PP0002), VISA, CAST	–	CC EAL5+ high (PP0002), VISA, CAST	CC EAL5+ high (PP0002), VISA, CAST

## Security controller overview by EEPROM sizes

EEPROM	16 KB	32 KB	32 KB	32 KB	32 KB	32 KB	32 KB
<b>Product name</b>	SLE 66CX162PE Secure µSlim EEPROM	SLE 50C363PE Secure µSlim EEPROM	SLE 66C324PE Secure µSlim EEPROM	SLE 66C327PE Secure µSlim EEPROM	SLE 66C360PE Secure µSlim EEPROM	SLE 66C367PE Secure µSlim EEPROM	SLE 66CX360PE Secure µSlim EEPROM
<b>Product description</b>	Security cryptocontroller	Security controller optimized for mobile communication applications	Security controller	Security controller	Security controller	Security controller	Security cryptocontroller
<b>User-ROM</b>	96 kByte	96 kByte	136 kByte	136 kByte	196 kByte	196 kByte	196 kByte
<b>EEPROM</b>	16 kByte	36 kByte	32 kByte	32 kByte	36 kByte	36 kByte	36 kByte
<b>RAM</b>	4,352 Byte + 700 Byte crypto	4,352 Byte	4,352 Byte	4,352 Byte	4,352 Byte	4,352 Byte	6,400 Byte + 700 Byte crypto
<b>CPU</b>	8-bit/16-bit	8-bit/16-bit	8-bit/16-bit	8-bit/16-bit	8-bit/16-bit	8-bit/16-bit	8-bit/16-bit
<b>Crypto coprocessor</b>	1,100-bit arithmetic	–	–	–	–	–	1,100-bit arithmetic
<b>Hardware triple DES</b>	Yes	No	Yes	Yes	Yes	Yes	Yes
<b>Clock (int.)</b>	1 – 33 MHz	1 – 33 MHz	1 – 33 MHz	1 – 33 MHz	1 – 33 MHz	1 – 33 MHz	1 – 33 MHz
<b>Clock (ext.)</b>	1 – 75 MHz	1 – 75 MHz	1 – 75 MHz	1 – 75 MHz	1 – 75 MHz	1 – 75 MHz	1 – 75 MHz
<b>Operating voltage</b>	1.62 V – 5.5 V	1.62 V – 5.5 V	1.62 V – 5.5 V	2.7 V – 5.5 V	1.62 V – 5.5 V	2.7 V – 5.5 V	1.62 V – 5.5 V
<b>Max. supply current (at 5 MHz, 5 V)</b>	10 mA	10 mA	10 mA	10 mA	10 mA	10 mA	10 mA
<b>Max. sleep mode current (typical)</b>	100 µA	100 µA	100 µA	100 µA	100 µA	100 µA	100 µA
<b>Ambient temperature</b>	-25 to +85°	-25 to +85°	-25 to +85°	-25 to +85°	-25 to +85°	-25 to +85°	-25 to +85°
<b>Write/erase time</b>	2 ms (typ.)	2 ms (typ.)	2 ms (typ.)	2 ms (typ.)	2 ms (typ.)	2 ms (typ.)	2 ms (typ.)
<b>EEPROM page programming</b>	1 to 64 Byte	1 to 64 Byte	1 to 64 Byte	1 to 64 Byte	1 to 64 Byte	1 to 64 Byte	1 to 64 Byte
<b>MMU</b>	Yes	Yes	Yes	Yes	Yes	Yes	Yes
<b>Security features</b>	Tamper-proof design, chip ID, countermeasures against SEMA/DEMA, SPA/DPA, DFA and timing attacks, sensor concept: low- and high-voltage sensors, frequency sensors and filters, light-, glitch-, temperature sensors, life test function for sensors, bus encryption, symmetric algorithms (e.g. DES/AES), triple DES in HW, RSA, elliptic curves in HW, active shield	Tamper-proof design, chip ID, basic countermeasures against SEMA/DEMA, SPA/DPA, DFA and timing attacks, exception sensors, life test function for sensors, life test for sensors, bus confusion, true random number generator, DES in software	Tamper-proof design, chip ID, countermeasures against SEMA/DEMA, SPA/DPA, DFA and timing attacks, sensor concept: low- and high-voltage sensors, frequency sensors and filters, light-, glitch-, temperature sensors, life test function for sensors, symmetric algorithms (e.g. DES/AES), triple DES in HW, elliptic curves in SW, bus encryption, active shield	Tamper-proof design, chip ID, countermeasures against SEMA/DEMA, SPA/DPA, DFA and timing attacks, sensor concept: low- and high-voltage sensors, frequency sensors and filters, light-, glitch-, temperature sensors, life test function for sensors, symmetric algorithms (e.g. DES/AES), triple DES in HW, elliptic curves in SW, bus encryption, active shield	Tamper-proof design, chip ID, countermeasures against SEMA/DEMA, SPA/DPA, DFA and timing attacks, sensor concept: low- and high-voltage sensors, frequency sensors and filters, light-, glitch-, temperature sensors, life test function for sensors, symmetric algorithms (e.g. DES/AES), triple DES in HW, elliptic curves in SW, bus encryption, active shield	Tamper-proof design, chip ID, countermeasures against SEMA/DEMA, SPA/DPA, DFA and timing attacks, sensor concept: low- and high-voltage sensors, frequency sensors and filters, light-, glitch-, temperature sensors, life test function for sensors, symmetric algorithms (e.g. DES/AES), triple DES in HW, elliptic curves in SW, bus encryption, active shield	Tamper-proof design, chip ID, countermeasures against SEMA/DEMA, SPA/DPA, DFA and timing attacks, sensor concept: low- and high-voltage sensors, frequency sensors and filters, light-, glitch-, temperature sensors, life test function for sensors, symmetric algorithms (e.g. DES/AES), triple DES in HW, elliptic curves in HW, active shield, bus encryption
<b>Peripherals</b>	CRC, UART, RNG, 2 x 16-bit autoreload timers, interrupt, ACE, DES, PLL	CRC, UART, RNG, 2 x 16-bit autoreload timers, interrupt, PLL	CRC, UART, RNG, 2 x 16-bit autoreload timers, interrupt, DES, PLL	CRC, UART, RNG, 2 x 16-bit autoreload timers, interrupt, DES, PLL	CRC, UART, RNG, 2 x 16-bit autoreload timers, interrupt, DES, PLL	CRC, UART, RNG, 2 x 16-bit autoreload timers, interrupt, DES, PLL	CRC, UART, RNG, 2 x 16-bit autoreload timers, interrupt, ACE, DES, PLL
<b>Delivery forms</b>	Module M5, MFC5-x, DSO-8, VQFN-8, die	Module M4.8, M5.1, MFC5-x, VQFN-8, die	Module M4.8, M5.1, MFC5-x, VQFN-8, die	Module M5, MFC5-x, DSO-8, VQFN-8, die	Module M4.8, M5.1, MFC5-x, VQFN-8, die	Module M4.8, M5, MFC5-x, VQFN-8, die	Module M5, MFC5-x, DSO-8, VQFN-8, die
<b>Typical applications</b>	Payment, EMV DDA, ePurse, Loyalty, Access, Health/Social Security, Digital Signature, Pay-TV, Open Platform	32k SIM, Native GSM, R-UIM	32k SIM, Native GSM, R-UIM	Payment, EMV SDA, ePurse, Loyalty, Access, Open Platform	32k SIM, UICC, Java, R-UIM	Payment, EMV SDA, ePurse, Loyalty, Access, Open Platform, Pay TV	Payment, EMV DDA, ePurse, Loyalty, Access, Health/Social Security, Digital Signature, ID-Card, Pay-TV, Open Platform, GSM, UICC
<b>Certifications</b>	CC EAL5+ high (PP0002), VISA, CAST	–	–	VISA, CAST	–	VISA, CAST	CC EAL5+ high (PP0002), VISA, CAST, ZKA

## Security controller overview by EEPROM sizes

EEPROM	32 KB	64 KB	new	64 KB	64 KB	64 KB	≥ 64 KB
<b>Product name</b>	SLE 66CX482PE Secure µSlim EEPROM	SLE 66CX480PE Secure µSlim EEPROM	SLE 76CF2560P Secure µSlim Flash/EEPROM	SLE 50C683PE Secure µSlim EEPROM	SLE 66C680PE Secure µSlim EEPROM	SLE 66C682PE Secure µSlim EEPROM	SLE 66C680PE Secure µSlim EEPROM
<b>Product description</b>	Security cryptocontroller	Security cryptocontroller	Security controller	Security controller optimized for mobile communication applications	Security controller	Security controller	Security cryptocontroller
<b>User-ROM</b>	196 kByte	244 kByte	–	136 kByte	244 kByte	196 kByte	244 kByte
<b>EEPROM</b>	48 kByte	48 kByte	256 kByte	68 kByte	68 kByte	68 kByte	68 kByte
<b>RAM</b>	6,400 Byte + 700 Byte crypto	6,400 Byte + 700 Byte crypto	8 kByte	4,352 Byte	6,400 Byte	4,352 Byte	6,400 Byte + 700 Byte crypto
<b>CPU</b>	8-bit/16-bit	8-bit/16-bit	16-bit	8-bit/16-bit	8-bit/16-bit	8-bit/16-bit	8-bit/16-bit
<b>Crypto coprocessor</b>	1,100-bit arithmetic	1,100-bit arithmetic	–	–	–	–	1,100-bit arithmetic
<b>Hardware triple DES</b>	Yes	Yes	Yes	Yes	Yes	Yes	Yes
<b>Clock (int.)</b>	1 – 33 MHz	1 – 33 MHz	1 – 33 MHz	2 – 33 MHz	1 – 33 MHz	1 – 33 MHz	1 – 33 MHz
<b>Clock (ext.)</b>	1 – 75 MHz	1 – 75 MHz	1 – 10 MHz	2 – 75 MHz	1 – 75 MHz	1 – 75 MHz	1 – 75 MHz
<b>Operating voltage</b>	1.62 V – 5.5 V	1.62 V – 5.5 V	1.62 V – 5.5 V	1.62 V – 5.5 V	1.62 V – 5.5 V	1.62 V – 5.5 V	1.62 V – 5.5 V
<b>Max. supply current (at 5 MHz, 5 V)</b>	10 mA	10 mA	10 mA	10 mA	10 mA	10 mA	10 mA
<b>Max. sleep mode current (typical)</b>	100 µA	100 µA	100 µA	100 µA	100 µA	100 µA	100 µA
<b>Ambient temperature</b>	-25 to +85°	-25 to +85°	-25 to +85°	-25 to +85°	-25 to +85°	-25 to +85°	-25 to +85°
<b>Write/erase time</b>	2 ms (typ.)	2 ms (typ.)	< 2.3 ms	3 ms (typ.)	2 ms (typ.)	2 ms (typ.)	2 ms (typ.)
<b>EEPROM page programming</b>	1 to 64 Byte	1 to 64 Byte	1 to 128 Byte	1 to 64 Byte	1 to 64 Byte	1 to 64 Byte	1 to 64 Byte
<b>MMU</b>	Yes	Yes	Yes	Yes	Yes	Yes	Yes
<b>Security features</b>	Tamper-proof design, chip ID, countermeasures against SEMA/DEMA, SPA/DPA, DFA and timing attacks, sensor concept: low- and high-voltage sensors, frequency sensors and filters, light-, glitch-, temperature sensors, life test function for sensors, symmetric algorithms (e.g. DES/AES), triple DES in HW, RSA, elliptic curves in HW, active shield, bus encryption	Tamper-proof design, chip ID, countermeasures against SEMA/DEMA, SPA/DPA, DFA and timing attacks, sensor concept: low- and high-voltage sensors, frequency sensors and filters, light-, glitch-, temperature sensors, life test function for sensors, symmetric algorithms (e.g. DES/AES), triple DES in HW, RSA, elliptic curves in HW, active shield, bus encryption	Tamper-proof design, chip ID, basic countermeasures against SEMA/DEMA, SPA/DPA, DFA and timing attacks, exception sensors, life test function for sensors, bus confusion, pseudo random number generator, watchdog timer, memory encryption device, DES/AES in software and hardware	Tamper-proof design, chip ID, basic countermeasures against SEMA/DEMA, SPA/DPA, DFA and timing attacks, exception sensors, life test function for sensors, bus confusion, true random number generator, DES in software and hardware	Tamper-proof design, chip ID, countermeasures against SEMA/DEMA, SPA/DPA, DFA and timing attacks, sensor concept: low- and high-voltage sensors, frequency sensors and filters, light-, glitch-, temperature sensors, life test function for sensors, symmetric algorithms (e.g. DES/AES), triple DES in HW, elliptic curves in SW, bus encryption, active shield	Tamper-proof design, chip ID, countermeasures against SEMA/DEMA, SPA/DPA, DFA and timing attacks, sensor concept: low- and high-voltage sensors, frequency sensors and filters, light-, glitch-, temperature sensors, life test function for sensors, symmetric algorithms (e.g. DES/AES), triple DES in HW, elliptic curves in SW, bus encryption, active shield	Tamper-proof design, chip ID, countermeasures against SEMA/DEMA, SPA/DPA, DFA and timing attacks, sensor concept: low- and high-voltage sensors, frequency sensors and filters, light-, glitch-, temperature sensors, life test function for sensors, bus encryption, symmetric algorithms (e.g. DES/AES), triple DES in HW, RSA, elliptic curves in HW, active shield
<b>Peripherals</b>	CRC, UART, RNG, 2 x 16-bit autoreload timers, interrupt, ACE, DES, PLL	CRC, UART, RNG, 2 x 16-bit autoreload timers, interrupt, ACE, DES, PLL	CRC, UART, RNG, 2 x 16-bit autoreload timers, interrupt, PEC, DES, PLL	CRC, UART, RNG, 2 x 16-bit autoreload timers, interrupt, PLL	CRC, UART, RNG, 2 x 16-bit autoreload timers, interrupt, DES, PLL	CRC, UART, RNG, 2 x 16-bit autoreload timers, interrupt, DES, PLL	CRC, UART, RNG, 2 x 16-bit autoreload timers, interrupt, ACE, DES, PLL
<b>Delivery forms</b>	Module M5, MFC5-x, DSO-8, VQFN-8, die	Module M5, MFC5-x, DSO-8, VQFN-8, die	Module M4.8, M5.1, MFC5-x, VQFN-8, die	Module M4.8, M5.1, MFC5-x, VQFN-8, die	Module M5, MFC5-x, VQFN-8, die	Module M4.8, M5.1, MFC5-x, VQFN-8, die	Module M5, MFC5-x, DSO-8, VQFN-8, die
<b>Typical applications</b>	Payment, EMV DDA, ePurse, Loyalty, Access, Health/Social Security, Digital Signature, ID-Card, Pay-TV, Open Platform, GSM, UICC	Payment, EMV DDA, ePurse, Loyalty, Access, Health/Social Security, Digital Signature, ID-Card, Pay-TV, Open Platform, GSM, UICC	64k SIM, UICC, Native, Java GSM, R-UIM	64k SIM, Native, Java, R-UIM	64k SIM, UICC, GSM, R-UIM, Java, Pay-TV	64k SIM, UICC, Native, Java GSM, R-UIM	Payment, EMV DDA, ePurse, Loyalty, Access, Health/Social Security, Digital Signature, ID-Card, Pay-TV, Open Platform, GSM, UICC
<b>Certifications</b>	CC EAL5+ high (PP0002), VISA, CAST, ZKA	CC EAL5+ high (PP0002), VISA, CAST, ZKA	–	–	–	–	CC EAL5+ high (PP0002), VISA, CAST, ZKA

## Security controller overview by EEPROM sizes

EEPROM	≥ 64 KB						
<b>Product name</b>	<b>SLE 50C1320PE</b> Secure $\mu$ Slim Flash/EEPROM	<b>SLE 76CF3200P</b> Secure $\mu$ Slim Flash/EEPROM <span style="float: right; font-size: small;">new</span>	<b>SLE 76CF3600P</b> Secure $\mu$ Slim Flash/EEPROM <span style="float: right; font-size: small;">new</span>	<b>SLE 88C920P</b> Secure $\mu$ Slim EEPROM	<b>SLE 88CF2920P</b> Secure $\mu$ Slim Flash/EEPROM	<b>SLE 88CFX2920P</b> Secure $\mu$ Slim Flash/EEPROM	<b>SLE 88CFX2921P</b> Secure $\mu$ Slim Flash/EEPROM
<b>Product description</b>	Flexible Security controller optimized for mobile communication applications. Optimal for flexible 64 K to 128 K applications.	Security controller	Security controller	Security controller optimized for mobile communication applications	Security controller	Security cryptocontroller	Security cryptocontroller designed for high-security applications
<b>User-ROM</b>	136 kByte	–	–	Up to 328 kByte	–	–	–
<b>EEPROM</b>	132 kByte	320 kByte	360 kByte	92 kByte	292 kByte	292 kByte	292 kByte
<b>RAM</b>	4,352 Byte	8 kByte	8 kByte	12 kByte	16 kByte	16 kByte + 880 Byte crypto	16 kByte + 880 Byte crypto
<b>CPU</b>	8-bit/16-bit	16-bit	16-bit	32-bit RISC	32-bit RISC	32-bit RISC	32-bit RISC
<b>Crypto coprocessor</b>	–	–	–	–	–	1,408-bit arithmetic	1,408-bit arithmetic
<b>Hardware triple DES</b>	No	Yes	Yes	Yes	Yes	Yes	Yes
<b>Clock (int.)</b>	1 – 33 MHz	1 – 33 MHz	1 – 33 MHz	Up to 33 MHz	Up to 66 MHz	Up to 66 MHz	Up to 66 MHz
<b>Clock (ext.)</b>	1 – 10 MHz	1 – 10 MHz	1 – 10 MHz	1 – 10 MHz	1 – 10 MHz	1 – 10 MHz	1 – 10 MHz
<b>Operating voltage</b>	1.62 V – 5.5 V	1.62 V – 5.5 V	1.62 V – 5.5 V	1.62 V – 5.5 V	1.62 V – 5.5 V	1.62 V – 5.5 V	1.62 V – 5.5 V
<b>Max. supply current (at 5 MHz, 5 V)</b>	10 mA	10 mA	10 mA	10 mA	10 mA	10 mA	10 mA
<b>Max. sleep mode current (typical)</b>	100 $\mu$ A	100 $\mu$ A	100 $\mu$ A	100 $\mu$ A	100 $\mu$ A	100 $\mu$ A	100 $\mu$ A
<b>Ambient temperature</b>	-25 to +85°	-25 to +85°	-25 to +85°	-25 to +85°	-25 to +85°	-25 to +85°	-25 to +85°
<b>Write/erase time</b>	3 ms (typ.)	< 2.3 ms	< 2.3 ms	< 2.3 ms	< 2.3 ms	< 2.3 ms	< 2.3 ms
<b>EEPROM page programming</b>	1 to 64 Byte	1 to 128 Byte	1 to 128 Byte	1 to 128 Byte	1 to 128 Byte	1 to 128 Byte	1 to 128 Byte
<b>MMU</b>	Yes	Yes	Yes	Yes	Yes	Yes	Yes
<b>Security features</b>	Tamper-proof design, chip ID, basic countermeasures against SEMA/DEMA, SPA/DPA, DFA and timing attacks, exception sensors, life test function for sensors, bus confusion, true random number generator, DES in software	Tamper-proof design, chip ID, basic countermeasures against SEMA/DEMA, SPA/DPA, DFA and timing attacks, exception sensors, life test function for sensors, bus confusion, pseudo random number generator, watchdog timer, memory encryption device, DES/AES in software and hardware	Tamper-proof design, chip ID, basic countermeasures against SEMA/DEMA, SPA/DPA, DFA and timing attacks, exception sensors, life test function for sensors, bus confusion, pseudo random number generator, watchdog timer, memory encryption device, DES/AES in software and hardware	Tamper-proof design, chip ID, countermeasures against reverse engineering, SPA/DPA, DFA/EMA, memory encryption, sensor concept: voltage-, frequency-, light-, temperature-, glitch sensor, active shield, triple DES in HW, bus encryption, dual rail logic	Tamper-proof design, chip ID, countermeasures against reverse engineering, SPA/DPA, DFA/EMA, memory encryption, sensor concept: voltage-, frequency-, light-, temperature-, glitch sensor, active shield, triple DES in HW, bus encryption, dual rail logic	Tamper-proof design, chip ID, countermeasures against reverse engineering, SPA/DPA, DFA/EMA, memory encryption, sensor concept: voltage-, frequency-, light-, temperature-, glitch sensor, active shield, triple DES in HW, elliptic curves in HW, asymmetric algorithms, hardware-supported (e.g. RSA), bus encryption, dual rail logic	Tamper-proof design, chip ID, countermeasures against reverse engineering, SPA/DPA, DFA/EMA, memory encryption, sensor concept: voltage-, frequency-, light-, temperature-, glitch sensor, active shield, triple DES in HW, elliptic curves in HW, asymmetric algorithms, hardware-supported (e.g. RSA), bus encryption, dual rail logic
<b>Peripherals</b>	CRC, UART, RNG, 2 x 16-bit autoreload timers, interrupt, PLL	CRC, UART, RNG, 2 x 16-bit autoreload timers, interrupt, PEC, DES, PLL	CRC, UART, RNG, 2 x 16-bit autoreload timers, interrupt, PEC, DES, PLL	UART, RNG, 3 x 16-bit autoreload timers, Interrupt, Trap System, DES, Power Manager for Classes A,B,C	UART, RNG, 3 x 16-bit autoreload timers, Interrupt, Trap System, DES, Crypto@1408, Power Manager for Classes A,B,C	UART, RNG, 3 x 16-bit autoreload timers, Interrupt, Trap System, DES, Crypto@1408, Power Manager for Classes A,B,C	UART, RNG, 3 x 16-bit autoreload timers, Interrupt, Trap System, DES, Crypto@1408, Power Manager for Classes A,B,C
<b>Delivery forms</b>	Module M4-8, M5-1, MFC5-x, VQFN-8, die	Module M4-8, M5-1, MFC5-x, VQFN-8, die	Module M4-8, M5-1, MFC5-x, VQFN-8, die	Module M4-8, M5-1, MFC5-x, die	Module M5, MFC5-x, DSO-20, die	Module M5, MFC5-x, DSO-20, die	Module M5, MFC5-x, DSO-20, die
<b>Typical applications</b>	64-128k SIM, R-UIM, Native, Java	64k SIM, UICC, Native, Java GSM, R-UIM	64k SIM, UICC, Native, Java GSM, R-UIM	64-72k SIM, GSM, UICC, R-UIM, Java	GSM, UICC, R-UIM, Java	GSM, UICC, Java, Digital Signature, EMV	High Secure Applications, Pay-TV, Secure Access, Digital Signature
<b>Certifications</b>	–	–	–	–	CC EAL5+ high (PP0002)	CC EAL5+ high (PP0002)	CC EAL5+ high (PP0002)

## Security controller overview by EEPROM sizes

EEPROM	≥ 64 KB			≥ 128 KB			
<b>Product name</b>	<b>SLE 88CF3520P</b> Secure μSlim Flash/EEPROM	<b>SLE 88CFX3520P</b> Secure μSlim Flash/EEPROM	<b>SLE 88CFX3521P</b> Secure μSlim Flash/EEPROM	<b>SLE 88CF4000P</b> Secure μSlim Flash/EEPROM	<b>SLE 76CF4000P</b> Secure μSlim Flash/EEPROM	<b>SLE 88CFX4000P</b> Secure μSlim Flash/EEPROM	<b>SLE 88CFX4001P</b> Secure μSlim Flash/EEPROM
<b>Product description</b>	Security controller	Security cryptocontroller	Security cryptocontroller designed for high-security applications	Security controller	Security controller	Security cryptocontroller	Security cryptocontroller designed for high-security applications
<b>User-ROM</b>	–	–	–	–	–	–	–
<b>EEPROM</b>	352 kByte	352 kByte	352 kByte	400 kByte	400 kByte	400 kByte	400 kByte
<b>RAM</b>	16 kByte	16 kByte + 880 Byte crypto	16 kByte + 880 Byte crypto	16 kByte	12kByte	16 kByte + 880 Byte crypto	16 kByte + 880 Byte crypto
<b>CPU</b>	32-bit RISC	32-bit RISC	32-bit RISC	32-bit RISC	16-bit	32-bit RISC	32-bit RISC
<b>Crypto coprocessor</b>	–	1,408-bit arithmetic	1,408-bit arithmetic	–	–	1,408-bit arithmetic	1,408-bit arithmetic
<b>Hardware triple DES</b>	Yes	Yes	Yes	Yes	Yes	Yes	Yes
<b>Clock (int.)</b>	Up to 66 MHz	Up to 66 MHz	Up to 66 MHz	Up to 66 MHz	1 – 33 MHz	Up to 66 MHz	Up to 66 MHz
<b>Clock (ext.)</b>	1 – 10 MHz	1 – 10 MHz	1 – 10 MHz	1 – 10 MHz	1 – 10 MHz	1 – 10 MHz	1 – 10 MHz
<b>Operating voltage</b>	1.62 V – 5.5 V	1.62 V – 5.5 V	1.62 V – 5.5 V	1.62 V – 5.5 V	1.62 V – 5.5 V	1.62 V – 5.5 V	1.62 V – 5.5 V
<b>Max. supply current (at 5 MHz, 5 V)</b>	10 mA	10 mA	10 mA	10 mA	10 mA	10 mA	10 mA
<b>Max. sleep mode current (typical)</b>	100 μA	100 μA	100 μA	100 μA	100 μA	100 μA	100 μA
<b>Ambient temperature</b>	-25 to +85°	-25 to +85°	-25 to +85°	-25 to +85°	-25 to +85°	-25 to +85°	-25 to +85°
<b>Write/erase time</b>	< 2.3 ms	< 2.3 ms	< 2.3 ms	< 2.3 ms	< 2.3 ms	< 2.3 ms	< 2.3 ms
<b>EEPROM page programming</b>	1 to 128 Byte	1 to 128 Byte	1 to 128 Byte	1 to 128 Byte	1 to 128 Byte	1 to 128 Byte	1 to 128 Byte
<b>MMU</b>	Yes	Yes	Yes	Yes	Yes	Yes	Yes
<b>Security features</b>	Tamper-proof design, chip ID, countermeasures against reverse engineering, SPA/DPA, DFA/EMA, memory encryption, sensor concept: voltage-, frequency-, light-, temperature-, glitch sensor, active shield, triple DES in HW, bus encryption, dual rail logic	Tamper-proof design, chip ID, countermeasures against reverse engineering, SPA/DPA, DFA/EMA, memory encryption, sensor concept: voltage-, frequency-, light-, temperature-, glitch sensor, active shield, triple DES in HW, elliptic curves in HW, asymmetric algorithms, hardware-supported (e.g. RSA), bus encryption, dual rail logic	Tamper-proof design, chip ID, countermeasures against reverse engineering, SPA/DPA, DFA/EMA, memory encryption, sensor concept: voltage-, frequency-, light-, temperature-, glitch sensor, active shield, triple DES in HW, elliptic curves in HW, asymmetric algorithms, hardware-supported (e.g. RSA), bus encryption, dual rail logic	Tamper-proof design, chip ID, countermeasures against reverse engineering, SPA/DPA, DFA/EMA, memory encryption, sensor concept: voltage-, frequency-, light-, temperature-, glitch sensor, active shield, triple DES in HW, bus encryption, dual rail logic	Tamper-proof design, chip ID, basic countermeasures against SEMA/DEMA, SPA/DPA, DFA and timing attacks, exception sensors, life test function for sensors, bus confusion, pseudo random number generator, watchdog timer, memory encryption device, DES/AES in software and hardware	Tamper-proof design, chip ID, countermeasures against reverse engineering, SPA/DPA, DFA/EMA, memory encryption, sensor concept: voltage-, frequency-, light-, temperature-, glitch sensor, active shield, triple DES in HW, elliptic curves in HW, asymmetric algorithms, hardware-supported (e.g. RSA), bus encryption, dual rail logic	Tamper-proof design, chip ID, countermeasures against reverse engineering, SPA/DPA, DFA/EMA, memory encryption, sensor concept: voltage-, frequency-, light-, temperature-, glitch sensor, active shield, triple DES in HW, elliptic curves in HW, asymmetric algorithms, hardware-supported (e.g. RSA), bus encryption, dual rail logic
<b>Peripherals</b>	UART, RNG, 3 x 16-bit autoreload timers, Interrupt, Trap System, DES, Power Manager for Classes A,B,C	UART, RNG, 3 x 16-bit autoreload timers, Interrupt, Trap System, DES, Crypto@1408, Power Manager for Classes A,B,C	UART, RNG, 3 x 16-bit autoreload timers, Interrupt, Trap System, DES, Crypto@1408, Power Manager for Classes A,B,C	UART, RNG, 3 x 16-bit autoreload timers, Interrupt, Trap System, DES, Power Manager for Classes A,B,C	CRC, UART, RNG, 2 x 16-bit autoreload timers, interrupt, PEC, DES, PLL	UART, RNG, 3 x 16-bit autoreload timers, Interrupt, Trap System, DES, Crypto@1408, Power Manager for Classes A,B,C	UART, RNG, 3 x 16-bit autoreload timers, Interrupt, Trap System, DES, Crypto@1408, Power Manager for Classes A,B,C
<b>Delivery forms</b>	Module M5, MFC5-x, DSO-20, die	Module M5, MFC5-x, DSO-20, die	Module M5, MFC5-x, DSO-20, die	Module M5, MFC5-x, DSO-20, die	Module M4,8, M5-1, MFC5-x, VQFN-8, die	Module M5, MFC5-x, DSO-20, die	Module M5, MFC5-x, DSO-20, die
<b>Typical applications</b>	GSM, UICC, R-UIM, Java	GSM, UICC, Java, Digital Signature, EMV	High Secure Applications, Pay-TV, Secure Access, Digital Signature	GSM, UICC, R-UIM, Java	64k SIM, UICC, Native, Java GSM, R-UIM	GSM, UICC, Java, Digital Signature, EMV	High Secure Applications, Pay-TV, Secure Access, Digital Signature
<b>Certifications</b>	CC EAL5+ high (PP0002)	CC EAL5+ high (PP0002)	CC EAL5+ high (PP0002)	CC EAL5+ high (PP0002)	–	CC EAL5+ high (PP0002)	CC EAL5+ high (PP0002)

## Security controller overview by EEPROM sizes

EEPROM	≥ 128 KB		≥ 256 KB			≥ 256 KB	
Product name	SLE 76CF4480P <b>new</b> Secure µSlim Flash/EEPROM	SLE 88CF1640P Secure µSlim EEPROM	SLE 88CF4002P Secure µSlim Flash/EEPROM	SLE 76CF5120P <b>new</b> Secure µSlim Flash/EEPROM	SLE 88CF4002P Secure µSlim Flash/EEPROM	SLE 88CFX4003P Secure µSlim Flash/EEPROM	SLE 88CFX6600P <b>new</b> Secure µSlim Flash/EEPROM
Product description	Security controller	Security controller optimized for mobile communication applications	Security controller	Security controller	Security cryptocontroller	Security cryptocontroller designed for high-security applications	Security cryptocontroller
User-ROM	–	Up to 328 kByte	160 kByte	–	160 kByte	up to 168 kByte	–
EEPROM	448 kByte	164 kByte	400 kByte	504 kByte	400 kByte	400 kByte	660 kByte
RAM	12kByte	12 kByte	16 kByte	12 kByte	16 kByte + 880 Byte crypto	16 kByte + 880 Byte crypto	20 kByte + 880 Byte crypto
CPU	16-bit	32-bit RISC	32-bit RISC	16-bit	32-bit RISC	32-bit RISC	32-bit RISC
Crypto coprocessor	–	–	–	–	1,408-bit arithmetic	1,408-bit arithmetic	1,408-bit arithmetic
Hardware triple DES	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Clock (int.)	1 – 33 MHz	Up to 33 MHz	Up to 66 MHz	1 – 33 MHz	Up to 66 MHz	Up to 66 MHz	Up to 33 MHz
Clock (ext.)	1 – 10 MHz	1 – 10 MHz	1 – 10 MHz	1 – 10 MHz	1 – 10 MHz	1 – 10 MHz	1 – 10 MHz
Operating voltage	1.62 V – 5.5 V	1.62 V – 5.5 V	1.62 V – 5.5 V	1.62 V – 5.5 V	1.62 V – 5.5 V	1.62 V – 5.5 V	1.62 V – 5.5 V
Max. supply current (at 5 MHz, 5 V)	10 mA	10 mA	10 mA	10 mA	10 mA	10 mA	10 mA
Max. sleep mode current (typical)	100 µA	100 µA	100 µA	100 µA	100 µA	100 µA	100 µA
Ambient temperature	-25 to +85°	-25 to +85°	-25 to +85°	-25 to +85°	-25 to +85°	-25 to +85°	-25 to +85°
Write/erase time	< 2.3 ms	< 2.3 ms	< 2.3 ms	< 2.3 ms	< 2.3 ms	< 2.3 ms	< 2.3 ms
EEPROM page programming	1 to 128 Byte	1 to 128 Byte	1 to 128 Byte	1 to 128 Byte	1 to 128 Byte	1 to 128 Byte	1 to 128 Byte
MMU	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Security features	Tamper-proof design, chip ID, basic countermeasures against SEMA/DEMA, SPA/DPA, DFA and timing attacks, exception sensors, life test function for sensors, bus confusion, pseudo random number generator, watchdog timer, memory encryption device, DES/AES in software and hardware	Tamper-proof design, chip ID, countermeasures against reverse engineering, SPA/DPA, DFA/EMA, memory encryption, sensor concept: voltage-, frequency-, light-, temperature-, glitch sensor, active shield, triple DES in HW, bus encryption, dual rail logic	Tamper-proof design, chip ID, countermeasures against reverse engineering, SPA/DPA, DFA/EMA, memory encryption, sensor concept: voltage-, frequency-, light-, temperature-, glitch sensor, active shield, triple DES in HW, bus encryption, dual rail logic, watchdog timer	Tamper-proof design, chip ID, basic countermeasures against SEMA/DEMA, SPA/DPA, DFA and timing attacks, exception sensors, life test function for sensors, bus confusion, pseudo random number generator, watchdog timer, memory encryption device, DES/AES in software and hardware	Tamper-proof design, chip ID, countermeasures against reverse engineering, SPA/DPA, DFA/EMA, memory encryption, sensor concept: voltage-, frequency-, light-, temperature-, glitch sensor, active shield, triple DES in HW, elliptic curves in HW, asymmetric algorithms, hardware-supported (e.g. RSA), bus encryption, dual rail logic, watchdog timer	Tamper-proof design, chip ID, countermeasures against reverse engineering, SPA/DPA, DFA/EMA, memory encryption, sensor concept: voltage-, frequency-, light-, temperature-, glitch sensor, active shield, triple DES in HW, elliptic curves in HW, asymmetric algorithms, hardware-supported (e.g. RSA), bus encryption, dual rail logic, watchdog timer	Tamper-proof design, chip ID, countermeasures against reverse engineering, SPA/DPA, DFA/EMA, memory encryption, sensor concept: voltage-, frequency-, light-, temperature-, glitch sensor, active shield, triple DES in HW, elliptic curves in HW, asymmetric algorithms, hardware-supported (e.g. RSA), bus encryption, dual rail logic, watchdog timer
Peripherals	CRC, UART, RNG, 2 x 16-bit autoreload timers, interrupt, PEC, DES, PLL	UART, RNG, 3 x 16-bit autoreload timers, Interrupt, Trap System, DES, Power Manager for Classes A,B,C	UART, RNG, 3 x 16-bit autoreload timers, Interrupt, Trap System, DES, Power Manager for Classes A,B,C	CRC, UART, RNG, 2 x 16-bit autoreload timers, interrupt, PEC, DES, PLL	UART, RNG, 3 x 16-bit autoreload timers, Interrupt, Trap System, DES, Crypto@1408, Power Manager for Classes A,B,C	UART, RNG, 3 x 16-bit autoreload timers, Interrupt, Trap System, DES, Crypto@1408, Power Manager for Classes A,B,C	CRC, UART, RNG, 3 x 16-bit autoreload timers, Interrupt, Trap System, DES, Crypto@1408, Power Manager for Classes A,B,C
Delivery forms	Module M4.8, M5.1, MFC5-x, VQFN-8, die	Module M4.8, M5.1, MFC5-x, die	Module M5, MFC5-x, DSO-20, die	Module M4.8, M5.1, MFC5-x, VQFN-8, die	Module M5, MFC5-x, DSO-20, die	Module M5, MFC5-x, DSO-20, die	Module M5, MFC5-x, DSO-20, die
Typical applications	64k SIM, UICC, Native, Java GSM, R-UIM	128-144k SIM, GSM, UICC, R-UIM, Java	GSM, UICC, R-UIM, Java	64k SIM, UICC, Native, Java GSM, R-UIM	GSM, UICC, Java, Digital Signature, EMV	High Secure Applications, Pay-TV, Secure Access, Digital Signature	GSM, UICC, Java, Digital Signature, EMV
Certifications	–	–	CC EAL5+ high (PP0002)	–	CC EAL5+ high (PP0002)	CC EAL5+ high (PP0002)	Planned: CC EAL5+ high, EMVCo

## Security controller overview by EEPROM sizes

EEPROM	≥ 512 KB		
Product name	SLE 88CFX6602P <b>new</b> Secure µSlim Flash/EEPROM	SLE 88CNFX6600P <b>new</b> Secure µSlim Flash/EEPROM	SLE 88CNFX6602P <b>new</b> Secure µSlim Flash/EEPROM
Product description	Security cryptocontroller	Security cryptocontroller	Security cryptocontroller
User-ROM	variable	–	variable
EEPROM	660 kByte	660 kByte	660 kByte
RAM	20 kByte + 880 Byte crypto	24 kByte + 880 Byte crypto	24 kByte + 880 Byte crypto
CPU	32-bit RISC	32-bit RISC	32-bit RISC
Crypto coprocessor	1,408-bit arithmetic	1,408-bit arithmetic	1,408-bit arithmetic
Hardware triple DES	Yes	Yes	Yes
Clock (int.)	Up to 33 MHz	Up to 33 MHz	Up to 33 MHz
Clock (ext.)	1 – 10 MHz	1 – 10 MHz	1 – 10 MHz
Operating voltage	1.62 V – 5.5 V	1.62 V – 5.5 V	1.62 V – 5.5 V
Max. supply current (at 5 MHz, 5 V)	10 mA	10 mA	10 mA
Max. sleep mode current (typical)	100 µA	100 µA	100 µA
Ambient temperature	-25 to +85°	-25 to +85°	-25 to +85°
Write/erase time	< 2.3 ms	< 2.3 ms	< 2.3 ms
EEPROM page programming	1 to 128 Byte	1 to 128 Byte	1 to 128 Byte
MMU	Yes	Yes	Yes
Security features	Tamper-proof design, chip ID, countermeasures against reverse engineering, SPA/DPA, DFA/EMA, memory encryption, sensor concept: voltage-, frequency-, light-, temperature-, glitch sensor, active shield, triple DES in HW, elliptic curves in HW, asymmetric algorithms, hardware-supported (e.g. RSA), bus encryption, dual rail logic, watchdog timer	Tamper-proof design, chip ID, countermeasures against reverse engineering, SPA/DPA, DFA/EMA, memory encryption, sensor concept: voltage-, frequency-, light-, temperature-, glitch sensor, active shield, triple DES in HW, elliptic curves in HW, asymmetric algorithms, hardware-supported (e.g. RSA), bus encryption, dual rail logic, watchdog timer	Tamper-proof design, chip ID, countermeasures against reverse engineering, SPA/DPA, DFA/EMA, memory encryption, sensor concept: voltage-, frequency-, light-, temperature-, glitch sensor, active shield, triple DES in HW, elliptic curves in HW, asymmetric algorithms, hardware-supported (e.g. RSA), bus encryption, dual rail logic, watchdog timer
Peripherals	CRC, UART, RNG, 3 x 16-bit autoreload timers, Interrupt, Trap System, DES, Crypto@1408, Power Manager for Classes A,B,C	SWP, Mifare® emulation, CRC, UART, RNG, 3 x 16-bit autoreload timers, Interrupt, Trap System, DES, Crypto@1408, Power Manager for Classes A,B,C	SWP, Mifare® emulation, CRC, UART, RNG, 3 x 16-bit autoreload timers, Interrupt, Trap System, DES, Crypto@1408, Power Manager for Classes A,B,C
Delivery forms	Module M5, MFC5.x, DSO-20, die	Module M5, MFC5.x, DSO-20, die	Module M5, MFC5.x, DSO-20, die
Typical applications	GSM, UICC, Java, Digital Signature, EMV	NFC, GSM, USIM, M-Commerce, Open Platform, EMV, ePurse, Payment, Loyalty, Access, Digital Signature	NFC, GSM, USIM, M-Commerce, Open Platform, EMV, ePurse, Payment, Loyalty, Access, Digital Signature
Certifications	Planned: CC EAL5+ high, EMVCo	Planned: CC EAL5+ high, EMVCo	Planned: CC EAL5+ high, EMVCo