| Manufacturer | Type/Model Name | Frequency | Description | Standard/Notes | Security | | | |
|---|---|------------------------------|---|------------------------|--|------|--|--|
| | Higgs 2 | 860~960 MHz | EPC up to 192 Bits, TID 64 Bits | ISO18000-6c - EPC Gen2 | ?none? Dynamic Authentication™ - Enhanced IC security using a non-digital, unique and non-cloneable "finger-print" - Practically eliminates | | | |
| Alien Technology | Higgs 3 | 860~960 MHz | EPC up to 480 Bits, TID 64 Bits | ISO18000-6c - EPC Gen2 | Torons? Departies, 41mentication ¹¹⁴ - Enhanced IC security using a non-digital, unique and non-chreatile "forger print" - Practically eliminates copied lags being applied to counterfeit or good of higher value. A 64-bit Unique TD for authentication and sensitization applications, and passed protected read and write support capabilities to prevent unauthorized viewing and modification of the target data applications. All passed of the protected read and write support capabilities to prevent unauthorized viewing and modification of the target data applications. All passed of the protected read and write support capabilities to prevent unauthorized viewing and modification of the target data. "Innore" Processing and the protected read and applications. All passed of the protection sensitization applications. All passed to prevent unauthorized viewing and modification of the target data. | | | |
| | Higgs 4 | 860~960 MHz | EPC up to 512 Bits, TID 64 Bits | ISO18000-6c - EPC Gen2 | An optimized memory footprint includes a 32-bit TID, a 64-bit Unique TID for authentication and next generation serialization applications, a 128-bit EPC memory bank, 128-bits of user memory for distributed data applications, and password protected read and | | | |
| | Monza 3 | 860~960 MHz | EPC up to 128 Bits | EPC Gen2 - ISO18000-6 | write support capabilities to prevent unauthorized viewing and modification of the tag's data. ?none? | | | |
| | Monza 4D | 860~960 MHz | EPC up to 128 Bits - User Memory 32 Bits | EPC Gen2 - ISO18000-6 | ?none? | | | |
| | Monza 4E | 860~960 MHz | EPC up to 496 Bits - User Memory 128 Bits | EPC Gen2 - ISO18000-6 | | | | |
| | Monza 4QT | 860~960 MHz | EPC up to 128 Bits - User Memory 128 Bits | EPC Gen2 - ISO18000-6 | 70mm2? Of technology is Short-Range Mode adds a layer of physical protection to a user's private data by reducing the tag's read range to less than one-term of its normal range. So while a reader can always singulate the tag and read its corrently exposed sentifier (EFC or alternate product detriffe) from normal range, any attempts due to access the Private Data Profer form a distance will cause the tag to lose power and drop out of its diadog with the reader. The short-range feature ensures that protected information is not readable unless the tag is very close to a reader atternate. | | | |
| Inpinj | Monza 5 | 860~960 MHz | User Memory 128 Bit | EPC Gen2 - ISO18000-6 | the tag is very close to a reader antenna. | | | |
| | Monza X-2K Dura | 860~960 MHz/I2C | EPC up to 128 Bits - User Memory 2176 Bits | EPC Gen2 - ISO18000-6 | 70008? Of technology is Short-Range Mode adds a layer of physical protection to a user's private data by reducing the tag's read range to less than one-term of its normal range. So while a reader can always singulate the tag and read its corrently exposed dentifier (EFC or alternate product dentifier) from normal range, may attempts due access the Private Data Profer form a distance will cause the tag to loss power and drop out of its diadig with the reader. The short-range feature ensures that protected information is not readable unless the tag is very colore to a reader atternate. | | | |
| | Monza X-8K Dura | 860~960 MHz/I2C | EPC up to 128 Bits - User Memory 8192 Bits | EPC Gen2 - ISO18000-6 | The last is very close to a staded raternal. Of licebondory Scheringer Monthanger Monta and Scheringer Scheri | | | |
| | H4001 | 50/130/400 kHz | Read only, 64 Bits | | none | | | |
| | EM4102/H4102 (replaced by EM4200) | 125 kHz | Read only, 64 Bits | | none | | | |
| | H4003 | 125 kHz - 3.25 MHz | Read only, 64 Bits | | none | | | |
| | EM4005/EM4105 (old H4005 - replaced by EM4200) | 100~150 kHz | Read only, 128 Bits | ISO11784/85 Compatible | none | | | |
| | EM4006 (old H4006) | 13.56 MHz | Read only, 64 Bits | | | | | |
| | EM4022/P4022 | Multifrequency | Read only, 64 Bits | | none | | | |
| | | | | | none | | | |
| | EM4025/EM4125 EM4026 | 100~150 kHz 125 kHz | Read only, 55 Bits Read only, 64 Bits | | none | | | |
| | EM4026 EM4033 | 125 KHZ 13.56 MHz | Read only, 64 Bits Read only, 64 Bits | ISO15693 | none | | | |
| | EM4034 (same as EM4035 but no crypto) | 13.56 MHz | R/W, 448 Bits | ISO15693 | Passeord (block (b) is never restable but written only in Secure mode. Super User Memory, FAS and Lock Block (block) (and hereat by all users but written only in Secure mode. Lock block defines which memory block are locked against pages memory words (Blocks 3 to 11) see always needable. Write access rights to bler Words (blocks 3 to 11) depend on appropriate Lock Block. Secure mode is enabled by Lock command. Login proprietaly command is a far all checks passed stored in block - password carrot be read - password can be charged only after a successful Joint Login (Secure Mode). Pass. 2010. Efforts and the transmission in the charge source in 50 words of 9 blocks, active word and the read- password in the transmission in the charge source in 50 words of 9 blocks, active word and the intervensibly locked [same as Pass. 2010. Efforts and the intervensible source and the passes and the intervensible source and the intervensible | | | |
| | EM4035 (same as EM4034 & EM4135 but with crypto) | 13.56 MHz | R/W, 3.2K Bits | ISO15693 | | | | |
| | V4050 | 125 KHz | R/W, 1024 Bits | | The choic portiants' Kinf of Exhibit which can be configured by the user, allowing a write infinited area, a reap potenticel area, and a many and read protecting area, and a market potential of the second and the second area and the second and the second and the second area and the second and the second area and the second and the second area and the second area and the second and the second area and the second and the second area and the second area and the second and the second area and the second and the second area area area and the second area and the second area area area area area area area are | | | |
| | EM4055 | 125 kHz | R/W, 1K Bits | | The memory can be secured by using the 32-bit password for all write and read protected operations. The password can be updated but never read. User defined Write protected words. User defined Read protected words. | | | |
| | EM4056/P4056 (aka MicroCID 1106) | 100~150 kHz | R/W, 2K Bits | | The user can define a password and protect part or all of the memory - password is (optionally) linked to a decremental counter, if the counter readches 0 all memory is totally locked, only non-protected blocks can be read-only. Each block can be read and/or write protected and this protection (bit=1) is OTP (unreversible). | | | |
| | EM4069/EM4169 (old Sokymat T5/Nova?) | 100~150 kHz | R/W, 128 Bits | | | | | |
| | V4070 | 125 kHz | R/W, 160 Bits | | none The chip contains an implementation of a crypto-algorithm with 96 Bits of user configurable secret-key (unreadable) contained in EEPROM. Blocks 4 through 9 contain the 96 bits of secret key. These bits influence the crypto-algorithm but cannot be read directly. | | | |
| | V4082 EM4083 | chip-only 115~140 kHz | ROM, 64 Bits R/W, 512 Bits | | none | | | |
| | P4092 | 100~150 kHz | Base Stations | | - | | | |
| | EM4094 | 13.56 MHz | Base Station | ISO15693-14443A/B | | | | |
| | EM4095 (old P4095) EM4100 (old H4100 - replaced by EM4200) | 125 kHz 100~150 kHz | Booster Circuits Read only, 64 Bits | | - none | | | |
| | EM4102 (old H4102 - replaced by EM4200) | 125 kHz | Read only, 64 Bits | | none | | | |
| | EM4105/EM4005 | 125 kHz | Read only, 128 Bits | | none | | | |
| | EM4122 | 860~960 MHz | Read only, 64 Bits | | none | | | |
| | EM4123 (protocol compatible with EM4122 & EM4222) EM4124 | 860~960 MHz 860~960 MHz | Read only, 64 Bits R/W, 176 Bits | 15018000 | none 32 bit Kill Password (block0+block1), and 32 bit Access Password (block2+block3) [default pwds = 0000'0000'0000'0000] | | | |
| EM-Marin Microelectronic (acquire Sokymat in 2003) | EM4126 | 860~960 MHz | R/W, 224 Bits R/W, 512 Bits | ISO18000 ISO15693 | none Password is located at block0 (it is never readable but written only in Secure mode after a successful Login command). Super User Memory, LAS and the Lock Block area (block2) can be read by all users but written only in Secure mode. Lock block bits define which can be wine prevented with the corresponding lock bits. Written constraints and the second s | | | |
| | | | | | can be write protected with the corresponding lock bits. Write access rights to User Words (blocks 3 to 11) depend on appropriate Lock Block bit. Secure mode is enabled only by a successful Login command (right password value). The 2.4 kb EEPROM memory contained in the chip is oronarized in 38 words of 64 bits. sech word can be irreversibly locked fsame as | | | |
| | EM4135 (same as EM4035 but no crypto) | 13.56 MHz | R/W, 2432 Bits | ISO15693 | EM40347]. The memory can be secured by using the 32 bit password (stored in block0) for all write and read protected operations. The password can be updated, but never read. Also chip has a control word (block2-bit16 pwd on/off) and a protection word (block1 - set blocks | | | |
| | EM4150/EM4350 (replaced by EM4450/EM4550) | 100~150 kHz | R/W, 1K Bits | | protection for read/write). | | | |
| | EM4170 | 125 kHz | R/W, 256 Bits | | The christ contrast are implementation of a hypical approximation to be based under contriguence access here contrasted in ELEVICA Sets To 2017 as when they are delevend. The memory can be underscaled by using the PR-kook command, in Fall care, the tack Site are reset from the value "s" to the value "s" Works & Rinning" at contrast the 56 bits of secret lay. These bits influence the cypical agrintment that the secret lay of the value "s" Works & Rinning" at contrast the 56 bits of secret lay. These bits influence the cypical agrintment without the secret lay of the value "s" Works & Rinning" at contrast the 56 bits of secret lay. These bits influence the cypical agrintment without the secret lay of the value "s" with a first lay of the secret lay. These bits influence the cypical agrintment without the secret lay of the secret lay of the secret lay. These bits influence the cypical agrintment bits without the secret lay of the secret lay of the secret lay. These bits influence the cypical agrintment without the secret lay of the secret lay of the secret lay. These bits influence the cypical agrintment bits without the secret lay of the secret lay of the secret lay. These bits influence the cypical agrintment bits without the secret lay of the secret lay of the secret lay. These bits influence the cypical agrintment bits without the secret lay of the secret lay of the secret lay. These bits influence the cypical agrintment bits without the secret lay of | | | |
| | EM4200 (replaces EM4100/4102/4005/4105) | 125~134.2 kHz | Read only, 64 Bits | ISO11784/85 Compatible | | | | |
| | EM4205/EM4305 | 125~134.2 kHz | R/W, 512 Bits | ISO11784/85 Compatible | one contains a 52 bit passend. The passend value can be charged outy after a successful Login command The 52 bit passend value can be charged outy after a successful Login command the value passend protecting dependions. The set was the set of the charged out and the read out with a read word command. There is also a "Read Login BF". When set to logit 1, the reading of all words, except Words 0 and 1 minute the read out with a read word command. There is also a "Read Login BF". When set to logit 1, the reading of all words, except Words 0 and 1 minute the read out with a read word command. There is also a "Read Login BF". When set to logit 1, the reading of all words, except Words 0 and 1 minute the set of | | | |
| | EM4222 | 300MHz~2GHz | Read only, 64 Bits | | none | | | |
| | EM4223 (replaces EM4035/EM4135) | 800MHz | Read only, 128 Bits | | none The enhanced 32 bit password (pwd changeable by write password command only in Secure Mode.) security feature permits a flexible | | | |
| | EM4233SLIC | 13.56 MHz | R/W, 1K Bits | ISO15693 | administration of the memory access rights which makes it the right soution for advanced thet protection. In Secure mode logging with password), the write access to the user's data memory depends on Lock blo only. A pair of tibs define the protection status of the corresponding user's data memory page against reading and/or writing - Protection bit status is not taken in account in secure mode Chanceable in Secure mode by Protect Page command. | | | |
| | EM4233 2k | 13.56 MHz | R/W, 2K Bits | ISO15693 | none The enhanced 2b bt passwortd (pred changeable by write passworld command only in Secure Mode.) security feature permits a flexible administration of the memory access rights which makes I the right solution for above control feature protection. In Secure mode (toggin corresponding user) and the memory access rights which makes I the right solution for above control feature protection. In Secure mode (toggin corresponding user) and the solution of th | | | |
| | EM4237SLIC | 13.56 MHz | R/W, 1K Bits | ISO15693 | Security features based on a 32-bit password - Advanced NVM management access conditions - Memory blocks/page. Locking mechanism - Lock mechanism for AFI, DSR1S and EAS - Password protected EAS and AFI functionality - Destroy function to deactivate the chip forever. | | | |
| | EM4237 | 13.56 MHz | R/W, 2K Bits | ISO15693 | Choip Security based on Cantel 28A cryptol algorithm - Mutual Authentication based on challengo/response - Secure Messaging - encryption of the RF communication channer - Message Authentication Code (March - Possibility located security level based on a 32- bit password - Optional Random ID for enhanced security and privacy - EEPROM blocks/pages Locking mechanisms - Destroy Inunction to deactivate the chip lower. | | | |
| | EM4269 | 125 kHz | R/W, 512 Bits | ISO FDX-B | bits which transform them in read-only. 32 bit Password read and write protection The reader integrates the crypto adortition of the EM435 transporter IC secondard with 4 second keys. Each secret keys is QR bit | | | |
| | EM4294 | 13.56 MHz | Front End | ISO15693/ISO 14443A/B | bit password - Optional Random II bit enhanced security and privacy - EEPROM biockspages Locking mechanisms - Destroy Inaction to designate the priviporour- bit privacy - Destroy - Des | | | |
| | EM4298 EM4322 | 860~960 MHz 125kHz+6.8MHz | Decoder Read only, 64 Bits | ISO18000 | UHF Decoder/Encoder circuit, iP-X, ISO 18000-6A/B & C compliant | | | |
| | EM4322 EM4324 | 125kHZ+6.8MHZ 860~960 MHz | Read only, 1024 Bits | ISO18000 | none 32-bit password-protected Kill command. 32-bit password-protected Access command. Anti-tearing feature to prevent malicious | | | |
| | EM4325 | 860~960 MHz | R/W, 4096 Bits | 15018000 | unlocking 32-bit password-protected Kill command. 32-bit password-protected Access command. BlockPermalock command for User memory (block is defined to be one page (4 words) in EEPROM. Only for User memory). | | | |
| | | 000 - 200 PH12 | .,.,., | 13010000 | (block is defined to be one page (4 words) in EEPROM. Only for User memory). | | | |

| Manufashunan | Turne (Mendel Manne | Freedoment | Description | Chan david (Natao | |
|---|--|---------------|--------------------------------|------------------------|--|
| Manufacturer | Type/Model Name | Frequency | Description | Standard/Notes | Security thanks to Hardware AES-128-Hardware ESISDE Shardware Random Number Generator FIPS140-2. New stream cipher Grant 282 with 728-bit key, High secure proprietally cryptor with 58 bit key, Hardware Random Number Generator. Three pass mutual authentication according is standard ISD 5978-2. Data subtractly provided with 25 bit Mox. Chr eV CC Getter Stree modes to scure or modes. Normal mode used by al users / Safe Access mode granted to power users / Administration mode for card personalization. The Safe Access and Administration mode can be protected by Getter Uter (Here Internet). |
| | EM4333 | 13.56 MHz | R/W, 1K System+4K User+64KCode | ISO15693-ISO14443A | Passavd protection House a difference of the second protection |
| | EM4350/EM4150 | 100~150 kHz | R/W. 1K Bits | | crypto modes can be used in orderent modes as EBU, doub and U.F. Acts conter suite outre and accountly win 1.20 for key reignt. DESV3DES offer schedund compatibility to previous products. The memory can be secured by using the 32bit password (stored in block) for all write and read protected operations. The password can be updated, but herer read. Acts OrdEx2DEST schedung and contection word plock 1 - set blocks Can be updated, but herer read. Acts OrdEx2DEST schedung and contection word plock 1 - set blocks |
| | EM4369 | 125 kHz | R/W, 512 Bits | ISO FDX-B | protection for read/write). |
| | EM4444 | 300MHz-2.4GHz | R/W, 512 Bits | | protected by setting tack bits which transform them in read-only. 7 pages dues programmable and tockable memory (64-bit pages) |
| | EM4450/EM4550 (replaces EM4150/EM4350) | 125 kHz | R/W, 1024 Bits | | The memory can be secured by using the 32 bit password (stored in blocks) for all write and read protocled operations. The password can be updated, but new resark Jako chip has a control word (block-2-bit for your control word (block-2-bit for your control word (block-2-bit for your control word block) and be protocled word (block-1-bit blocks) |
| | EM4469/EM4569 (same as EM4469 with extended range) | 100~150 KHz | R/W, 512 Bits | ISO11785 Compatible | protection for resolvinte). Read and vite access to EEPROM can be protected by 32 bit password. All EEPROM words can be write protected by setting lock bits which transform them in read-only. 32 bit Password read raid write protection. The 32 bit Password word has to be sett in Login command the available password protected positions. The Password word has to be setting lock bits which transform them in read-only. 32 bit Password read raid write protected on the solution to the solution of the password protected position. The 32 bit Password word has to be setting lock bits which transform them in read-only. 32 bit Password word has been available to the solution of the password protected position. The 32 bit password word has been available to the password protected by a pair to bits in the protected to password protected by a pair to bits in the word can be write (the becomes read-only). |
| | EM4522 | 125kHz+6.8MHz | R/W, 640 Bits | | |
| | EM4550/EM4450 (replaces EM4150/EM4350) | 125 kHz | R/W, 1024 Bits | | The memory can be secured by using the 32b it password (doned in block) for all write and read protected operations. The password can be update, but hower read, Alch oright as a control word (block) 2bit 6 pwd on/off) and a protection word (block) as protection for read/write). The chip security features are based on ALS-126 opytography. In order to enforce the confidentially level of the data exchanged between the reader and the N4 chip, the contactes communication channel the chip maximizes Undertication of the data and and and and and and and and and an |
| | NF4 | 13.56 MHz | R/W, 8K/32K/64K Bytes | IS014443A | Adhentication Code MACQ Optional Secure Newspacing (SM) Elon Calo In 6 Provide Intel RF communication Calo Intel R |
| | TK5530 | 125 kHz | Read only, 126 Bits | | |
| | TK5551 | 125 kHz | R/W, 264 Bits | ISO11784, 11785 | ImableX 2). The number of transported as and the time to read out are dependent on the application. If the ACR mode has been configured by ACR bit all bock 0, the transported remains in the product in the ACR mode has been command is sent, the dedicated transported remains in the product in the ACR in the AcR mode has been command is sent, the dedicated transported remains in the Armen, the transported re able to modulate the Edit (State Head). De to the ACRS the transported is able on to ACR with use up command is sent, the dedicated transported is worked on the ZS bit parameter. The transmit the transported is able to modulate the Edit (State Head). De to the ACRS the transport is able to modulate the Edit (State Head). De to the ACRS the transport is able to modulate the Edit (State Head). De to the ACRS the transport is able to modulate the Edit (State Head). De to the State Test Head Head Test and the ACR with use up sequence measured with the Internative the transport is the Acr (State Head). The Armed Head Test and the ACR with use up sequence DP code to stop the modulation of the transport. The books can be protected against overwriting by using took bits. The books can be protected against overwriting by using took bits. The Books can be protected against overwriting by using took the Ct. the |
| | e5561 | 125 kHz | 36 Bytes | none | crypto circul uses the coefficient AUT68 algorithm the encrypt the challinge which a written to the ed5613. The computed result can be proceedure is established. This proceedure requires the crypto key of the 5501 and the base station to be equify the stored in tocks 5 to 6 of the EEPROL and can be tocked by the user to avoid read out or changes. Another tock contains a password to prover user setting to the contained out of the 5501 and the base station to be equify the stored in tocks 5 to 6 of the EEPROL and can be tocked by the user to avoid read out or changes. Another tock contains a password to prover user substration of the store and the store out of the 5501 and the test store out of the store in all other cases, an enror handing procedure is statisticating and the store out of the EEPROMs content and store user conduct. The cost of the test store test store out of the EEPROMs or the store out of the costs of the crypto key and the compression base all bodies and the if the base statistication of the store out of the costs and the test of the test store in the costs of the crypto key and the compression base all bodies and the if the base statistication is to read of the proceeding exception base all bodies and the if the base statistication is to read of the proceeding exception base all bodies and any more. These are several lock-bits available, each the crypto key lock bit is static the region key can not be modified or read out any more. These are several lock-bits available, each - Lock bits bits the programming of the secolification of the EEPROM - Lock bits bits the programming of the secolification of the SEPROM - Lock bits bits the programming of the secolification of a specification are and my more. These are several lock-bits available, each - Lock bits bits the programming of the secolification of a specification are an enror handing procedure (i.e., the e5561 enters |
| | ATA5550 | 125 KHz | R/W, 264 Bits | | The blocks can be protected against overwriting. One block is reserved for setting the operation modes of the IC. Another block can bloin a nessward to proved un suptrivited writing unartherized writing the operation modes of the IC. Another block can bloin a nessward to proved unartherized writing the operation modes of the IC. Another block can bloin a nessward to proved unartherized writing the operation modes of the IC. Another block can block can be protected against overwriting. One block is reserved for setting the operation modes of the IC. Another block can block can be protected against overwriting. One block is reserved for setting the operation modes of the IC. Another block can block can be protected against overwriting. |
| | ATA5551 | 125 KHz | R/W, 264 Bits | | The ACR mode is an anti-collasion procedure for transpronders to reset, e.g., and transpronders in the field during 500ms (6762, mablock 2). The unturned or transprodures and the time to read use dependent on the apopriation. If the ACR mode has been configured by ACR bit at block 0, the transproder remains in steep mode while putting intrin be field. If the specified ACR wake-up command is surt, the declated transproder generates an interact RESET (see section VP Code Genards 1 in the Arrel edSS01 databate), Due to the RESET the transported is avoiden up. That means, the transproder is avoide to modulate the field (ead mode). The ACR wake-up commond consist of the Or Code soft mode 3 is the transproder is avoided to modulate the field (ead mode). The ACR wake-up sequences measured write-firme frames and the content of the password. The electration section flow end the Arrel edSS01 measured write-firme frames and the content of the password. The other content is the field, the necessary (or write the stop) (PC code to stop the modulation of the transproder. It is ablock to avoid the stop (or bit) (PC code to stop the modulation of the transproder. Bit bits and the procedure datarial or eventified by using to bits (b). |
| | T/TK/5552 | 125 KHz | R/W, 1024 Bits | ISO11784, 11785 | BI 0 drevy block is the lock bit for that block. Once locked, the block (including the lockbit itsef) asamot be field-reprogrammed. Blocks 1 to 6 are freely programmable. Block 7 may be used for the used for user data. When prevent the analysis are regarded as the prevent the used for user data. When prevent the third is a the regarder of the prevent the used for the |
| | T5554 | 100-150 KHz | R/W, 264 Bits | ISO11784, 11785 | compared bit-by-det with the contents of block / stamming at ut 1. The comparison task, the IC will not program the memory, but related to in near mode bit-by both roow writing participation of the content of the co |
| | T5556 | 125 KHz | R/W, 2560TP+224 Bits | | BIt 0 drevery block is the lock bit for that block. Once locked, the block (including the lockbit itself) cannot be modified again during configuration. In password mode (PMD bit set), the direct access to a single block needs the valid 32-bit password to be transmitted. Bit 0 of every |
| | ATA5557 | 100-150 KHz | R/W, 330 Bits | | block is the lock bit for that block. Once locked, the block (including the lock bit itself) is not re-programmable through the RF field analin |
| Atmel (acquired Tenic Semiconductre) Integrated Circuit Business in 1998) | ATA5558 | 125 kHz | 1344 BRs (1024+320) | 15011784, 11785 | Plasmod Protection - The user memory is subdivided into continuous page arrays which can be confidented to that write or readivities operations on tobols write the segretized prevalence of t |
| | TK5561A-PP | 125 kHz | 128 bits | ISO11784, 11785 | base status, e.g. based on the U22706. Up to four blocks consisting of the user programmable D cooks, the crypto key and configurations are stored in skibolost. The crypto key and the D cooks can be crypto key and in passed mode (PWD bit ke), the direct access to a single block needs the valid 32-bit password to be transmitted. BI 0 of every block at the lock 10 for that block. One clock, the block (inclusing the lock 11 test) or in derogrammable D cooks and the provide the agent of the direct block at the lock 10 for that block. One clock, the block (inclusing the lock 11 test) or in derogrammable Bit of every block at the lock 10 for that block. One clock, the block (inclusing the lock 11 test) or in derogrammable Bit of the direct block at the lock 10 for that block. One clock, the block (inclusing the lock 11 test) or in derogrammable Bit of test block at the lock 10 for that block. One clock, the block (inclusions) are block test block (inclusions) are programmable Bit of test block at the lock 10 for that block. One clock, the block (inclusion 12 test) are block test block (inclusions) are programmable Bit of test block. The block (inclusions) are block test block (inclusions) are block test block (inclusions) are programmable Bit of test block (inclusions) are block test block (inclusions) are bl |
| | ATA5567 (upgraded version of ATA5557) | 100-150 KHz | R/W, 330 Bits | | In password mode (rm-uo rag, in errere acteds to a single block needs the valid 32-oft gassword to be transmitted. SHI 0 of every block is the lock bit for that block. Once locked, the block (including the lock bit listel) is not re-programmable through the RF field again). In Terric databatest a dagarent mention the word "password" but it should be an enrollypo. |
| | ATA5570 | 125 kHz | RW, 330 Bits | ISO11784, 11785 | again) in Temic databated adagam menton the word "baseword" but altwold be an enrorhypo. In password mode (PMD bit set), the direct access to a single block meeds the valid 32-bit password ob be transmitted. Bit 0 of every block is the lock for that block. Choce locket, the block (including the lock Titled) is not e-programmable through the RT field |
| | ATA5577 (replaces ATA5567/T5557/TK5551) | 125 KHz | R/W, 363 Bits | ISO11784/85 Compatible | again. "When parameter done is acids: PMO = 11, the first 32 bits difference of an Parameter of a Parameter of the parameter |
| | ATA5575M1 | 100-150 KHz | R/W, 128 Bits (OTP) | | The lock bits of the Configuration register are the bits 1 to 5 of the configuration type (type 16) and are able to prevent the whole memory and the Configuration of the Configuration of the type of the configuration |
| | ATA5575M1 | 100-150 KHz | R/W, 128 Bits (OTP) | ISO11784/85 - FDX-A/B | The lock bits of the Configuration register are the bits 1 to 5 of the configuration type (type 16) and are able to prevent the whole memory of the Annel ATASSTM1 from reprogramming. As in go as the lock bits are set to 100000° the memory is alterable and the device can be programmed by the cachiner. In this case the Annel ATASSTM3 set dots Annum via all digits are to 70, by setting the lock bits to 11010° the whole memory is locked and cannot be altered. After Reset the Annel ATASSTM1 entires regular read mode and sets dots of alta. Consequently the used a 1 arrangorder with an Annel ATASSTM1 by the combiner to the recombinations of bit 1 - bit 5 are not defined and may lead to mailunction of the IC. |

| Manufacturer | Type/Model Name | Frequency | Description | Standard/Notes | Security | | | | | |
|---------------|---|------------|---------------------------|----------------------------|--|------|------|------|------|--|
| | | | | | Password checking (8 bytes password sotred in block3), data locking, a oneway counter. The LOCK command can be executed only after proper password validation has been performed. The LOCK command locks the addressed memory location from future changes. | | | | | |
| | | | | | The memory location can still be read with proper presumed validation. The bits within the LockRite field correspond to the panes within | | | | | |
| | AT88RF001 | 13.56 MHz | R/W, 256 Bits | IS014443B | the memory and, if set to "1", prevent all future writes to the corresponding page; i.e., LockBits field bit 6 locks Page 6 when it is set to a "1". There is no mechanism to ever "unlock" a page, so once a page is locked, it can never be unlocked and, as such, can never be | | | | | |
| | ATOOKFUUI | 13.30 MHZ | K/W, 250 bits | 15U14443B | There is no inectiation of the second sec | | | | | |
| | | | | | modified. The 31-bit LockBits field is set to all "0"s upon shipment from the factory. The 16-bit value stored in the counter field of Page 2 is incremented by one each time COUNT is executed. Once the value of the counter reaches 0x8000, no further count operations will be executed, and Page 2 will be effectively locked against further modification. Password validation must occur before the COUNT | | | | | |
| | | | | | be executed, and Page 2 will be effectively locked against further modification. Password validation must occur before the COUNT command is nermitted | | | | | |
| | | | | | command is permitted. Password checking (8 bytes password solted in block3), data locking, a oneway counter. The LOCK command can be executed only after proper password validation has been performed. The LOCK command locks the addressed memory location from future changes. | | | | | |
| | | | | | There is no merchanism to exclusion that been performed. The LOCK commune to be the addressed memory location from these changes The memory location can all be read in proper passion of the state of the the LocAB field for the second to be prevent and there is no performed the memory and, fast bir T, prevent all thure writes to be corresponding page i.e. LocAB is failed to II locAs fage 6 when it is set to ". There is no memory and, fast bir T, prevent all thure writes to be corresponding page i.e. LocABB field to II locAs fage 6 when it is set to any adjust bir the state of the state of the state of the state of the control field of the modified. The 31-bit LocABB field is set to all '0's upon shorement from the taketory. The Teb-N take stored in the count field of Page 1 is incremented by one each time COUNT is executed. Once the value of the count read-bib 3000. On them count specification will be addressed by the state of the state of the count read-bib 3000. The taket store of the count read- tion of the state of the state of the state of the count read-bib 3000. The taket store of the count read-bib 3000. The state of the count read- tion of the state of the state of the state of the count read-bib 3000. The state of the count read-bib 30000. These count read-bib 30000. These count read-bib 300000000000000000000000000000000000 | | | | | |
| | | | | | the memory and, if set to "1, prevent all future writes to the corresponding page; i.e., LockBits field bit 6 locks Page 6 when it is set to a | | | | | |
| | AT88RF020 | 13.56 MHz | 256 Bytes | ISO14443B | "1". There is no mechanism to ever 'unlock' a page, so once a page is locked, it can never be unlocked and, as such, can never be | | | | | |
| | | | | | modified. The 31-bit Lockats here is set to all 0's upon shipment from the factory. The To-bit value stored in the counter here of Page 2 is incremented by one each time COUNT is executed. Once the value of the counter reacters bx8000. no further count operations will | | | | | |
| | | | | | be executed, and Page 2 will be ellectively locked against further modification. Password validation must occur before the Cobint | | | | | |
| | AT88RF256 | 125kHz | R/W, 32 Bytes | | command is permitted. | | | | | |
| | AT88SC0104CRF CRYPTO | 13.56 MHz | 128 Bytes | IS014443B | Password and Write Lock Protection. ID lenght programmable (4-19 bytes) | | | | | |
| | AT885C0204CRF CRYPTO | 13.56 MHz | 256 Bytes | IS014443B | Symmetrical Dynamic Mutual Authentication with 84-bit Cryptographic Keys ((under exclusive patent license from ELVA)) | | | | | |
| | AT88SC0404CRF CRYPTO | 13.56 MHz | 512 Bytes | IS014443B | Encrypted Passwords with Attempts Counters Stream Encryption Ensures Data Privacy | | | | | |
| | AT88SC0808CRF CRYPTO | 13.56 MHz | 1024 Bytes | IS014443B | - Four Key Sets for Authentication and Encryption | | | | | |
| | AT88SC1616CRF CRYPTO | 13.56 MHz | 2048 Bytes | ISO14443B | Eight Sets of two 24-bit Passwords Selectable Access Rights by Zone | | | | | |
| | AT88SC3216CRF CRYPTO | 13.56 MHz | 4096 Bytes | ISO14443B | - Write Lock Mode | | | | | |
| | AT88SC6416CRF CRYPTO | 13.56 MHz | 8192 Bytes | ISO14443B | Iamper Sensors | | | | | |
| | | | | | Lock bytes (block2) - They enable the user to lock parts of the complete memory area for writing. A Read from user | | | | | |
| | MIFARE Ultralight (MF0ICU1) | 13.56 MHz | R/W, 64 Bytes | ISO14443A | memory area cannot be restricted via lock bytes functionality. OTP bytes - Block3 is the OTP page and it is preset so that all bits are set to logic 0 after production. These bytes can be bitwise modified using the WRITE command. The | | | | | |
| | | | | | WRITE command bytes and the current contents of the OTP bytes are bitwise OR'ed. The result is the new OTP byte contents. This process is irreversible and if a bit is set to logic 1, it cannot be changed back to logic 0. | | | | | |
| | | | | | contents. This process is irreversible and if a bit is set to logic 1, it cannot be changed back to logic 0. 3 independent 24-bit true one-way counters - Field concrementative read-only locking function per gage (or 2 pages for the extended | | | | | |
| | MIFARE Ultralight EV1 (MF0ULx1) | 13.56 MHz | R/W, 128 Bytes | ISO14443A | 3) independent 74-bit the one way counters - Field programmable read-only locking function per page (per 2 page) for the extended memory section - ECC based originally significant - 32-bit gased protection for persent in memory and memory pendention. Lock bytes - They enable the use to lock parts of the complete memory area for writing. A Read from user memory area cannot be retricted via lock bytes functionally (or 1994s - Nage) for the 10-Page and 18 is presers to hall all bits are to logic 0 after production. These bytes cannot be bitwise modified using the WRITE command bytes and the current contents of the 07P bytes and 18 is a lost 0 bits of per 1, and 18 is a lost 0 bits of per 1, and 18 is a lost 0 bits of the 07P bits and 18 is a lost 0 bits of the 07P bits and 18 is a lost 0 bits of the 07P bits and 18 is a lost 0 bits of the 07P bits and 18 is a lost 0 bits of the 07P bits and 18 is a lost 0 bits of the 07P bits and 18 is a lost 0 bits of the 07P bits and 18 is a lost 0 bits of the 07P bits and 18 is a lost 0 bits 0 bits of the 07P bits and 18 is a lost 0 bits 0 bits of the 07P bits and 18 is a lost 0 bits 0 bits of the 07P bits and 18 is a lost 0 bits 0 bits of the 07P bits and 18 is a lost 0 bits 0 bits of the 07P bits and 18 is a lost 0 bits 0 bits of the 07P bits and 18 is a lost 0 bits 0 bits of the 07P bits and 18 is a lost 0 bits 0 | | | | | |
| | | | | | Lock bytes - They enable the user to lock parts of the complete memory area for writing. A Read from user memory area cannot be reactively use by hudes functionality. OTB buttes - Paren 0% is the OTB paren and it is present on that all bits are active to locif. | | | | | |
| | MIFARE Ultralight C (MF0ICU2) | 13.56 MHz | R/W, 192 Bytes | IS014443A | production. These bytes can be bitwise modified using the WRITE command. The WRITE command bytes and the current contents of | | | | | |
| | MITARE Oktalight C (MIDICO2) | 13.30 PH12 | Nyw, 152 bytes | 13014443A | the OTP bytes are bitwise OR'ed. The result is the new OTP byte contents. This process is irreversible and if a bit is set to logic 1, it cannot he changed back to logic 0. 3DES authenticitien proved that hun entities have the same series and each entity can be seen as | | | | | |
| | | | | | a reliable partner for the coming communication. The applied encryption algorithm e(1) is 2 key 3DES encryption. | | | | | |
| | | | | | Mutual three pass authentication (ISO/IEC DIS 9798-2); individual set of two 6 Bytes keys per sector (per application) to support multi-application with key hierarchy. The access conditions for every data block and sector trailer are defined by 3 bits, which are | | | | | |
| | MIFARE Mini (MF1ICS20) | 13.56 MHz | R/W, 320 Bytes | IS014443A | multi-application with key hierarchy. The access conditions for every data block and sector trailer are defined by 3 bits, which are stored non-inverted and inverted in the sector trailer of the specified sector. The access bits control the rights of memory access using | | | | | |
| | MIFARE MINI (MF11C520) | 13.30 MHZ | R/W, 320 Bytes | 15014443A | stored non-inverted and inverted in the sector trailer of the specified sector. The access bits control the ngits of memory access using the secret keys A and B. The access conditions may be altered, provided one knows the relevant key and the current access condition | | | | | |
| | | | | | allows this operation. Weakness: - Proprietary cipher - Short key (max. 48 bit) < Analytical attacks possible. | | | | | |
| | MIFARE Plus S 2K (MF1SPLUS6001/6011/6031) | 13.56 MHz | R/W, 2K Byte; UID: 7Bytes | ISO14443A / AES encryption | - Access conditions freely configurable - Optional support of random IDs Multi-sector authentication, Multi-block read and write - | | | | | |
| | MIFARE Plus S 4K (MF1SPLUS8001/8011/8031) | 13.56 MHz | R/W, 4K Byte; UID: 7Bytes | ISO14443A / AES encryption | AES-128 used for authenticity and integrity - Anti-tearing mechanism for writing AES keys - Keys can be stored as MIFARE | | | | | |
| | MIFARE Plus X 2K (MF1PLUS6001/6011/6031) | 13.56 MHz | R/W, 2K Byte; UID: 7Bytes | ISO14443A / AES encryption | - Access conditions freely configurable - Optional support of random IDs Multi-sector authentication, Multi-block read and write - | | | | | |
| | MIFARE Plus X 4K (MF1PLUS8001/8011/8031) | 13.56 MHz | R/W, 4K Byte; UID: 7Bytes | ISO14443A / AES encryption | AES-128 used for authenticity and integrity - Anti-tearing mechanism for writing AES keys - Keys can be stored as MIFARE Mutual three pass authentication (ISO/IEC DIS 9798-2); individual set of two 6 Bytes keys per sector (per application) to support | | | | | |
| | | | | | mutual three pass authentication (ISO/IEC DIS 9/96-2); individual set of two 6 bytes keys per sector (per application) to support multi-application with key hierarchy. The access conditions for every data block and sector trailer are defined by 3 bits, which are | | | | | |
| | MIFARE Classic S50 (MF1ICS50) | 13.56 MHz | R/W, 1K Bytes | ISO14443A | stored non-inverted and inverted in the sector trailer of the specified sector. The access bits control the rights of memory access using | | | | | |
| | | | | | the secret keys A and B. The access conditions may be altered, provided one knows the relevant key and the current access condition | | | | | |
| | | | | | allows this operation. Weakness: - Proprietary cipher - Short key (max. 48 bit) < Analytical attacks possible. Mutual three pass authentication (ISO/IEC DIS 9798-2); individual set of two 6 Bytes keys per sector (per application) to support | | | | | |
| | | | | | multi-application with key hierarchy. The access conditions for every data block and sector trailer are defined by 3 bits, which are | | | | | |
| | MIFARE Classic S70 (MF1ICS70) | 13.56 MHz | R/W, 4K Bytes | ISO14443A | stored non-inverted and inverted in the sector trailer of the specified sector. The access bits control the rights of memory access using | | | | | |
| | | | | | the secret keys A and B. The access conditions may be altered, provided one knows the relevant key and the current access condition | | | | | |
| | | | | | allows this operation. Weakness: - Proprietary cipher - Short key (max. 48 bit) < Analytical attacks possible. | | | | | |
| | Mifare Classic Next Generation (MF1S50yyX) | 13.56 MHz | R/W, 1K Bytes | ISO14443A | authentication (ISO/IEC DIS 978-2) - Individual set of two keys per sector to support multi-application with key hierarchy | | | | | |
| | Mifare Classic Next Generation (MF1S70yyX) | 13.56 MHz | R/W, 4K Bytes | ISO14443A | Manufacturer programmed 7-byte UID or 4-byte NUID identifier for each device - Random ID support - Mutual three pass authentienter (IS-01EC-DIS-02002) - teliniqued end func lear para enders the unrened with it and leafer with lear this terreture | | | | | |
| | | | | | Manufacture programmed 73/sky UID or 4-5yk NUD dentifier for each oravie - Randon ID asport - Mutal three pass authentication (DECE DIS 578-2) - in vinicial as of the keys per sector to support - Mutal Shere pass authentication (DECE DIS 578-2) - in 4-5yk NUD bentifier for each oracine. Random ID asport - Mutal three pass authentication (DECE DIS 578-2) - in 4-5yk NUD bentifier for each oracine. Random ID asport - Mutal three pass authentication (DECE DIS 578-2) - in 4-5yk NUD bentifier for each oracine. Random ID asport - Mutal three pass - SISE will Tab Hay for authentication and data encryption | | | | | |
| | | | | | - 14 keys per application + 1 master key | | | | | |
| | MIFARE DESFire V0.6 (MF3ICD40) | 13.56 MHz | R/W, 4K Bytes | ISO14443A | Based on asynchronous 8051 w/ 3DES engine | | | | | |
| | | | | | Analytical attacks not possible but Side-channel attacks are possible Anasys multial authentication based on the crynto used | | | | | |
| | | | | | - Access rights on the level Based on asynchronous 805 UH 3/DES engine - Analytical attacks not possible but Side-channel attacks are possible - Spass multia anterinization based on torght used Confidentially EnDecryction based on torght used TDES DEST: Note Mode: 160-byte; based on key - TDES DEST: Note Mode: 160-byte; based on key - TDES DEST: Note: Mode: 160-byte; based on key - TDES DEST: Note: Mode: 160-byte; based on key - TDES DEST: Note: Mode: 160-byte; based on key - TDES DEST: Note: Mode: 160-byte; based on key - TDES DEST: Note: Mode: 160-byte; based on key - TDES DEST: Note: Mode: 160-byte; based on key - TDES DEST: Note: Mode: 160-byte; based on key - TDES DEST: Note: Mode: 160-byte; based on key - TDES DEST: Note: Mode: 160-byte; based on key - TDES DEST: Note: Mode: 160-byte; based on key - TDES DEST: Note: Mode: 160-byte; based on key - TDES DEST: Note: Mode: 160-byte; based on key - TDES DEST: Note: Mode: 160-byte; based on key - TDES DEST: Note: Mode: 160-byte; based on key - TDES DEST: Mode: 160-byte; based - TDES DEST: Mode: 160-byte; based - TDES DEST: Mode: 160-byte; based - T | | | | | |
| | MIFARE DESFire EV1 (MF3ICD21/MF3ICD41/MF3ICD81) | | | | TDES DESFire Native Mode: 16-byte; based on key symmetry DES or TDES. TDES Standard Mode: 16-byte; based on key symmetry DES or TDES. 3KTDES: 24-byte. AES: 16-byte, AES-128. | | | | | |
| | (MF31CDH21/MF31CDH31/MF31CDH41) | 13.56 MHz | R/W, 2K/4K/8K Bytes | ISO14443A | -3-pass mutual authentication based on the crypto used. - Confidentiality En/Decryption based on crypto used. | | | | | |
| | | | | | - Confidentiality En/Decryption based on crypto used. | | | | | |
| | MIFARE ProX P8RF6x | 13.56 MHz | R/W, 4-16 KBytes+OS | IS07816+IS014443A | | | | | | |
| | SmartMX P5Sxxxx | 13.56 MHz | R/W, 10-72 KBytes+OS | IS07816+IS014443A | | | | | | |
| | | | | | | | | | | |
| | SmartMX P5Cxxx | 13.56 MHz | R/W, 10-72 KBytes+OS | IS07816+IS014443A | | | | | | |
| | | | | | The Write Access Condition bits in block 2 determine the write access conditions for each of the 16 blocks. These bits can be set only | | | | | |
| NXP (Philips) | I.CODE1 (SL1ICS30) | 13.56 MHz | R/W, 512 Bits | | to 0 (and never be changed to 1), i.e. already write protected blocks can never be written to from this moment on. This is also true for block 2. If this block is set into write protected state by clearing of bits 4 and 5 at byte 0, no further changes in write access conditions | | | | | |
| | | | | | | | | | | |
| | I.CODE1 (SLIICS31) | 13.56 MHz | R/W, 512 Bits | | The Write Access Condition bits in block 2 determine the write access conditions for each of the 16 blocks. These bits can be set only to 0 (and never be changed to 1), i.e. already write protected blocks can never be written to from this moment on. This is also true for block 2. If his block is set into write protected state by dearing of bits 4 and 5 at byte 0, no further changes in write access conditions | | | | | |
| | neober (seriessi) | 13.30 PH12 | N/W, 512 Dits | | block 2. If this block is set into write protected state by clearing of bits 4 and 5 at byte 0, no further changes in write access conditions are possible. | | | | | |
| | LCODE UID (SL2ICS11) | 13.56 MHz | R/W. 192 Bits | | none | | | | | |
| | | | | | The Write Access Condition bits in block -1 determine the write access conditions for each of the 28 user blocks and the special data block. These bits can be set only to 1 with a lock command (and never be changed back to 0), i.e. already write protected blocks can | | | | | |
| | I.CODE SLI (SL2ICS20) | 13.56 MHz | R/W, 1024 Bits | ISO15693 | block. These bits can be set only to 1 with a lock command (and never be changed back to 0), i.e. already write protected blocks can never be written to from this moment on | | | | | |
| | | | | | never be written to from this moment on. Password protected Label Destroy. With the 32-bit destroy password an addressed label can be destroyed with the Destroy command. | | | | | |
| | | | | | That status is inversible and the label will never respond to any command again. Password protected Privacy (New With the 32-bit Privacy password a label can be set to the Privacy mode with the Set to Privacy Mode command. In that mode the label will not respond to any command except of the command Get Random Number III il receives again the right Privacy password. That mode is | | | | | |
| | I.CODE SLI - L (SL2ICS50) | 13.56 MHz | R/W, 512 Bits | ISO15693 | respond to any command except of the command Get Random Number till it receives again the right Privacy password. That mode is | | | | | |
| | | | | | especially designed to meet the increasing demand to take care of the customers privacy Password protected EAS Functionality: With the 32-bit EAS password the addressed label can be set in a mode that the commands Set EAS and Reset EAS are only executed by the label if the right EAS password is transmitted to the label within the mentioned commands. Lock mechanism for each | | | | | |
| | | | | | executed by the label if the right EAS password is transmitted to the label within the mentioned commands. Lock mechanism for each | | | | | |
| | | | | | executed by the lader with religit EXPS associate a transmission of the lader within the international count manual. Lock million protection is ser memory block (write protection). Password protected Label Destroy. With the 32-bit destroy password an addressed label can be destroyed with the Destroy command. That status is intrevensible and the label will never respond to any command again. Password protected Privacy Mode: With the 32-bit that status is intrevensible and the label will never respond to any command again. Password protected Privacy Mode: With the 32-bit protection of the label will never respond to any command again. Password protected Privacy Mode: With the 32-bit protection. | | | | | |
| | | | | | That status is irreversible and the label will never respond to any command again. Password protected Privacy Mode: With the 32-bit | | | | | |
| | | | | | Privacy password a label can be set to the Privacy mode with the Set to Privacy wood command, in that mode the label will not respond to any command except of the command Get Random Number till it receives again the right Privacy password. That mode is | | | | | |
| | I.CODE SLI - L HC (SL2ICS51) | 13.56 MHz | R/W, 512 Bits | ISO15693 | Prassword protected Late Leterity With the 32-64 destroy password an adversed table can be destroyed with the Leterity command. Protacy password is a balance of the second seco | | | | | |
| | | | | | executed by the label if the right EAS password is transmitted to the label within the mentioned commands. Lock mechanism for each | | | | | |
| | | | | | user memory block (write protection). OTB Memory for EPC Code: The end of the EPC Code is an one time accommodely memory, which are used that the data are | | | | | |
| | | | | | OTP Memory for EPC Code: The memory for the EPC Code is an one time programmable memory, which ensures that the data can not be changed after user programming (can be write only once) - Password protected memory management (Read/Write access) : | | | | | |
| | | | | | Pages (1 page = 4 blocks of 4 byte each) can be protected with a password, which ensures that only authorized users get read/write | | | | | |
| | | | | | Page (1 page = 4 blocks of 4 byte each) can be protected with a password, which ensures that only authorized users get read/write access to the protected parts of the user memory (and counterfeiting). Password protected Label Destroy. With the 32-bit destroy password an addressed label can be destroyed with the Destroy command. That status is treversible and the label will never respond | | | | | |
| | I.CODE SLI – S (SL2ICS53) | 13.56 MHz | R/W, 2048 Bits | ISO15693 | to any command again - Password protected PPinacy Mode With the 32-bit Privacy password a table can be set to the Privacy mode with the Set to Privacy Mode command. In that mode the table will not respond to any command use except of the commond GeR Random Number III it receives again the right Privacy password. That mode is especially designed to meet the increasing demand to take care of the customers privacy - Password protected EAS Prunciconality. With the 23-bit RASP assword is dual data can be set in a start privacy - Password protected EAS Prunciconality. With the 23-bit RASP assword is dual data can be set in a start privacy - Password protected EAS Prunciconality. With the 23-bit RASP assword is dual data can be set in a start privacy in the start protected EAS Prunciconality. With the 23-bit RASP assword is dual data and bit the start privacy in the start protected EAS Prunciconality. With the 23-bit RASP assword is dual data and bit privacy protected EAS Prunciconality. With the 23-bit RASP assword is dual to the 24-bit RASP assword is dual to the 24-bit RASP assword in the distribution of the start privacy privacy material to the 24-bit RASP assword is dual to the 24-bit RASP assword in the distribution of the 24-bit RASP assword in the 24-bit RASP assword in the distribution of the distribution of the distribution of the 24-bit RASP assword in the 24-bit RASP | | | | | |
| | | | | | win the Set to Privacy indee command, in that indue the label win for tespecially designed to meet the increasing demand to take care Number till it receives again the right Privacy password. That mode is especially designed to meet the increasing demand to take care | | | | | |
| | | | | | of the customers privacy Password protected EAS Functionality: With the 32-bit EAS password the addressed label can be set in a mode that the regression EAS and Deade EAS processing and the the label if the cited EAS ensemble is the label. | | | | | |
| | | | | | mode that the commands Set EAS and Reset EAS are only executed by the label if the right EAS password is transmitted to the label within the mentioned commands. Lock mechanism for each user memory block (write protection). | | | | | |
| | | | | | OTP Memory for EPC Code: The memory for the EPC Code is an one time programmable memory, which ensures that the data can not be changed after user programming (can be write only once). Password protected memory management (Read/Write access) : Pages (1) page = 4 blocks of 4 byte each) can be protected with a password, which ensures that only authorized users get read/write access that the second | | | | | |
| | | | | | Pages (1 page = 4 blocks of 4 byte each) can be protected with a password, which ensures that only authorized users get read/write | | | | | |
| | | | | | access to the protected parts of the user memory (anti counterfeiting) Password protected Label Destroy. With the 32-bit destroy password an addressed Label can be destroyed with the Destroy command. That status is inversible and the label will never respond to any command again Password protected Privacy Mode: With the 32-bit Privacy password a label can be set to the Privacy mode | | | | | |
| | I.CODE SLI - S HC (SL2ICS54) | 13.56 MHz | R/W, 2048 Bits | ISO15693 | to any command again Password protected Privacy Mode: With the 32-bit Privacy password a label can be set to the Privacy mode | | | | | |
| | | | | | with the Set to Privacy Mode command. In that mode the label will not respond to any command except of the command Get Random Number till it receives anain the right Privacy password. That mode is especially designed to meet the increasing demand to take care | | | | | |
| | | | | | of the customers privacy Password protected EAS Functionality: With the 32-bit EAS password the addressed label can be set in a | | | | | |
| | | | | | of the customers privacy Password protected EAS Functionality: With the 32-bit EAS password the addressed label can be set in a mode that the commands Set EAS and Reset EAS are only executed by the label if the right EAS password is transmitted to the label within the mentioned commands. Lock mechanism for each user memory block (within the protection). | | | | | |
| | | | | | | | | | | |
| | I.CODE SLIX (SLS2002/SLS2102) | 13.56 MHz | R/W, 1024 Bits | ISO15693/ISO18000-3 | the EAS status and the AFI value can only be changed if the correct EAS/AFI password is transmitted to the label within the mentioned commands. Lock mechanism for each user memory block (write protection). | | | | | |
| | | | | | Password protected Label Destroy. The 32-bit Destroy password enables an addressed label to be destroyed with the DESTROY | | | | | |
| | | | | | Password protected Label Destroy: The 32-bit Destroy password enables an addressed label to be destroyed with the DESTROY SLXL command. That status is inneversible and the label will never respond to any command again - Password protected Privacy Mode: The 32-bit Privacy password enables a label to be set to the Privacy mode with the ENABLE FRUNCY command. In this mode | | | | | |
| | I.CODE SLIX-L (SLS5002/SLS5102) | 13.56 MHz | R/W, 512 Bits | ISO15693/ISO18000-3 | the label will not respond to any command except the command GET RANDOM NUMBER, until it next receives the correct Privacy | | | | | |
| | | | | | demand to take care of the customers privacy - Password protected EAS and AFI functionality. The 32-bit EAS/AFI password enables | | | | | |
| | | | | | The table will not respond to any command except the command GET RANDOM NUMBER, util 1 not receive the covered Privacy password. This mode is especially dependent of meet the increasing A.S. or AFI Learning and the CASAFT password enables the addressed late to be set in a mode where the EAS status and the AFI value can only be charged if the correct EASAFT password to standing the label within the membrande commands. Los mechanism pass and the AFI value can only be charged if the correct EASAFT password to standing the label within the membrande commands. Los mechanism for east at the memory took charge passion and the AFI value can only be charged if the correct EASAFT password enables to standing the label within the membrande commands. Los mechanism for east use memory took charge passion. | | | | | |
| | | | | | a consensation to the label where the memories commands, cock mechanism for each user memory block (write protection). | | | | | |
| | | | | | | | | | | |

| Notion Notion Notion Notion Notion Notion Notion Notion Notion | er | | _ | | | - | | | | | |
|---|----|--|--|---|---|--|------|-------|------|--------|--|
| Partner < | | Type/Model Name | Frequency | Description | Standard/Notes | Security Password protected memory management (Read/Write access): Pages (1 page = 4 blocks of 4 bytes each) can be protected with a password, which ensures that only authorized users get read/write access to the protected parts of the user memory (anti | | | | - | |
| Normal Normal < | | | | | | counterfeiting) - Password protected Label Destroy. The 32-bit Destroy password enables an addressed label to be destroyed with the DESTROY SI IX-S command. That status is increasible and the label will never record to any command again - Password protected. | | | | | |
| Normal Normal < | | LCODE SLIX-S (SLS5302/SLS5402) | 13.56 MHz | R/W, 512 Bits | ISO15693/ISO18000-3 | Privacy Mode: The 32-bit Privacy password enables a label to be set to the Privacy mode with the ENABLE PRIVACY command. In | | | | | |
| Normal Normal < | | | | .,.,., | | this mode the label will not respond to any command except the command GET RANDOM NUMBER, until it next receives the correct Privacy password. This mode is especially designed to meet the increasing demand to take care of the customers privacy - Password | | | | | |
| Normal | | | | | | protected EAS and AFI functionality. The 32-bit EAS/AFI password enables the addressed label to be set in a mode where the EAS | | | | | |
| Increase Normal | | | | | | mentioned commands. Lock mechanism for each user memory block (write protection). | | | | | |
| Instantion Note | | LCODE ILT (SL2S1402/1502/1602) | 13.56 MHz | R/W. 240 Bits | ISO18000-3 | EAS (Electronic Article Surveillance) functionality - Recommissioning feature (privacy) with 32-bit kill password - 32-bit access password to allow a transition into the secured state - Long read/write ranges due to extremely low-power design. Lock mechanism for | | | | | |
| Name Note Note <t< td=""><td></td><td></td><td></td><td>.,,</td><td></td><td>each user memory block (write protection). EAS (Electronic Article Sumplifymen) functionality. Becommissioning feature (educed) with 22 bit fill executed</td><td> </td><td></td><td></td><td> </td><td></td></t<> | | | | .,, | | each user memory block (write protection). EAS (Electronic Article Sumplifymen) functionality. Becommissioning feature (educed) with 22 bit fill executed | | | | | |
| Name Norm | | I.CODE ILT-M (SL2S1412/1512/1612) | 13.56 MHz | R/W, 510 Bits | ISO18000-3 | password to allow a transition into the secured state. The user memory can be write locked, permanently write locked, unlocked, | | | | | |
| Normal Normal Normal Normal Normal Normal Normal Normal Normal Normal Same Same< | | LCODE ERC (SL2ICS10) | 13 56 MHz | P/W 136 Bite | EDC | permanently unlocked or block permalocked. | | _ | | | |
| Normal Array and Array | | | | | | | | | | | |
| Instant Mathem | | | | | EPC | Memory is OTP. Label destroy command with 24 bit destroy code protection. | | | | | |
| Parten Non < | | | | | | Encryption, authentication, 2x32 Bit passwords.Parts of memory can be write protected by the user. | | | | | |
| International Int | | HITAG1 HT1DC20S30 | 125 KHz | R/W, 2048 Bits | | Encryption, authentication, 2x32 Bit passwords.Parts of memory can be write protected by the user. Encryption, authentication, 16 Bit KeyHigh and 48 Bit KeyLow: 2 passwords (32 and 24 Bit): 5 Modes: Crypto = r/w using crypted | | _ | | | |
| Normal Normal </td <td></td> <td></td> <td></td> <td></td> <td></td> <td>transmission; Password = r/w in plain text previous password check; A = EM4100 - B = Animal ID; C = PCF793x. HITAG 2 is the name</td> <td></td> <td></td> <td></td> <td></td> <td></td> | | | | | | transmission; Password = r/w in plain text previous password check; A = EM4100 - B = Animal ID; C = PCF793x. HITAG 2 is the name | | | | | |
| Internation Int | | HITAG2 HT2ICS20 | 125 KHz | R/W, 32 Bytes | ISO11784/11785 | of the protocol used by the transponder and is identified as ID46 by SILCA's RW4. The original transponder from NXP is of the type PCF7936 (or same product family). Nevertheless, SILCA and JMA offer compatible transponder types, too, in case of SILCA, this | | | | | |
| Normal Normal </td <td></td> <td></td> <td></td> <td></td> <td></td> <td>transponder is called T14 and in case of JMA it is called TP12. Still, one will in most cases find the more generic name "Philips 2nd</td> <td></td> <td></td> <td></td> <td></td> <td></td> | | | | | | transponder is called T14 and in case of JMA it is called TP12. Still, one will in most cases find the more generic name "Philips 2nd | | | | | |
| Image: Section of the section of | | | 135 644 | D/W 22 Puter | 10011784/11785 | Encryption, authentication, 16 Bit KeyHigh and 48 Bit KeyLow; 2 passwords (32 and 24 Bit); 5 Modes: Crypto = r/w using crypted | | _ | | | |
| Normal Normal </td <td></td> <td></td> <td></td> <td></td> <td>15011784/11785</td> <td></td> <td> </td> <td> _</td> <td></td> <td></td> <td></td> | | | | | 15011784/11785 | | | _ | | | |
| Normal sector Normal | | | | | | | | | | | |
| Image: state | | | | | | | | | | _ | |
| Image: state of the | | HITAG µ HTMS1001 | 125 KHz | R/W, 128 Bits | ISO14223 | | | | | | |
| Name Note Note Note Note Note Note Note Note < | | | | | | Memory Lock functionality - 32-bit password feature. | | | | | |
| Instant Name 100 0.000 <td< td=""><td></td><td></td><td></td><td></td><td></td><td>Memory Lock functionality - 32-bit password feature.</td><td> </td><td> _</td><td></td><td> </td><td></td></td<> | | | | | | Memory Lock functionality - 32-bit password feature. | | _ | | | |
| Print Print Print | | | | Read only, 64 Bits | ISO11784/11785 | none | | _ | | | |
| N7300 10 M0 10 M0 <t< td=""><td></td><td></td><td></td><td></td><td></td><td></td><td> </td><td> </td><td>_</td><td></td><td></td></t<> | | | | | | | | | _ | | |
| N730 IA30 IA30 </td <td></td> <td>PCF7930</td> <td>125 kHz</td> <td>R/W, 1024</td> <td></td> <td>transponder is a 2nd generation type transponder and uses the PIT protocol. It is compatible to the 1st generation protocol and offers the option of using a synchronization code scheme. Recause of this strengt all car manufacturary have implemented that are explained.</td> <td></td> <td></td> <td></td> <td></td> <td></td> | | PCF7930 | 125 kHz | R/W, 1024 | | transponder is a 2nd generation type transponder and uses the PIT protocol. It is compatible to the 1st generation protocol and offers the option of using a synchronization code scheme. Recause of this strengt all car manufacturary have implemented that are explained. | | | | | |
| N730 IA30 IA30 </td <td></td> <td></td> <td></td> <td></td> <td></td> <td>Write lock mechanism (reversible) [excluded block1]. Password (56 bits) to protect from writing (may be readable or not). This 1st</td> <td></td> <td></td> <td></td> <td>+++</td> <td></td> | | | | | | Write lock mechanism (reversible) [excluded block1]. Password (56 bits) to protect from writing (may be readable or not). This 1st | | | | +++ | |
| Namb Namb No. | | PCF/931 | 125 KHz | K/W, 1024 | | generation type transponder implements the read capabilities of the PIT protocol. As this transponder is OTP, there is no option of | | | | | |
| norm | | | | | | Write lock mechanism (reversible) [excluded block1]. Password (56 bits) to protect from writing (may be readable or not). Additional | | | | | |
| norm | | PCF/935 | 125 KHZ | K/W, 1152 | | snauow memory (not present in PGP731). It implements the SEG1 protocol which is a simple challenge/response protocol, using a not specified cipher. | | | | | |
| | | PCF7036 (Hitao2) | 125 KH2 | 2 | | 48 bit Secret Key and a random number in order to cipher any communication between the device and the basestation. EEPROM read/write protection features. This is the first HTAG2 transponder and does not have any THE canabilities. Hence, it is used early for | | | | | |
| Production Production </td <td></td> <td></td> <td>120 KHZ</td> <td></td> <td></td> <td>immobilizers. UID scheme: XX XX XX 1X.</td> <td></td> <td></td> <td></td> <td></td> <td></td> | | | 120 KHZ | | | immobilizers. UID scheme: XX XX XX 1X. | | | | | |
| Name | | | ? | ? | | ? | | | | | |
| Index Image: second se | | | ? | R/W, 448 Bytes | | | | _ | | | |
| NotationNotati | | | | <i>1</i> | | This transnowlar includes LIHE canabilities and a RISC Controller with a 4 kB ROM that is used to program keylass antru features | | | | | |
| Network | | | Remote keyless entry | 1 | | Transponders of this type are also termed "STARC lite" (Security Transponder and RISC Controller). | | _ | | | |
| Note Note </td <td></td> <td>PCF7942/43/44 (Hitag2)</td> <td>?</td> <td>?</td> <td></td> <td>features. Transponders of this type are also called "STARC" (Security Transponder and RISC Controller). UID scheme: XX XX XX 4X.</td> <td></td> <td></td> <td></td> <td></td> <td></td> | | PCF7942/43/44 (Hitag2) | ? | ? | | features. Transponders of this type are also called "STARC" (Security Transponder and RISC Controller). UID scheme: XX XX XX 4X. | | | | | |
| main | | PCF7945 (Hitag2) | Remote keyless entry | ? | | | | | | | |
| Image: state Image: state <t< td=""><td></td><td></td><td>2</td><td>7</td><td></td><td>In contrast to the STARC based transponders, this transponder does not have a RISC controller and instead features a built-in rolling</td><td></td><td></td><td></td><td></td><td></td></t<> | | | 2 | 7 | | In contrast to the STARC based transponders, this transponder does not have a RISC controller and instead features a built-in rolling | | | | | |
| Printing Name Printing | | | Kevless entru/on | 2 | | | | _ | | | |
| Non-Statistic | | | | ? | | This transponder is the first for keyless-go applications and again offers a RISC controller. UID scheme: XX XX XX 7X. ? | | _ | | | |
| Network Notice Notice Notice Notice Notice Notice Notice Notice Notice | | | | ? | | ? | | | | | |
| Non- | | | | ? | | ? | | | | | |
| Interstant Notation No | | | | ? | | ? | | _ | | | |
| Needed:< | | | Keyless entry/go 860~960MHz/2 45CHz | ? P/W 256 Bytes | 15018000 | ? Look mechanism (with protection) for each lute | | _ | | | |
| Index Mander | | | | | | 22-bit access password - 32-bit kill password | | _ | | | |
| | | | | | | 32-bit kill password to permanently disable the tag - 32-bit access password to allow a transition into the secured transmission state. | | | | | |
| | | ocode LPC G2 (SESICSIO) | 000~900 Miliz | N/W, 04 Bytes | 13018000 | | | | | | |
| | | UCode G2iL/+ (SL3S1203/1213) | 840~960 MHz | R/W, 128 Bits | | Private User Memory area protected by special User Password - Memory read protection - Tag tamper alarm - 32 bit Kill Password to permanently disable the tag - 32 bit Access Password to allow a transition into the secured state - 32 bit User Password to allow | | | | | |
| | | | | | | access to the private user memory segment - Read protection - BlockWrite (32 bit) - Write Lock - BlockPermalock. Private User Memory area protected by special User Password - Memory read protection - Tag tamper alarm - 32 bit Kill Password to | | _ | | | |
| | | UCode G2iM/+ (SL3S1003/1013) | 840~960 MHz | R/W, 256 Bits | | permanently disable the tag - 32 bit Access Password to allow a transition into the secured state - 32 bit User Password to allow access to the private user memory segment - Beed potential or BlockWite (32 bit) - Write Lock - BlockPermalock | | | | | |
| No. 2 1/2 3 2003/1 No. 4 000 mode No. 2 1/2 3 2000 mode No. 2 1/2 3 2000 mode No. 2 1/2 3 2000 mode No. 2 1/2 2000 mode< | | UCode G2XM (SL3ICS1002) | 860~960 MHz | R/W, EPC 240 Bit, TID 64 Bits | 15018000-6 | Read Protect: protects all memory content including CRC16 from unauthorized reading 32-bit kill password to permanently disable | | | | | |
| Note of the stand of the st | | | | | | Read Protect: protects all memory content including CRC16 from unauthorized reading 32-bit kill password to permanently disable | | _ | | | |
| NAME | | | | | | the tag - 32-bit access password to allow a transition into the secured transmission state. | | _ | | | |
| NAME | | | | | | 32-bit kill password to permanently disable the tag - 32-bit access password. Memory read protection - 32-bit KILL password to permanently disable the tag - 32-bit ACCESS password to allow a transition into the | | _ | | | |
| N1201 N0.10 Mpc D0.104100 Construction of the programments in the prog | | UCode I2C (SL354011/4021) | 860~960 MHz/12C | R/W, 3328 Bits | ISO18000-6 | secured transmission state. | | | | | |
| N1201 N12010 N120100 N120100 N120100 N120100 N120100 N120100000000000000000000000000 | | NTAG203/F | 13.56 MHz | R/W, 168 Bytes | ISO14443A | Field programmable read-only locking function per page for first 64 bytes - Field programmable read-only locking function per block - 32-bit user definable One-Time Programmable (OTP) area - 16-bit counter | | | | | |
| NA222 NA234 NA246 NA246 <td< td=""><td></td><td>NTAG210</td><td>13 56 MHz</td><td>P/W 80 Bytes</td><td>150144438</td><td>Capability container with one time programmable bits - Field programmable read-only locking function per page (per 2 pages for the</td><td></td><td></td><td></td><td></td><td></td></td<> | | NTAG210 | 13 56 MHz | P/W 80 Bytes | 150144438 | Capability container with one time programmable bits - Field programmable read-only locking function per page (per 2 pages for the | | | | | |
| NACCI 00000000000000000000000000000000000 | | | | | 13014443A | extended memory section) - ECC based originality signature - 32-bit password protection to prevent unauthorized memory operations. | | | | | |
| NACCI 00000000000000000000000000000000000 | | NTAG212 | 13.56 MHz | R/W, 164 Bytes | ISO14443A | Capability container with one time programmable bits - Heid programmable read-only locking function per page (per 2 pages for the extended memory section) - ECC based originality signature - 32-bit password protection to prevent unauthorized memory operations. | | | | | |
| NAC125219 No.90 bysic B01404 B014040 B0140400 B0140400 B014040 | | NTAG213 | 13.56 MHz | R/W. 180 Bytes | | Field programmable read-only locking function per page for the first 16 pages - Field programmable read-only locking function above | | | | | |
| NAC214/2197 State Mark No. 93 by types State Mark S | | | | | | me inst to pages per double page. Field programmable read-only locking function per page for the first 16 pages - Field programmable read-only locking function per 16 | | | | ++ | |
| NAC214/2197 State Mark No. 93 by types State Mark S | | NTAG215/215F | 13.56 MHz | R/W, 540 Bytes | ISO14443A | pages. Configurable password protection with optional limit of unsuccessful attempts - Anti-tearing support for capability container (CC) | | | | | |
| NTOX 150 MP | | | | | | Field programmable read-only locking function per page for the first 16 pages - Field programmable read-only locking function per 16 | | | | ++ | |
| NEXC 13.6 MP 7 150 (M = 10 | | NTAG216/216F | 13.56 MHz | K/W, 924 Bytes | ISO14443A | pages. Contigurable password protection with optional limit of unsuccessful attempts - Anti-tearing support for capability container (CC) and lock bits - ECC supported originality check. | | | | | |
| Prine ML256 Private Multication Private Multication < | | | | ??? | | | | | | | |
| Prine MIAD24 Ray March Mar | | NTP3xxx | 13.56 MHz | | | Encrypted data transmission and a high security due to unique authorisation concept. Individually programmable read/write protection | | - | | ++ | |
| Arc128W Ais PMI With 28 by Res Ais PMI | | | | | | | | | | | |
| Ancloame Condensity Condensity <thcondensity< th=""> Condensity</thcondensity<> | | | | R/W, 256 Bytes | LEGIC RF Standard (failed ISO14443F) | cryplography. | | | | | |
| ArC256W 3.05 MHz W, 25 Myz G10507 255, LEGL compton 98 Bit ophgraphic alleritation. A </td <td></td> <td>Prime MIM256</td> <td>13.56 MHz</td> <td></td> <td>LEGIC RF Standard (failed ISO14443F)</td> <td>on compagnition compatible with the containing become matching and the authoritation control and the containing the containini</td> <td></td> <td></td> <td></td> <td></td> <td></td> | | Prime MIM256 | 13.56 MHz | | LEGIC RF Standard (failed ISO14443F) | on compagnition compatible with the containing become matching and the authoritation control and the containing the containini | | | | | |
| ATCSBM 13.6 M2 NV, 26 Byts 15.0 Byts Bits Bits <t< td=""><td></td><td>Prime MIM256 Prime MIM1024</td><td>13.56 MHz 13.56 MHz</td><td>R/W, 1024 Bytes</td><td>LEGIC RF Standard (failed ISO14443F)</td><td>cryptography. Encrypted data transmission and a high security due to unique authorisation concept. Individually programmable read/write protection for each segment, compatible with the existing LEGIC infrastructure. Cards and readers cannot authenticate each other; lack of</td><td> </td><td> _</td><td></td><td></td><td></td></t<> | | Prime MIM256 Prime MIM1024 | 13.56 MHz 13.56 MHz | R/W, 1024 Bytes | LEGIC RF Standard (failed ISO14443F) | cryptography. Encrypted data transmission and a high security due to unique authorisation concept. Individually programmable read/write protection for each segment, compatible with the existing LEGIC infrastructure. Cards and readers cannot authenticate each other; lack of | | _ | | | |
| ATC3D4W 13.56 H4z NV, 512 Mgc G1010903 SDS, LGGC exploration, SBB (replopragine autheritation, SBB (replopragine) autheritation, SBB (replopragine autheritation, SBB (replopragine autheritation, SBB (replopragine) autheritation, SBB (replopragin | | Prime MIM256 Prime MIM1024 | 13.56 MHz 13.56 MHz | R/W, 1024 Bytes | LEGIC RF Standard (failed ISO14443F) | cryplography. The crypled games is a set of the security due to unique authorisation concept. Individually programmable read/write protection Encrypled gamest. compatible with the existing LEGIC infrastructure. Cards and readers cannot authenticate each other: lack of cryplography. | | | | | |
| ATC1024MV 13.56 MHz RVI, 104 Syste 1501563 0055, DE5, LEGC excryptor, 48 Bit cryptographic authentication. 0 < | | Prime MIM256 Prime MIM1024 ATC128MV | 13.56 MHz 13.56 MHz 13.56 MHz | R/W, 1024 Bytes R/W, 128 Bytes | LEGIC RF Standard (failed ISO14443F) ISO15693 | Indexast/M., Insumisation and a high nearly facto to invige authorization concept. Individually programmable easilymite protection Encyption generation compatible with the existing LEGIC infrastructure. Cards and readers cannot authenticate each other; tack of cryptography. 3DES, LEGIC encyption; 96 Bit cryptographic authentication. | | | | | |
| ATCOMM 305 MHz NV, 204 Byrds 105 MHZ 305 DSE, LEGC exception; 48 Bir optographic adherication. 0 | | Prime MIM356 Prime MIM1024 ATC128MV ATC256MV | 13.56 MHz 13.56 MHz 13.56 MHz 13.56 MHz | R/W, 1024 Bytes R/W, 128 Bytes R/W, 256 Bytes | LEGIC RF Standard (failed ISO14443F) ISO15693 ISO15693 | crybotacyby. Encrystel data mannission and a high security due to unique authorisation concept. Individually programmable read/write protection for programmable with the existing LEGIC initiativucture. Cards and readers cannot authenticate each other; luck of sportugation. 30ES, DES, LEGIC encryption: 96 Bit cryptographic authentication. 30ES, DES, LEGIC encryption: 96 Bit cryptographic authentication. | | | | | |
| ATC2048MV 13.56 Mtz NV, 2048 Bytes 1515630 Sp. DES, LEGC exception, 4B Exceptio | | Prime MIM256 Prime MIM1024 ATC128HV ATC256HV ATC256HV | 13.56 MHz 13.56 MHz 13.56 MHz 13.56 MHz 13.56 MHz | R/W, 1024 Bytes R/W, 128 Bytes R/W, 256 Bytes R/W, 512 Bytes | LEGIC RF Standard (failed ISO14443F) ISO15693 ISO15693 ISO15693 | crybotacyby. Encrystel data mannission and a high security due to unique authorisation concept. Individually programmable read/write protection for programmable with the existing LEGIC initiativucture. Cards and readers cannot authenticate each other; luck of sportugation. 30ES, DES, LEGIC encryption: 96 Bit cryptographic authentication. 30ES, DES, LEGIC encryption: 96 Bit cryptographic authentication. | | | | | |
| ATC4096W 3.56 MHz NV,009 Bytes 3150 State 3150 State NV,009 Bytes 3150 State 3150 State NV,009 Bytes 3150 State 3 | | Prime MIM256 Prime MIM1024 ATC128HV ATC256HV ATC256HV | 13.56 MHz 13.56 MHz 13.56 MHz 13.56 MHz 13.56 MHz | R/W, 1024 Bytes R/W, 128 Bytes R/W, 256 Bytes R/W, 512 Bytes | LEGIC RF Standard (failed ISO14443F) ISO15693 ISO15693 ISO15693 | vrybozachy, mennission and a high recently due to incluse authorisation concept. Individually programmable read/write protection forcypted dates of compatible with the existing LEGIC infrastructure. Cards and readers cannot authenticate each other; lock of crybography. 20ES, DES, LEGIC encryption; 98 Bit crybographic authentication. 20ES, DES, LEGIC encryption; 98 Bit crybographic authentication. 30ES, DES, LEGIC encryption; 94 Bit crybographic authentication. | | | | | |
| ATC12MP 13.56 Mtrz NV, 512 Pytes G100443 SDE, ELGE comptos ABI comptosaria: authentiation. G104143 G10444 | | Prime MIM256 Prime MIM1024 ATC128MV ATC325MV ATC512HV ATC1024MV | 13.56 MHz 13.56 MHz 13.56 MHz 13.56 MHz 13.56 MHz 13.56 MHz | R/W, 1024 Bytes R/W, 128 Bytes R/W, 256 Bytes R/W, 512 Bytes R/W, 1024 Bytes | LEGIC RF Standard (failed ISO14443F) ISO15693 ISO15693 ISO15693 ISO15693 ISO15693 | vrokozatyw, s warnisano nad a klyb ieszerki du bi vrojeze autorisation concept. Holidially programmable readvirte protection for schr segment compatible with the existing LEGIC infrastructure. Cards and readers cannol authenicate each other; lack of schrobazety. 30ES, DES, LEGIC encryption; 98 Bit cryptographic authenication. 30ES, DES, LEGIC encryption; 64 Bit cryptographic authenication. 30ES, DES, LEGIC encryption; 64 Bit cryptographic authenication. | | | | | |
| ATC204MP 13.56 MHz R/V. 1024 System 15014443 Displace thereoption to the optiopramic authentication. Image: Control optiopramic authentica | | Prime MIM256 Prime MIM1024 ATC128MV ATC128MV ATC512MV ATC1024MV ATC1024MV | 13.56 MHz 13.56 MHz 13.56 MHz 13.56 MHz 13.56 MHz 13.56 MHz 13.56 MHz | R/W, 1024 Bytes R/W, 128 Bytes R/W, 256 Bytes R/W, 512 Bytes R/W, 1024 Bytes R/W, 1024 Bytes | LEGIC RF Standard (falled ISO14443F) ISO15693 ISO15693 ISO15693 ISO15693 ISO15693 | In the second se | | | | | |
| ATC2048Ph ASS MHz RV, 208 Bytes ASS ML2 | | Prime MIM256 Prime MIM1024 ATC128MV ATC525MV ATC5252VV ATC1024MV ATC1024MV ATC2048MV ATC4096MV | 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 | R/W, 1024 Bytes R/W, 128 Bytes R/W, 256 Bytes R/W, 512 Bytes R/W, 1024 Bytes R/W, 2048 Bytes R/W, 2048 Bytes | LEGIC RF Standard (failed ISO14443F) ISO15693 ISO15693 ISO15693 ISO15693 ISO15693 ISO15693 ISO15693 | In the second se | | | | | |
| ATC2048Ph No. 2085, Visit, Line Herripartice aller infordazine | | Prime MIM256 Prime MIM1024 ATC128MV ATC525MV ATC5252VV ATC1024MV ATC1024MV ATC2048MV ATC4096MV | 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 | R/W, 1024 Bytes R/W, 128 Bytes R/W, 256 Bytes R/W, 512 Bytes R/W, 1024 Bytes R/W, 2048 Bytes R/W, 2048 Bytes | LEGIC RF Standard (failed ISO14443F) ISO15693 ISO15693 ISO15693 ISO15693 ISO15693 ISO15693 ISO15693 | In product and the second seco | | | | | |
| ATC4096MP 13.56 MHz R/W, 4096 Systes 15014443 DES, LEGC encrytion, 98 all cryptographic submittation. Image: Company Compa | | Prime MIM356 Prime MIM1024 ATC128MV ATC256MV ATC326MV ATC324MV ATC3204MV ATC32049MV ATC32049MV ATC32049MV ATC3224PP | 13.56 MHz 13.56 MHz 13.56 MHz 13.56 MHz 13.56 MHz 13.56 MHz 13.56 MHz 13.56 MHz | R/W, 1024 Bytes R/W, 128 Bytes R/W, 256 Bytes R/W, 256 Bytes R/W, 2048 Bytes R/W, 2048 Bytes R/W, 2049 Bytes R/W, 2049 Bytes R/W, 512 Bytes | LEGIC RF Standard (falled ISO14443F) ISO15693 ISO15693 ISO15693 ISO15693 ISO15693 ISO15693 ISO15693 ISO15693 | rynborazhy, sunemasion end a hyle neordy due to vinique autheniastic monest. Hidrideally programmable nesłwite protection for scha segmet compatible with the existing LEGIC infrastructure. Cards and readen cannot authenticate each other; tack of crynborazhy. 30ES, DES, LEGIC encryption; 98 Bit crynborashic authentication. 30ES, DES, LEGIC encryption; 94 Bit crynborashic authentication. | | | | | |
| ArS4095/P 13.56 MHz R/W, 4096 Bytes 15014443A ArS2052 Bit, SEG. Electro derrytiption auteritation. crC4096MP 13.56 MHz R/W, 4096 Bytes 15014443A/LEGIC RF Standard ArS2052 Bit, SEG. Electro derrytiption 12 di cryptographic auteritation. Image: Critical Standard Im | | Prime MIN256 Prime MIN1024 ATC128MV ATC256MV ATC556MV ATC522MV ATC2048MV ATC2048MV ATC2048MV ATC312MP ATC1024MP | 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 13.56 MHz | R/W, 1024 Bytes R/W, 128 Bytes R/W, 256 Bytes R/W, 512 Bytes R/W, 1024 Bytes R/W, 2048 Bytes R/W, 2059 Bytes R/W, 512 Bytes R/W, 1024 Bytes R/W, 1024 Bytes R/W, 1024 Bytes | LEGIC RF Standard (falled ISO14443F) ISO15693 ISO15693 ISO15693 ISO15693 ISO15693 ISO15693 ISO15693 ISO15693 ISO14443 | verbiogaziv, services and the set of the se | | | | | |
| AFS4096/P 13.56 MHz R/W, 4096 Bytes IS014443A AES (128256 B/l, 3065, DES, LEGC encryption, 112 Bit cryptographic authentication. CTC4096MP 13.56 MHz R/W, 1002/2964 Bytes IS014443A/LEGIC RF Standard AES (128256 B/l, 3065, DES, LEGC encryption, 112 Bit cryptographic authentication. Image: Company Co | | Prime MIM256 Prime MIM1024 ATC128MV ATC128MV ATC125MV ATC1024MV ATC1024MV ATC1024MP ATC1024MP ATC1024MP ATC1024MP | 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 13.56 MHz | R/W, 1024 Bytes R/W, 128 Bytes R/W, 256 Dytes R/W, 512 Bytes R/W, 1024 Bytes R/W, 4096 Bytes R/W, 4096 Bytes R/W, 1024 Bytes | LEGIC RF Standard (falled ISO14443F) ISO15693 ISO15693 ISO15693 ISO15693 ISO15693 ISO15693 ISO1693 ISO14443 ISO14443 | verbiogaziv, services and the set of the se | | | | | |
| CTC4096MP 13.56 MHz R/W, 1002/2984 Bytes ISO14443/LEGIC RF Standard AES (128/268 Bit), 30:ES, LEGIC encryption, 12 Bit cryptographic authentication. | | Prime MIM256 Prime MIM1024 ATC128MV ATC128MV ATC125MV ATC1024MV ATC1024MV ATC1024MP ATC1024MP ATC1024MP ATC1024MP | 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 13.56 MHz | R/W, 1024 Bytes R/W, 128 Bytes R/W, 256 Dytes R/W, 512 Bytes R/W, 1024 Bytes R/W, 4096 Bytes R/W, 4096 Bytes R/W, 1024 Bytes | LEGIC RF Standard (falled ISO14443F) ISO15693 ISO15693 ISO15693 ISO15693 ISO15693 ISO15693 ISO1693 ISO14443 ISO14443 | In Research, Service Constraints and an High security due to vince authorisation concept. Holidically programmable readwrite protocom for each segment compatible with the existing LEGIC infrastructure. Cards and readers cannot authenticale each other; lack of crystoparaty. 3DES, DES, LEGIC encryption; 96 Bit crystoparaphic authentication. 3DES, DES, LEGIC encryption; 64 Bit crystoparaphic authentication. | | | | | |
| NES (120/20 Bit), 30/25, LEGIC encryption. 112 Bit cryptographic authentication. | | Prime MIM256 Prime MIM1024 ATC128MV ATC125MV ATC152MV ATC1024MV ATC1024MV ATC1024MP ATC1024MP ATC10496MP ATC4096MP | 13.56 MHz 13.56 MHz | R/W, 1024 Bytes R/W, 128 Bytes R/W, 128 Bytes R/W, 512 Bytes R/W, 1024 Bytes R/W, 4096 Bytes R/W, 4096 Bytes R/W, 1024 Bytes R/W, 4096 Bytes R/W, 1024 Bytes R/W, 4096 Bytes R/W, 1024 Bytes R/W, 4096 Bytes | LEGIC RF Standard (falled ISO14443F) ISO15693 ISO15693 ISO15693 ISO15693 ISO15693 ISO16433 ISO14443 ISO14443 ISO14443 | vmborazhy, se managene en | | | | | |
| SLE 44K32/1/5 | | Риме MIM256 Риме MIM024 ATC128HV ATC256MV ATC256MV ATC322MV ATC324MV ATC3046MV ATC4096MV ATC324MP ATC3048MP ATC4096MP ATC4096MP ATC4096MP | 13.56 MHz 13.56 MHz | R/W, 1024 Bytes R/W, 128 Bytes R/W, 128 Bytes R/W, 256 Dytes R/W, 2048 Bytes R/W, 2048 Bytes R/W, 2048 Bytes R/W, 512 Bytes R/W, 1024 Bytes R/W, 1026 Bytes R/W, 4096 Bytes R/W, 4096 Bytes | LEGIC RF Standard (falled ISO1443F) ISO15693 ISO15693 ISO15693 ISO15693 ISO15693 ISO15693 ISO15693 ISO14443 ISO14443 ISO14443 ISO14443 | vmborazhy, monazh kaji kaji kasarih kaji kasarih duk bornique authoritation concept. Nahindanih programmable wath wire protocion for schi segment compatible with the existing LEGIC infrastructure. Cards and readers cannot authenticate each other; lack of schi borgent compatible with the existing LEGIC infrastructure. Cards and readers cannot authenticate each other; lack of SDES, DES, LEGIC encryption; 98 Bit cryptographic authentication. SDES, DES, LEGIC encryption; 94 Bit cryptographic authentication. | | | | | |
| | | Prime MIN256 Prime MIN1024 ATC128MV ATC256MV ATC356MV ATC326MV ATC326MV ATC3204MV ATC3204MV ATC4096MV ATC4096MP ATC4096MP ATC4096MP ATC4096MP ATC4096MP ATC4096MP | 13.56 MHz 13.56 MHz | R/W, 1024 Bytes R/W, 1024 Bytes R/W, 256 Bytes R/W, 256 Bytes R/W, 1024 Bytes R/W, 1026 Bytes R/W, 1026 Bytes R/W, 1026 Bytes R/W, 1024 Bytes R/W, 1024 Bytes R/W, 1024 Bytes R/W, 1024 Bytes | LEGIC RF Standard (falled ISO14443F) ISO15693 ISO15693 ISO15693 ISO15693 ISO15693 ISO15693 ISO15693 ISO14443 ISO14443 ISO14443 ISO14443 ISO14443A | vmboraphy. services and the set of the set | | | | | |

Manufacti

LEGIC

Infined

| | Type/Model Name | Frequency | Description | Standard/Notes | Security - 2-way authentication with 64-bit secret key between reader and card | | | | |
|---------------------|--|---|---|--|--|------|--|------|----|
| | | | | | - 2 keys for each sector allow hierarchical key management | | | | |
| | SLE 55R01 | 13.56 MHz | R/W, 160 bytes | ISO14443A | - Multi-level security structure possible - Individual access rights for each twy within a sector for each page - Only one sector can be opened at a time - Data intentive summer but high BPC / ISON 3000 and 32 hit MAC (effer subsection) - Data intentive summer but high BPC / ISON 3000 and 32 hit MAC (effer subsection) - Data intentive summer but high BPC / ISON 3000 and 32 hit MAC (effer subsection) - Data intentive summer but high BPC / ISON 3000 and 32 hit MAC (effer subsection) - Data intentive summer but high BPC / ISON 3000 and 32 hit MAC (effer subsection) - Data intentive summer but high BPC / ISON 3000 and 32 hit MAC (effer subsection) - Data intentive summer but high BPC / ISON 3000 and 32 hit MAC (effer subsection) - Data intentive summer but high BPC / ISON 3000 and 32 hit MAC (effer subsection) - Data intentive summer but high BPC / ISON 3000 and 32 hit MAC (effer subsection) - Data intentive summer but high BPC / ISON 3000 and 32 hit MAC (effer subsection) - Data intentive summer but high BPC / ISON 3000 and 32 hit MAC (effer subsection) - Data intentive summer but high BPC / ISON 3000 and 32 hit MAC (effer subsection) - Data intentive summer but high BPC / ISON 3000 and 32 hit MAC (effer subsection) - Data intentive summer but high BPC / ISON 3000 and 32 hit MAC (effer subsection) - Data intentive summer but high BPC / ISON 3000 and 32 hit MAC (effer subsection) - Data intentive summer but high BPC / ISON 3000 and 32 hit MAC (effer subsection) - Data intentive summer but high BPC / ISON 3000 and 32 hit MAC (effer subsection) - Data intentive summer but high BPC / ISON 3000 and 32 hit MAC (effer subsection) - Data intentive summer but high BPC / ISON 3000 and 32 hit MAC (effer subsection) - Data intentive summer but high BPC / ISON 3000 and 32 hit MAC (effer subsection) - Data intentive summer but high BPC / ISON 3000 and 32 hit MAC (effer subsection) - Data intentive summer but high BPC / ISON 3000 and 32 hit MAC (effer subsection) - Data intentive summer but high BPC / ISON 3000 and 32 hit MAC (| | | | |
| | | | | | Only one sector can be opened at at time One of the sector of the opened at a sector of the | | | | |
| | CIE FER04 | 12.55 101- | D.01/ 770 b. b. c | 100144404 | - 2 keys for each sector allow hierarchical key management - Multi-level security structure possible | | | | |
| | SLE 55R04 | 13.56 MHz | R/W, 770 bytes | ISO14443A | - Individual access rights for each key within a sector for each page - Only one sector can be opened at a time - Data integrity supported by 16 bit CRC (ISO 3309) and 32 bit MAC (after authentication) - Data integrity in the supported by 16 bit CRC (ISO 3309) and 32 bit MAC (after authentication) - Data integrity in the supported by 16 bit CRC (ISO 3309) and 32 bit MAC (after authentication) | | | | |
| | | | | | - Data integrity supported by 16 bit CRC (ISO 3309) and 32 bit MAC (after authentication) | | | | |
| | | | | | Access protection of EEPROM by transport keys on chip delivery Access protection of EEPROM by transport keys on chip delivery -2 way authentication with 64-bit secret key between reader and card -2 keys for each sector allow tearchicat key management | | | | |
| | | | | | 2 keys for each sector allow hierarchical key management Will level acquirity structure acquirity | | | | |
| | SLE 55R04E my-d™ prox-enhanced | 13.56 MHz | R/W, 6160 Bits | ISO14443A | Multi-level security structure possible Individual access rights for each key within a sector for each page | | | | |
| | | | | | Only one sector can be opened at a time Data integrity supported by 16 bit CBC (ISO 3300) and 32 bit MAC (after authentication) | | | | |
| | | | | | - Only one sector can be opened at a time - Data integrity supported by 15 bit CRC (ISO 3309) and 32 bit MAC (after authentication) - Access protection of EEPROM by transport keys on chip delivery - Avay authentication with 64-bit sect key between meder and card | | | | |
| | | | | | 2-way authentication with 64-bit secret key between reader and card 2 keys for each sector allow biararchical key management | | | | |
| | | | | | - 2 keys for each sector allow hierarchical key management - Multi-kevil security structure possible - Individual access rights for each key within a sector for each page | | | | |
| | SLE 55R08 | 13.56 MHz | R/W, 1280 bytes | ISO14443A | Individual access rights for each key within a sector for each page Only one sector can be opened at a time | | | | |
| | | | | | Only one sector can be opened at a time Data integrity supported by 16 bit CRC (ISO 3309) and 32 bit MAC (after authentication) | | | | |
| | | | | | Access protection of EEPROM by transport keys on chip delivery 2-way authentication with 64-bit server key between reader and card 2 keys for each sector allow therarchical key management | | | | |
| | | | | | 2 keys for each sector allow hierarchical key management Multi level security structure securities | | | | |
| | SLE 55R16 | 13.56 MHz | R/W, 2560 bytes | ISO14443A | Multi-level security structure possible Individual access rights for each key within a sector for each page | | | | |
| | | | | | Only one sector can be opened at a time Data integrity supported by 16 bit CRC (ISO 3309) and 32 bit MAC (after authentication) | | | | |
| | | | | | - Only one sector can be opened at a time - Data integrity supported by 16 bit (CR)(S0 3309) and 32 bit MAC (after authentication) - Access protection of EEFPROM by transport keys on chip delivery | | | | |
| | | | | | 2 keys for each sector allow hierarchical key management Multi-level security structure possible | | | | |
| | SLE 55R16E my-d™ prox-enhanced | 13.56 MHz | R/W. 20480 Bits | ISO14443A | Multi-level security structure possible Individual access rights for each key within a sector for each page | | | | |
| | SLE SSRIGE my-um prox-enhanced | 13.30 MHZ | R/W, 20480 Bits | 15014443A | Only one sector can be opened at a time | | | | |
| | | | | | - Only one sector can be opened at a time - Data integrity supported by 16 bit CRC (ISO 3309) and 32 bit MAC (after authentication) - Access protection of EEPROM by transport keys on chip delivery* | | | | |
| | SRF 55V01P my-d™ light | 13.56 MHz | R/W, 104 Bytes | ISO/IEC 18000-3 Mode 1 | Each block can be permanently locked against overwriting. | | | | |
| | SRF 55V02P my-d™ vicinity | 13.56 MHz | R/W, 256 bytes | ISO15693 | | | | | |
| | SRF 55V02P HC my-d™ vicinity | 13.56 MHz | R/W, 256 bytes | ISO15693 | | | | | |
| | SRF 55V02S my-d™ vicinity secure | 13.56 MHz | R/W, 256 bytes | IS015693 | Individual locking of blocks / pages (reast only) - State of The and Tabletoge and response security algorithm (mutual authentication) - Secietive memory access control of loc 1 to 4 sectors secured by authentication - xww, mutual authentication with 64-bit key (reght - 2 keys per sector allow herarchicat key management Multi-level security structure possible - 32-bit message authentication code (MAC) veryfing data access - Trinsport Key at olic divelow; | | | | ++ |
| | SRF 55V02S HC my-d [™] vicinity secure SRF 55V10P my-d [™] vicinity | 13.56 MHz 13.56 MHz | R/W, 256 bytes R/W, 1024 bytes | ISO15693 ISO15693 | Selective memory access control of up to 14 sectors secured by authentication - 2-way mutual authentication with 64-bit key length - 2 keys per sector allow hierarchical key management- Multi-level security structure possible - 32-bit message authentication onde (MAC) | | | | + |
| | SRF 55V10P my-d™ vicinity SRF 55V10P HC my-d™ vicinity | 13.56 MHz 13.56 MHz | R/W, 1024 bytes R/W, 1024 bytes | ISO15693 ISO15693 | verifying data access - Transport Key at chip delivery. | | | | ++ |
| | SRF 55V105 my-d™ vicinity secure | 13.56 MHz | R/W, 1024 bytes R/W, 1024 bytes | IS015693 | | | | | + |
| | SRF 55V10S HC my-d™ vicinity secure | 13.56 MHz | R/W, 1024 bytes | ISO15693 | | | | | |
| | SRF 66V10 PJM (Phase Jitter Modulation) | 13.56 MHz | R/W, 10K Bits | ISO/IEC 18000-3 | 48 bit password - Lockable chip memory. | | | | |
| | SLE 55x2 (5532/5542/5552) | contact only | R/W, 256 Bytes | ISO7816 | 48 bit password - Lockable chip memory. 5532: Write Protection - 5542: Write Protection+Programmable Security Code (PSC) - 5552: Write Protection+Read Protection+Programmable Security Code (PSC). | | | | |
| | SLE 55X8 | contact only | R/W, 1024 Bytes | IS7816 | · | | | | |
| | SLE 66R01P/PN my-d™ move (PN is already NFC initialized) | | R/W, 152 Bytes | ISO14443A | 32 bit of One Time Programmable (OTP) memory area | | | | |
| | SLE 66R01P/PN my-d [™] move (PN is already NFC initialized) | 13.56 MHz | R/W, 152 Bytes | ISO14443A | Locking mechanism for each block | | | | |
| | SLE 66R04P my-d™ NFC | 13.56 MHz | R/W, 616 Bytes | ISO14443A | Block Lock mechanism Online 13 bit Desement for Read/Write or Write access | | | | |
| | SLE 66R16P my-d™ NFC | 13.56 MHz | R/W, 2048 Bytes | ISO14443A | Optional 25th Password for Read/Write or Write access Optional Password Retry Counter | | | | |
| | SLE 66R32P my-d™ NFC SLE 66R04S my-d™ proximity 2 | 13.56 MHz 13.56 MHz | R/W, 4096 bytes R/W, 512 bytes | ISO14443A ISO14443A | Optional 16 bit Value Counter - State-of-the-art challenge and response security algorithm - avay mutual authentication with 64-bit secret key between reader and card for basic security | | | | |
| | SLE 66R16S my-d™ proximity 2 | 13.56 MHz | R/W, 2048 bytes | IS014443A | 2-way mutual authentication with 64-bit secret key between reader and card for basic security | | | | |
| | SLE 66R32S my-d™ proximity 2 | 13.56 MHz | R/W, 4096 bytes | ISO14443A | 2 keys for actin sector enable hierarchical key management - Multi-level security structure possible | | | | |
| | SLE 66R35 (Mifare compatible 4Bytes Unique UID) | 13.56 MHz | R/W, 1K Bytes | ISO14443A | Mutual three-pass authentication between card and reader for basic security | | | | |
| | SLE 66R35I (Mifare compatible 4Bytes non-unique UID) | 13.56 MHz | R/W, 1K Bytes | ISO14443A | - 48-bit key length - 2 keys per sector enabling key management | | | | |
| | SLE 66R35R (Mifare compatible 4Bytes Reused UID) | 13.56 MHz | R/W, 1K Bytes | ISO14443A | Transport key at chip delivery Selective memory access secured by authentication and access conditions | | | | |
| | SLE 66R35E7 (Mifare compatible 7Bytes UID) | 13.56 MHz | R/W, 1K Bytes | ISO14443A | - Certified True Random Number Generator with firmware test function supporting AIS-31 requirements | | | | |
| | | | | | - Dual Key Triple DES (DDES) Accelerator | | | | |
| | SLE 66CLXXPE (security IC / Crypto) | 13.56 MHz | R/W, 4K/8K/16K/18K/36K/78K/80K Bytes | ISO14443A/B+contact | - Advanced Crypto Engine with support of: - Up to 1100-bit RSA calculation in Hardware - Up to 2048-bit RSA calculation via fast and secure RSA 2048 crypto library (CC EAL5+ already certified with SLE66CX360PE) - Eliptic Curves over GF(p) - Eliptic Curves over GF(p) | | | | |
| | SLE 77CLFxxxP | 13.56 MHz | up to 100 | ISO14443+contact | | | | | |
| | SLE 77CLFXxxP | 13.56 MHz | up to 240K | ISO14443+contact | | | | | |
| | SLE 77CLF81CIP | 13.56 MHz | up to 16K | ISO14443+contact | | | | | |
| | SLE 66CL81TRM4 | | up to 8K | ISO14443 | | | | | |
| | SRF66V10IT | 13.56 MHz | R/W, 10K Bits | ISO/IEC 18000-3 Mode compliant | Lockable chip memory to prevent overwriting of user or manufacturer selected defined area - Optional 48 bit password protection to | | | | |
| | SRF66V10ST | 13.56 MHz | R/W, 10K Bits | ISO/IEC 18000-3 Mode 2 | prevent unauthorised write to memory | | | | |
| | | | | | | | | | |
| | SRF66V01ST | 13.56 MHz | R/W, 1280 Bits | ISO/IEC 18000-3 Mode 2 | ? | | | | |
| | SR176 | 13.56 MHz | R/W, 176 Bits | ISO14443B | Blocks from 4 to 15 can be write protected (blocks from 0 to 3 are ROM) in groups of 2 blocks; write access is controlled by the 8 Bits of the OTP_LOCK_REG register located at block address 0F. Once protected these blocks (4 to 15) cannot be unprotected. Blocks can be write protected; write access is controlled by the 8 Bits of the OTP_LOCK_REG register located at block address FF. | | | | |
| | | | | | | | | | |
| | SRI512 | | | | Blocks can be write protected; write access is controlled by the 8 Bits of the OTP_LOCK_REG register located at block address FF. | | | | |
| | | 13.56 MHz | R/W, 512 Bits | ISO14443B | Blocks can be write protected; write access is controlled by the 8 Bits of the OTP_LOCK_REG register located at block address FF. Once protected these blocks cannot be unprotected. 2 Count-Down Binary Counters with automated anti-tearing protection (a renteded counter block behaves like a ROM block) | | | | |
| | | 13.56 MHz | R/W, 512 Bits | | Once protected these blocks cannot be unprotected. 2 Count-Down Binary Counters with automated anti-tearing protection (a protected counter block behaves like a ROM block). Bindre can be write protected write access is controlled by the 8 Bite of the OTE LOCK_PEG register located at block address EE | | | | _ |
| | SRIX512 | 13.56 MHz 13.56 MHz | R/W, 512 Bits R/W, 512 Bits | ISO14443B ISO14443B | Once protected these blocks cannot be unprotected. 2 Count-Down Binary Counters with automated anti-tearing protection (a protected counter block behaves like a ROM block). Bindre can be write protected write access is controlled by the 8 Bite of the OTE LOCK_PEG register located at block address EE | | | | |
| | SRIX512 | | | | Does protected these blocks cannot be unprotected. Zount Doem Rinery Counters with automated anti-bearing protection (a Books can be write protected, write accesses is controled by the Bio of the orTL LOCRE (Ceregistre located at block address FF. Once protected these blocks cannot be unprotected. These bio of the ort BL control and the and the start and the start of the start | | | | |
| | SRIX512 SRI2K | | | | Once protected these blocks cannot be unprotected. 2 Count-Down Binary Counters with automated anti-testing protection (a protected counter) which behaves the SAO block), and the SAO block of the SAO block of the SB bits of the OFP. LOCK, REC register located at block advises RF. Once protected these blocks cannot be unprotected. Possible mutual authentication with specific reader (provided with CRX14 day) proprietienty agointym. 2 Count-Down Binary Counters (blocks 5 and 6) with automated anti-testing protection (a protected counter and the start of th | | | | |
| | | 13.56 MHz | R/W, 512 Bits | ISO14443B | Done protected these block cannot be unprotected. Z Count-Done Thenry Counters with automated anti-bearing protection (a Books can be write protected, write access is controlled by the SB for dh tor TL COURCE orgenito rectard at block address FF. Done protected these blocks cannot be unprotected. These blocks and the start and the sta | | | | |
| | | 13.56 MHz | R/W, 512 Bits | ISO14443B | Once protected these block cannot be unprotected. 2 Count-Down Rhang Counters with automated anti-learing protection (a protected counter block cherws tills a CAU block). All your is Bio of the OTT_LOCE, CEGE torgetion tectores and a block address FF. Blocks can be write protected, write access is control the Paylities multial authentication with specific reader (provided with CRX14 chip - proprietary algorithm). Zound-Down Briany Counters (blocks 5 and 6) with automated anti-learing protection (a protected counter block behaves like a RCM block). | | | | |
| | SRIZK SRI4K | 13.56 MHz 13.56 MHz 13.56 MHz | R/W, 512 Bits R/W, 1024 Bits R/W, 4096 Bits | ISO144438 ISO144438 ISO144438 | Once protected these block cannot be unprotected. 2 Count-Down Rinary Counters with automated anti-learing protection (a protected counter block before tills a CAL block), and by the BIG of the OTT-LOCK, REG register tocated at block adverses FF. Once protected these blocks cannot be unprotected. Possible mutual authentication with specific reader (provided with CRX14 Ontp- operised) and the counter block cannot be unprotected. Possible mutual authentication with specific reader (provided with CRX14 Ontp- operised) and the counter block cannot be unprotected. Possible mutual authentication with specific reader (provided with CRX14 Ontp- block behaves like a ROM block). Block lime / h IS can be write protected with accounts is controlled by the B Bib of the OTP_LOCK, REG register boated at block address FF. Once protected these blocks (7 to 15) cannot be unprotected. 2 Count-Down Binary Counters with automated at block address FF. Once protected these blocks (7 to 15) cannot be unprotected. 2 Count-Down Binary Counters with automated at block address FF. Once protected these blocks (7 to 15) cannot be unprotected. 2 Count-Down Binary Counters with automated anti-learing protection. | | | | |
| | SRI2K | 13.56 MHz 13.56 MHz | R/W, 512 Bits R/W, 1024 Bits | ISO14443B ISO14443B | Once protected these block cannot be unprotected. 2 Count-Down Rinary Counters with automated anti-learing protection (a protected counter block before tills a CAL block), and by the BIG of the OTT-LOCK, REG register tocated at block adverses FF. Once protected these blocks cannot be unprotected. Possible mutual authentication with specific reader (provided with CRX14 Ontp- operised) and the counter block cannot be unprotected. Possible mutual authentication with specific reader (provided with CRX14 Ontp- operised) and the counter block cannot be unprotected. Possible mutual authentication with specific reader (provided with CRX14 Ontp- block behaves like a ROM block). Block lime / h IS can be write protected with accounts is controlled by the B Bib of the OTP_LOCK, REG register boated at block address FF. Once protected these blocks (7 to 15) cannot be unprotected. 2 Count-Down Binary Counters with automated at block address FF. Once protected these blocks (7 to 15) cannot be unprotected. 2 Count-Down Binary Counters with automated at block address FF. Once protected these blocks (7 to 15) cannot be unprotected. 2 Count-Down Binary Counters with automated anti-learing protection. | | | | |
| | SRIZK SRIAK SRIX4K | 13.56 MHz 13.56 MHz 13.56 MHz 13.56 MHz | R/W, 512 Bits R/W, 1024 Bits R/W, 4096 Bits R/W, 4096 Bits | IS0144438 IS0144438 IS0144438 IS0144438 | Once protected these block cannot be unprotected. 2 Count-Down Rinary Counters with automated anti-learing protection (a protected counter block before tills a CAL block), and by the BIG of the OTT-LOCK, REG register tocated at block adverses FF. Once protected these blocks cannot be unprotected. Possible mutual authentication with specific reader (provided with CRX14 Ontp- operised) and the counter block cannot be unprotected. Possible mutual authentication with specific reader (provided with CRX14 Ontp- operised) and the counter block cannot be unprotected. Possible mutual authentication with specific reader (provided with CRX14 Ontp- block behaves like a ROM block). Block lime / h IS can be write protected with accounts is controlled by the B Bib of the OTP_LOCK, REG register boated at block address FF. Once protected these blocks (7 to 15) cannot be unprotected. 2 Count-Down Binary Counters with automated at block address FF. Once protected these blocks (7 to 15) cannot be unprotected. 2 Count-Down Binary Counters with automated at block address FF. Once protected these blocks (7 to 15) cannot be unprotected. 2 Count-Down Binary Counters with automated anti-learing protection. | | | | |
| | SRIZK SRI4K | 13.56 MHz 13.56 MHz 13.56 MHz | R/W, 512 Bits R/W, 1024 Bits R/W, 4096 Bits | ISO144438 ISO144438 ISO144438 | Done protected These block cannot be unprotected. 2 Count-Down Theory Counters with automated anti-bearing protection (a Books can be wire protected, with accesses is controlled by the Bits of the OTP_LOCK_REG register located at block address FF. Once protected These blocks cannot be unprotected. These bits of the OTP_LOCK_REG register located at block address FF. Done protected these blocks cannot be unprotected. These bits of the OTP_LOCK_REG register located at block address FF. Blocks from 7 to 15 can be wine protected, with access as controlled by the Bits of the OTP_LOCK_REG register located at block address FF. One protected these blocks (1 for 15 cannot be winnotected. 2 Count-Dom Binary Counters) with automated anti-bearing protection. 7 to 15 can be wine protected, wine access as controlled by the Bits of the OTP_LOCK_REG register located at block address FF. One protected these blocks (1 for 15 cannot be winnotected. 2 Count-Dom Binary Counters with automated anti-bearing protection. 7 to 15 can be wine protected, the start boroked. 2 Count-Dom Binary Counters with automated at hearing protection. 7 to 15 can be wine protected (1 for 15 cannot be winnotected. 2 Count-Dom Binary Counters with automated at hearing protection. 7 to 15 can be wing protected (1 for 15 cannot be winnotected. 2 Count-Dom Binary Counters with automated at hearing protection. 7 to 15 can be wing protected (1 for 15 cannot be winnotected. 2 Count-Dom Binary Counters with automated at hearing protection. 7 to 5 can be wing protected (1 for 15 cannot be winnotected. 2 Count-Dom Binary Counters with automated at hearing protection. 7 to 5 can be wing protected (1 for 15 cannot be wing protected) with a block and balance thereing bits of the protected at block address FF. Blocks can be wing protected with scokes as controlied by the Bits of the OTP_LOCK, REG register located at block address FF. Once protected with scokes as control bits by the Bits of the OTP_LOCK, REG register located at block address FF. Once p | | | | |
| | SRI2K SRIAK SRIXAK SRI512 | 13.56 MHz 13.56 MHz 13.56 MHz 13.56 MHz 13.56 MHz 13.56 MHz | R/W, 512 Bits R/W, 1024 Bits R/W, 4096 Bits R/W, 4096 Bits R/W, 512 Bitss | IS0144438 IS0144438 IS0144438 IS0144438 IS0144438 IS0144438 | Done protected these blocks cannot be unprotected. 2 Count-Down Rinery Counters with automated anti-bearing protection (a Books can be wire protection, with accounts be unprotected. The Statistic Counters with automated anti-bearing protection (a proprintical your section) and the statistical section of statistical sectistical section of statistical sectistica | | | | |
| | SRIZK SRIAK SRIX4K | 13.56 MHz 13.56 MHz 13.56 MHz 13.56 MHz | R/W, 512 Bits R/W, 1024 Bits R/W, 4096 Bits R/W, 4096 Bits | IS0144438 IS0144438 IS0144438 IS0144438 | Done protected these blocks cannot be unprotected. 2 Count-Down Rinery Counters with automated anti-bearing protection (a Books can be wire protection, with accounts be unprotected. The Statistic Counters with automated anti-bearing protection (a proprintical your section) and the statistical section of statistical sectistical section of statistical sectistica | | | | |
| | SRI2K SRI4K SRI512 SRI512 IRI64 | 13.56 MHz 13.56 MHz 13.56 MHz 13.56 MHz 13.56 MHz 13.56 MHz | R/W, 512 Bits R/W, 1024 Bits R/W, 4096 Bits R/W, 4096 Bits R/W, 512 Bitss R/W, 120 Bits (UID) | IS0144438 IS0144438 IS0144438 IS0144438 IS0144438 IS0144438 IS015693 with WORM User Area | Done protected These block cannot be unprotected. 2 Count-Down Thany Counters with automated anti-bearing protection (a Books can be with protected, with accesses is controlled by the Bits of the OTP_LOCK_REG register located at block address FF. Once protected These blocks cannot be unprotected. These bits of the OTP_LOCK_REG register located at block address FF. Done protected These blocks cannot be unprotected. These bits of the OTP_LOCK_REG register located at block address FF. Blocks from 7 to 15 can be with protected, with access as controlled by the Bits of the OTP_LOCK_REG register located at block address FF. Done protected These blocks cannot be unprotected. To 15 cannot be unprotected. 2 Count-Don Binary Counters minimation and the address FF. Done protected These blocks (T 16 15 cannot be unprotected. 2 Count-Don Binary Counters minimation and the address FF. Done protected These blocks (T 16 15 cannot be unprotected. 2 Count-Don Binary Counters minimation and the address FF. Done protected These blocks (T 16 15 cannot be unprotected. 2 Count-Don Binary Counters minimation and the address FF. Done protected These blocks (T 16 15 cannot be unprotected. 2 Count-Don Binary Counters minimation and the address FF. Done protected These blocks (T 16 15 cannot be unprotected. 2 Count-Don Binary Counters minimation and the address FF. Done protected these blocks is controlled by the Bits of the OTP_LOCK, REG register located at block address FF. Done protected with colocks is controlled by the Bits of the OTP_LOCK, REG register located at block address FF. Done protected with colock is control by the Bits of the OTP_LOCK, REG register located at block address FF. Done protected with colock is control by the Bits of the OTP_LOCK, REG register located at block address FF. Done protected with colock is an environ with the Bits of the OTP_LOCK REG register located at block address FF. Done protected with colock address FF. Done protected with colock address FF. Done protected with colock addres | | | | |
| | SRI2K SRIAK SRIXAK SRI512 | 13.56 MHz 13.56 MHz 13.56 MHz 13.56 MHz 13.56 MHz 13.56 MHz | R/W, 512 Bits R/W, 1024 Bits R/W, 4096 Bits R/W, 4096 Bits R/W, 512 Bitss | IS0144438 IS0144438 IS0144438 IS0144438 IS0144438 IS0144438 | Done protected these blocks cannot be unprotected. Z Count-Down Rhany Counters with automated anti-bearing protection (a Books can be write protected, with accesses is controlled by the Bits of the OTP_LOCK, REG register located at block address FF. Once protected these blocks cannot be unprotected. The shall be multial automatication with specific reader (provided with CRX14 day), protected writes the shall be controlled by the Bits of the OTP_LOCK, REG register located at block address FF. Bits of the DTP to | | | | |
| ST Microelectronics | SRI2K SRI4K SRI512 SRI512 IRI64 | 13.56 MHz 13.56 MHz 13.56 MHz 13.56 MHz 13.56 MHz 13.56 MHz | R/W, 512 Bits R/W, 1024 Bits R/W, 4096 Bits R/W, 4096 Bits R/W, 512 Bitss R/W, 120 Bits (UID) | IS0144438 IS0144438 IS0144438 IS0144438 IS0144438 IS0144438 IS015693 with WORM User Area | Done protected These block cannot be unprotected. 2 Count-Down Thany Counters with automated anti-bearing protection (a Books can be with protected, with accesses is controlled by the Bits of the OTP_LOCK_REG register located at block address FF. Once protected These blocks cannot be unprotected. These bits of the OTP_LOCK_REG register located at block address FF. Done protected These blocks cannot be unprotected. These bits of the OTP_LOCK_REG register located at block address FF. Blocks from 7 to 15 can be with protected, with access as controlled by the Bits of the OTP_LOCK_REG register located at block address FF. Done protected These blocks cannot be unprotected. To 15 cannot be unprotected. 2 Count-Don Binary Counters minimation and the address FF. Done protected These blocks (T 16 15 cannot be unprotected. 2 Count-Don Binary Counters minimation and the address FF. Done protected These blocks (T 16 15 cannot be unprotected. 2 Count-Don Binary Counters minimation and the address FF. Done protected These blocks (T 16 15 cannot be unprotected. 2 Count-Don Binary Counters minimation and the address FF. Done protected These blocks (T 16 15 cannot be unprotected. 2 Count-Don Binary Counters minimation and the address FF. Done protected These blocks (T 16 15 cannot be unprotected. 2 Count-Don Binary Counters minimation and the address FF. Done protected these blocks is controlled by the Bits of the OTP_LOCK, REG register located at block address FF. Done protected with colocks is controlled by the Bits of the OTP_LOCK, REG register located at block address FF. Done protected with colock is control by the Bits of the OTP_LOCK, REG register located at block address FF. Done protected with colock is control by the Bits of the OTP_LOCK, REG register located at block address FF. Done protected with colock is an environ with the Bits of the OTP_LOCK REG register located at block address FF. Done protected with colock address FF. Done protected with colock address FF. Done protected with colock addres | | | | |
| ST Microelectronics | SRI2K SRIMK SRIMK SRIMK SRT512 LRI64 LRI564K LRI1K | 13.56 MHz | R/W, 512 Bits R/W, 1024 Bits R/W, 1024 Bits R/W, 4096 Bits R/W, 512 Bits R/W, 512 Bits R/W, 512 Bits R/W, 512 Bits R/W, 120 Bits (UID) R/W, 64K+120 Bits (UID) R/W, 1024 Bits | IS0144438 IS0144438 IS0144438 IS0144438 IS0144438 IS015693 with WORM User Area IS015693 with WORM User Area | Done protected these block cannot be unprotected. Zount-Down Rinery Counters with automated anti-kerning protection (a Books can be with protected, with accesses is controlled by the Bits of the OTP_LOCK_REG register located at block address FF. Done protected misses block cannot be unprotected. The source and by the automated and kerning protection (a Books can be with protected, with accesses a controlled by the Bits of the OTP_LOCK_REG register located at block address FF. One protected miss accesses a control on the protected. Zourt Down Binary Counters with automated and hearing protection of the Distribution of t | | | | |
| ST Microelectronics | SRIZK SRIAK SRIXAK SRT512 LRI64 LRI564K | 13.56 MHz | R/W, 512 Bits R/W, 1024 Bits R/W, 4096 Bits R/W, 4096 Bits R/W, 512 Bitss R/W, 120 Bits (UID) R/W, 64K+120 Bits (UID) | IS014443B IS0144438 IS0144438 IS0144438 IS0144438 IS0144438 IS0144438 IS015693 with WORM User Area | Done protected these blocks cannot be unprotected. Zount Down Rhany Counters with automated anti-kerning protection (a Books can be with protected, with accesses is controled by the Bits of the OTP_LOCK_REG register located a block address FF. Once protected these blocks cannot be unprotected. The shall be multial authentication with specific reader (provided with CRX14 day) – days and the shall be approved by the shall be multiple of the Shall be | | | | |
| ST Microelectronics | SRI2K SRIMK SRIMK SRIMK SRT512 LRI64 LRI564K LRI1K | 13.56 MHz | R/W, 512 Bits R/W, 1024 Bits R/W, 1024 Bits R/W, 4096 Bits R/W, 512 Bits R/W, 512 Bits R/W, 512 Bits R/W, 120 Bits (UID) R/W, 64K+120 Bits (UID) R/W, 64K+120 Bits | IS0144438 IS0144438 IS0144438 IS0144438 IS0144438 IS015693 with WORM User Area IS015693 with WORM User Area | Done protected these blocks cannot be unprotected. Zocark Down Rhany Counters with automated anti-kerning protection (a Books can be write protection, with access the counters) with a soft and the soft of the CPL CPC REG register located at block at block can be write protection, with access the counters blocks and the share protection of a Books and be write protection. With access the counters blocks and the share protection of the soft and the share and the soft access the soft access the soft access the soft access the soft access the soft access the soft access the soft acc | | | | |
| ST Microelectronics | SRI2K SRIMK SRIMK SRIMK SRT512 LRI64 LRI564K LRI1K | 13.56 MHz | R/W, 512 Bits R/W, 1024 Bits R/W, 1024 Bits R/W, 4096 Bits R/W, 512 Bits R/W, 512 Bits R/W, 512 Bits R/W, 120 Bits (UID) R/W, 64K+120 Bits (UID) R/W, 64K+120 Bits | IS0144438 IS0144438 IS0144438 IS0144438 IS0144438 IS015693 with WORM User Area IS015693 with WORM User Area | Done protected these blocks cannot be unprotected. Count-Bow Rev Counters with automated anti-bearing protection (a Books can be write protection, with access the counters) with automated anti-bearing protection (a Books can be write protection, with access the counters) with a Bio of the OTP_LOCK_REG register located at block atdeses FF. Once protection with access the counters blocks and the shared protection of the shared protection (a block bearing with a short the short bear protected. The short bearing protection (a protection of the short of the short bearing the short bearing protection (b protection of the short bearing protected at block address FF. Blocks from 7 to 15 can be write protected, write access a controlled by the Bibs of the OTP_LOCK_REG register located at block address FF. Once protected these blocks and the short bearing protected at a Blocks Biorn 7 to 15 can be write protected, write access a controlled by the Bibs of the OTP_LOCK_REG register located at block address FF. Once protected these blocks and the short bearing protected at block address FF. Once protected these blocks and the short bearing protection (b blocks Biorn 7 to 15 can be write protected, write access as controlled by the B Bibs of the OTP_LOCK_REG register located at block address FF. Once protected these blocks and the supreticed. To short bearing write protection (b Blocks Biorn 7 to 15 can be write protected, write access as controlled by the B Bibs of the OTP_LOCK_REG register located at block address FF. Once protected these blocks cannot be unprotected. To short bearing and address FF. Blocks and the short short write and write access, the blocks and the unprotected. To short short write material and address BF. Blocks from 10 to 14 are write once read many (WORM) memory, it is possible to write to scale of them conce, after the fift valid write access. Be bloc | | | | |
| ST Microelectronics | SRI2K SRI4K SRIX4K SRI512 LRI64 LRI564K LRI564K LRI564 | 13.56 MHz | R/W, 512 Bits R/W, 1024 Bits R/W, 4096 Bits R/W, 4096 Bits R/W, 4096 Bits R/W, 202 Bits (UID) R/W, 64K+120 Bits (UID) R/W, 1024 Bits R/W, 2048 Bits | IS014443B IS014443B IS014443B IS014443B IS014443B IS014443B IS014443B IS014443B IS014443B IS015693 with WORM User Area IS015693 IS015693 | Done protected these blocks cannot be unprotected. Count-Bow Rev Counters with automated anti-bearing protection (a Books can be write protection, with access the counters) with automated anti-bearing protection (a Books can be write protection, with access the counters) with a Bio of the OTP_LOCK_REG register located at block atdeses FF. Once protection with access the counters blocks and the shared protection of the shared protection (a block bearing with a short the short bear protected. The short bearing protection (a protection of the short of the short bearing the short bearing protection (b protection of the short bearing protected at block address FF. Blocks from 7 to 15 can be write protected, write access a controlled by the Bibs of the OTP_LOCK_REG register located at block address FF. Once protected these blocks and the short bearing protected at a Blocks Biorn 7 to 15 can be write protected, write access a controlled by the Bibs of the OTP_LOCK_REG register located at block address FF. Once protected these blocks and the short bearing protected at block address FF. Once protected these blocks and the short bearing protection (b blocks Biorn 7 to 15 can be write protected, write access as controlled by the B Bibs of the OTP_LOCK_REG register located at block address FF. Once protected these blocks and the supreticed. To short bearing write protection (b Blocks Biorn 7 to 15 can be write protected, write access as controlled by the B Bibs of the OTP_LOCK_REG register located at block address FF. Once protected these blocks cannot be unprotected. To short bearing and address FF. Blocks and the short short write and write access, the blocks and the unprotected. To short short write material and address BF. Blocks from 10 to 14 are write once read many (WORM) memory, it is possible to write to scale of them conce, after the fift valid write access. Be bloc | | | | |
| ST Microelectronics | SRI2K SRIAK SRIXAK SRITS12 LRI564 LRIS5AK LRI1K LRIXK LRIXK | 13.56 MHz | R/W, 512 Bits R/W, 1024 Bits R/W, 4096 Bits R/W, 4096 Bits R/W, 4096 Bits R/W, 202 Bits (UID) R/W, 64K+120 Bits (UID) R/W, 1024 Bits R/W, 2048 Bits | ISO14443B ISO14443B ISO14443B ISO14443B ISO14443B ISO15693 with WORM User Area ISO15693 with WORM User Area ISO15693 | Done protected these blocks cannot be unprotected. Zouth Down Rhang Counters with automated anti-bearing protection (a Books can be write protected, with access is controlled by the BB in of the OTP_LOCK_REG register located at block address FF. Once protected these blocks cannot be unprotected. The south and automated anti-bearing protection (a protected these blocks cannot be unprotected. The south and automated anti-bearing protection (a protected these blocks cannot be unprotected. The south and automated anti-bearing protection (a protected these blocks cannot be unprotected. The south and automated anti-bearing protection (a protected these blocks cannot be unprotected. The south and the south and automated anti- bearing protected these blocks (a protected these blocks) (b 15) (c protected these blocks) (c protected these blocks) (c protected these blocks) (b 15) (c protected these blocks) (c pr | | | | |
| ST Microelectronics | SRI2K SRI4K SRIX4K SRI512 LRI64 LRI564K LRI1K LRI2K LRI2K LRI52K | 13.56 MHz | R/W, 512 Bits R/W, 1024 Bits R/W, 1024 Bits R/W, 4096 Bits R/W, 512 Bits R/W, 64K+120 Bits (UID) R/W, 2048 Bits R/W, 2048 Bits | IS0144438 IS0144438 IS0144438 IS0144438 IS0144438 IS015693 with WORM User Area IS015693 with WORM User Area IS015693 IS015693 IS015693 IS015693 | Done protected these block cannot be unprotected. 2 Count-Down Rinery Counters with automated anti-kerning protection (a Books can be with protected, with accesses is controlled by the Bills of the OTP_LOCK, REG register located at block address FF. Done protected these blocks cannot be unprotected. The shall be multi-automatic and the sharing protection (a protected these blocks cannot be unprotected. The shall be multi-automatic and the sharing protection (a protected these blocks cannot be unprotected. The shall be multi-automatic and the sharing protection (a protected these blocks cannot be unprotected. The shall be multi-automatic and the sharing protection (a protected these blocks) (b 16) (a most be unprotected. 2 Count-Doom Billany Counters with automated anti-kerning protection. 71 to 15 can be write protected, write access as controlled by the Bills of the OTP_LOCK, REG register located at block address FT. One protected these blocks (1 fo 15) cannot be unprotected. 2 Count-Doom Bilany Counters with automated anti-kerning protection. 71 to 15 can be write protected, write access as controlled by the Bills of the OTP_LOCK, REG register located at block address FT. One protected these blocks (1 fo 15) cannot be unprotected. 2 Count-Doom Binary Counters with automated anti-kerning protection. 71 to 15 can be write protected, 1 for 15 cannot be unprotected. 2 Count-Doom Binary Counters with automated anti-kerning protection. 71 bills cannot be unprotected. The shall be address Bills of the OTP_LOCK, REG register located at block address FT. One protected these blocks cannot be unprotected. 2 Count-Down Bilany Counters with automated anti-kerning protection. 71 bills cannot be address Bills of Bills (2 Bills Bi | | | | |
| ST Microelectronics | SRI2K SRIAK SRIXAK SRITS12 LRI564 LRIS5AK LRI1K LRIXK LRIXK | 13.56 MHz | R/W, 512 Bits R/W, 1024 Bits R/W, 4096 Bits R/W, 4096 Bits R/W, 4096 Bits R/W, 202 Bits (UID) R/W, 64K+120 Bits (UID) R/W, 1024 Bits R/W, 2048 Bits | ISO14443B ISO14443B ISO14443B ISO14443B ISO14443B ISO15693 with WORM User Area ISO15693 with WORM User Area ISO15693 | Done protected these blocks cannot be unprotected. Count-Down Rhang Counters with automated anti-bearing protection (a Books can be write protection, with access to controlled by the B Bits of the OTP_LOCK_REG register located at block atdees FF. Once protected these blocks cannot be unprotected. The source and the bits of the OTP_LOCK_REG register located at block atdees at block atdees at the bits of the OTP_LOCK_REG register located at block atdees at b | | | | |
| ST Microelectronics | SRI2K SRI4K SRI4K SRI54K LRI564 LRI564K LRI56K LRI5ZK ST13 family replaced by ST21 family ST16820 | 13.56 MHz | R/W, 512 Bits R/W, 1024 Bits R/W, 4096 Bits R/W, 512 Bitss R/W, 120 Bits (UID) R/W, 1024 Bits R/W, 1024 Bits R/W, 024 Bits R/W, 2048 Bits R/W, 2048 Bits R/W, 2048 Bits | ISO14443B ISO14443B ISO14443B ISO14443B ISO14443B ISO15693 with WORM User Area ISO15693 with WORM User Area ISO15693 ISO15693 ISO15693 ISO15693 ISO15693 | Once protected these block cannot be unprotected. Could Down Rhang Courters with automated anti-bearting protection (a Book can be with protection, with access to controlled by the B B of the OTP_LOCK_REG register located at block attracts of the unprotection. The unprotection of the unprotection. The unprotection of the unprotection of the unprotection of the unprotection of the unprotection. The unprotection of the unpr | | | | |
| ST Microelectronics | SRI2K SRI4K SRIX4K SRI512 LRI54 LRI564 LRI564 LRI564 LRI52K ST13 family replaced by ST21 family ST168752 ST168758 | 13.56 MHz | R/W, 512 Bits R/W, 1024 Bits R/W, 1024 Bits R/W, 4096 Bits R/W, 606 Bits R/W, 512 Bits R/W, 64K+120 Bits (UID) R/W, 2048 Bits R/W, 756 bytess R/W, 756 bytess R/W, 8Kb | IS0144438 IS0144438 IS0144438 IS0144438 IS0144438 IS0144438 IS015693 with WORM User Area IS015693 with WORM User Area IS015693 IS015693 IS015693 IS015693 IS0144438 IS0144438 IS0144438 | Done protected these blocks cannot be unprotected. Count Down Rhang Counters with automated anti-kerning protection (a Blocks can be write protection, with accesses a controlled by the Blio of the OTP_LOCK_REG register located at block and see the start of the start of the start of the unprotected. The start of th | | | | |
| ST Microelectronics | SRI2K SRI4K SRIX4K SRI512 LRI64 LRI564K LRI564K LRI2K LRI52K STI3 family replaced by ST21 family STI66820 STI66752 | 13.56 MHz | R/W, 512 Bits R/W, 1024 Bits R/W, 1024 Bits R/W, 4096 Bits R/W, 4096 Bits R/W, 512 Bits R/W, 64K+120 Bits (UID) R/W, 2048 Bits R/W, 2048 Bits R/W, 2048 Bits R/W, 756 Bytes R/W, Xb | IS0144438 IS0144438 IS0144438 IS0144438 IS0144438 IS0144438 IS015693 with WORM User Area IS015693 IS015693 IS015693 IS015693 IS015693 IS0144438 IS0144438 | Done protected these blocks cannot be unprotected. Count-Down Rhang Counters with automated anti-bearing protection (a Books can be write protected, with access is controloid by the B Bin of the OTP_LOCK_REG register located at block and see the start of the start of the unprotected. The start of the | | | | |
| ST Microelectronics | SRI2K SRI4K SRIX4K SRI512 LRI54 LRI564 LRI564 LRI564 LRI52K ST13 family replaced by ST21 family ST168752 ST168758 | 13.56 MHz | R/W, 512 Bits R/W, 1024 Bits R/W, 1024 Bits R/W, 4096 Bits R/W, 606 Bits R/W, 512 Bits R/W, 64K+120 Bits (UID) R/W, 2048 Bits R/W, 756 bytess R/W, 756 bytess R/W, 8Kb | IS0144438 IS0144438 IS0144438 IS0144438 IS0144438 IS0144438 IS015693 with WORM User Area IS015693 with WORM User Area IS015693 IS015693 IS015693 IS015693 IS0144438 IS0144438 IS0144438 | Done protected these block cannot be unprotected. Count Down Rhang Counters with automated anti-kerning protection (a Block can be write protection, with accessing the supported of the standard set of the | | | | |
| ST Microelectronics | SRI2K SRI4K SRI4K SRI512 LRI564 LRI564K LRI564K LRI564K LRI57 LRI57 LRI57 ST168752 ST168752 ST168752 ST168756 ST169752 S | 13.56 MHz 13.56 MHz | R/W, 512 Bits R/W, 1024 Bits R/W, 1024 Bits R/W, 1026 Bits R/W, 512 Bits R/W, 512 Bits R/W, 512 Bits R/W, 120 Bits (UID) R/W, 64K+120 Bits (UID) R/W, 248 Bits R/W, 206 Bits R/W, 204 Bits R/W, 204 Bits R/W, 205 Bits R/W, 205 R/W, 205 R/W, 205 | IS014443B IS014443B IS0144438 IS0144438 IS0144438 IS0144438 IS0144438 IS015693 with WORM User Area IS015693 with WORM User Area IS015693 IS015693 IS015693 IS015693 IS015693 IS015693 IS0144438 IS0144438 IS0144438 | Done protected these blocks cannot be unprotected. Count-Down Rhang Counters with automated anti-bearing protection (a Books can be write protected, with access a controlled by the B Bits of the OTP_LOCK_REG register located at block atlock at block and be unprotected. The source and an advantate anti-bearing and bearing protected at a block and bears and bearing and bearing protected. The source and an advantate anti-bearing and bearing and | | | | |
| ST Microelectronics | SRI2K SRI4K SRIX4K SRI512 LRI54 LRI564 LRI564 LRI564 LRI52K ST13 family replaced by ST21 family ST168752 ST168758 | 13.56 MHz | R/W, 512 Bits R/W, 1024 Bits R/W, 1024 Bits R/W, 4096 Bits R/W, 606 Bits R/W, 512 Bits R/W, 64K+120 Bits (UID) R/W, 2048 Bits R/W, 756 bytess R/W, 756 bytess R/W, 8Kb | IS0144438 IS0144438 IS0144438 IS0144438 IS0144438 IS0144438 IS015693 with WORM User Area IS015693 with WORM User Area IS015693 IS015693 IS015693 IS015693 IS0144438 IS0144438 IS0144438 | Done protected these block cannot be unprotected. Count Down Rhang Counters with automated and kerning protection (a Block can be write protection, with access the counters with automated and kerning protection (a Block can be write protection, with access the counters by the Bloch of the CTP_LOCK_REG register located at block and eser protection of the service | | | | |
| ST Microelectronics | SRI2K SRI4K SRI4K SRI512 LRI564 LRI564K LRI564K LRI564K LRI57 LRI57 LRI57 ST168752 ST168752 ST168752 ST168756 ST169752 S | 13.56 MHz 13.56 MHz | R/W, 512 Bits R/W, 1024 Bits R/W, 1024 Bits R/W, 1026 Bits R/W, 512 Bits R/W, 512 Bits R/W, 512 Bits R/W, 120 Bits (UID) R/W, 64K+120 Bits (UID) R/W, 248 Bits R/W, 206 Bits R/W, 204 Bits R/W, 204 Bits R/W, 205 Bits R/W, 205 Bits R/W, 205 R/W, 205 | IS014443B IS014443B IS0144438 IS0144438 IS0144438 IS0144438 IS0144438 IS015693 with WORM User Area IS015693 with WORM User Area IS015693 IS015693 IS015693 IS015693 IS015693 IS015693 IS0144438 IS0144438 IS0144438 | Done protected these blocks cannot be unprotected. Count-Down Rhang Counters with automated anti-bearing protection (a Books can be write protected, with access a controlled by the B Bits of the OTP_LOCK_REG register located at block atleses FF. Once protected these blocks cannot be unprotected. The source and the bits of the OTP_LOCK_REG register located at block atleses and be unprotected. The source and the bits of the OTP_LOCK_REG register located at block atleses at block atleses at the other protected of the source and the source of the State at the source of the State at the | | | | |

| Manufacturer | Type/Model Name | Fraguancy | Description | Standard/Notes | Cogurity | | | |
|---|---|------------------------|--|--|--|------|--|------|
| manufacturer | Type/Model Name | Frequency | Description | Stanuaru/Notes | Security Security hardware firewall for memories (access rules are user defined and can be selected by mask-options) and hardware DES | | | |
| | ST23YR08 | 13.56+contact | R/W, 8Kb | ISO14443B/B'/PayPass | Security hardware firewall for memories (access rules are user defined and can be selected by mask-options) and hardware DES accelerator (accessible via cryptographic software libraries located in ST ROM) with library support for symmetrical algorithms: DES, triple DES, DESX computations and CBC chaining mode; FIPS 140-2 compliant random number generator with two G LN. registers | | | |
| | | | | | Generators of Unpredictable Number). Enhanced NESCRYPT crypto-processor for public key cryptography. Security hardware firewall for memories (access rules are user defined and can be selected by mask-options) and hardware DES accelerator (accessible via cryptographic software libraries located in ST ROM) with library support for symmetrical algorithms: DES, | | | |
| | | | | | accelerator (accessible via cryptographic software libraries located in ST ROM) with library support for symmetrical algorithms: DES, tricle DES, DESX computations and CRC chaining mode. FIPS 140-2 compliant random number generator with two G LLN, registers | | | |
| | ST19XR34 | 13.56+contact | R/W, 34Kb | ISO14443B/B' | triple DES, DESX computations and CBC channing mode; FIPS 140-2 compliant random number generator with hivo G UN registers (Generators of Unpredictable Number). 1088 Bit Modular arithmetic processor with litrary support for asymmetrical algorithms - Fast modular multiplication and squaring using Montgomery method - Software Crypto litraries in separate ST ROM area for efficient | | | |
| | | | | | | | | |
| | | | | | Three-key Triple DES accelerator AES accelerator | | | |
| | MR31 | 13.56+contact | R/W, 16K, 22K, 38K, 52K Bytes | ISO14443A/B/B' | NESCRYPT coprocessor for public key cryptography algorithm Protection against multiple attacks The SRS12052 Elevatives hardware accelerators for advanced cryptographic functions. The AES accelerator provides a high-performance implementation of AES-128, AES-192, AES-256 algorithms. The 3-key Triple DES | | | |
| | MR31 | 13.30+contact | K/W, 10K, 22K, 30K, 52K bytes | 15014443A/B/B | AES accelerator provides a high-performance implementation of AES-128, AES-192, AES-256 algorithms. The 3-key Triple DES accelerator (EDES+) peripheral enables Cipher Block Chaining (CBC) mode fast DES and triple DES computation based on three key. | | | |
| | | | | | accelerator (EDES+) peripheral enables Cipher Block Chaining (CBC) mode, fast DES and triple DES computation based on three key registers and one data register, while the NESCRYPT crypto-processor efficiently supports the public key algorithm with native operations up to 4096 bits long. Two 16-bit general-purpose timers are available, one is configurable as a watchdog. | | | |
| | SR31 | 13.56+contact | R/W, 16K, 22K, 38K, 40K, 52K Bytes | ISO14443A/B/B' | | | | |
| | | | | | Lock-sector command sets the access rights and permanently locks the selected sector (1 sector = 32 blocks). Multiple password protection in RF mode | | | |
| | M24LR04/16/64E-R | 13.56+12C | R/W, 4K, 16K, 64K Bytes | ISO15693 | Single password protection in I2C mode. In I2C modeThe M24LR04E-R controls I2C sector write access using the 32bit-long I2C password and the 64-bit I2C_Write_Lock bit area. In RF mode, each memory sector of the M24LR04E-R can be individually protected | | | |
| | | | .,,, | | by one out of three available 32bit passwords, and each sector can also have Read/Write access conditions set. Each memory sector of the M24LR04E-R is assigned with a Sector security status byte including a Sector Lock bit, two Password Control bits and two | | | |
| | | | | | Read/Write protection bits. "Lock-sector command sets the access rights and permanently locks the selected sector (1 sector = 32 blocks). Multiple password | | | |
| | | | | | - Single password protection in IIC mode. In I2C mode. The M24LR04E-R controls I2C sector write access using the 32bit-long I2C | | | |
| | M24LR64-R | 13.56+I2C | R/W, 65536 Bits | ISO15693 | password and the 64-bit I2C write Lock bit area. In RF mode, each memory sector of the M24LR04E-R can be individually protected | | | |
| | | | | | password and the 64-bit ICC. Write Lock bit area. In RF mode, each memory sector of the NA24R04E-R can be dividually protected by one out of three available 32bit passwords, and each sector can also have ReadWrite access conditions set. Each memory sector of the INZ4R04E-R is assigned with a Sector security status type including a Sector Lock bit, two Password Control bits and two | | | |
| | XRA00 | 866-928 MHz | R/W. 128 Bits, 96-bit EPC code | EPC Class 1b | Read/Write protection bits." 8-bit destruct code - 8-bit lock code. | | | |
| | XRAG2 | 866-928 MHz | R/W, 432 Bits | EPC Gen2 | Kill Command - Access Password - Lock mechanism. | | | |
| | RC-S919 | 13.56 MHz | R/W, 576 Bytes | ISO/IEC 18092 | ? The access key is generated from the area key and service key of the area and service to be accessed. Mutual authentication is a | | | |
| | RC-S962/1 | 13.56 MHz | R/W, 2464 Bytes | ISO/IEC 18092-FeLiCa (failed ISO14443C) | process of cross-checking confirmation between PCD and PICC, using the access key mentioned above. By using information as the key which is generated in the mutual authentication process. The subsequent data on the communication path is ancurated | | | |
| | RC-S965 (Lite) | 13.56 MHz | R/W, 224 Bytes FRAM | ISO/IEC 18092-FeLiCa Lite | Streamlined authentication via triple DES data encryption algorithm. By adding a Message Authentication Code (MAC) to the readout data. the authentication the arrife best data encryption algorithm. By adding a Message Authentication Code (MAC) to the readout data. the authentication the arrife best data encryption algorithm. By adding a Message Authentication Code (MAC) to the readout data. the authentication the arrife best data encryption algorithm. By adding a Message Authentication Code (MAC) to the readout data. the authentication of the arrife best data encryption algorithm. By adding a Message Authentication Code (MAC) to the readout data. the authentication of the arrife best data encryption algorithm. By adding a Message Authentication Code (MAC) to the readout data. the authentication of the arrife best data encryption algorithm. By adding a Message Authentication Code (MAC) to the readout data. the authentication of the arrife best data encryption algorithm. By adding a Message Authentication Code (MAC) to the readout data. the authentication of the arrife best data encryption algorithm. By adding a Message Authentication Code (MAC) to the readout data. the authentication of the arrife best data encryption algorithm. By adding a Message Authentication Code (MAC) to the readout data. the authentication of the arrife best data encryption algorithm. By adding a Message Authentication Code (MAC) to the readout data. the authentication of the arrife best data encryption algorithm. By adding a Message Authentication of the arrive and the a | | | |
| | | | | | The access key is generated from the arise key and service key on the area and service to be accessed, Maula autentication is a process of cross-before access and access access and acces | | | |
| | RC-S966 (Lite-S) | 13.56 MHz | R/W, 432 Bytes FRAM | ISO/IEC 18092-FeLiCa Lite-S | - Read / Write Access | | | |
| Sony | (inc 3) | | | 100/IEC 100/2-FEICe Lite-5 | - Read After Authentication - Write After Authentication - Write With MAC | | | |
| | RC-SA00 | 13.56 MHz | R/W, 6K Bytes | ISO/IEC 18092 | Write With MAC AES and DES encryption; AES-encrypted commands; DES-encrypted commands; Non-encrypted commands | | | |
| | RC-SA01 | 13.56 MHz 13.56 MHz | R/W, 6K Bytes R/W, 4K Bytes | ISO/IEC 18092 ISO/IEC 18092 | AES and DES encryption; AES-encrypted commands; DES-encrypted commands; Non-encrypted commands AES encryption; AES-encrypted commands; Non-encrypted commands | | | |
| | RC-5888 | 13.56 MHz | R/W, 4K Bytes | ISO/IEC 18092 | Embedded IC chip (RC-S962) with superior tamper resistant characteristics | | | |
| | RC-5889 | 13.56 MHz | R/W, 9K Bytes | ISO/IEC 18092 | Embedded IC chip (RC-S960) with superior tamper resistant characteristics riple-DES encryption is used for the mutual authentication between a card and reader, reader and controller. Transmission data is | | | |
| | RC-5860 | 13.56 MHz | R/W, 4K Bytes | ISO/IEC 18092 | rpie-DSS encryption is used for the mutual authentication between a card and reader, reader and controller. Transmission data is encrypted using a transaction key which is dynamically generated at every mutual authentication. These features make forgery and card fraud nearly impossible. | | | |
| | MB89R118 | 13.56 MHz | R/W, 2K Bytes FRAM | ISO/IEC 15693 | | | | |
| FUJITSU | | 13.56 MHz | R/W. 256 Bytes FRAM | | Lock (disable to write) the requested 1 block in the user area. | | | |
| | MB89R119 | | .,, | ISO/IEC 15693 | Lock (disable to write) the requested 1 block in the user area. | | | |
| | UNIQUE (EM4102) T5/Nova (JMA TP05) | 125 KHz 130 kHz | Read only, 64 Bits R/W, 160 Bits (64 or 128 selectable) | | none Password functions. | | | |
| | Magic (probably Megamos Crypto) | 125 kHz | R/W, 192 Bits | | Cypto protection. Password functions. | | | |
| | Q5 (same as T5555) | 125 KHz | R/W, 264 Bits | | Password mode allows reading one word after password check - Write protection command to lock the words independently from one another. | | | |
| | TITAN (EM4550) | 125 KHz | R/W, 1024 Bits | | another. The memory can be secured by using the 32 bit password (stored in block0) for all write and read protected operations. The password can be updated, but never read. Also chip has a control word (block2-bit16 pwd on/off) and a protection word (block1 - set blocks protection for read/write). | | | |
| | | | | | protection for read/write). The advantage of two way authentication over conventional crystographic transponders | | | |
| | | | | | The advantage of two way authentication over conventional cryptographic transponders is that only a valid interrogation of the transponder can result in the return of the cryptographic reply that is sent | | | |
| | TagCoder Lite | 125 KHz | R/W, 512 Bits | | back to the vehicle reader. The first authentication takes place within the transponder; the second authentication is carried out within the transponder unit itself. Due to this two way authentication method and the 96 bit Secret Key | | | |
| | | | | | one of the highest security level available for automotive transponders on the market is reached. 32 Bit password; 2 lock bits, 23 Bit customer low | | | |
| | | | | | The advantage of two way authentication over conventional cryptographic transponders is that only a valid interrogation of the transponder can result in the return of the cryptographic reply that is sent | | | |
| Sokymat Automotive (acquired in | TagCoder (as the previous IC but with integrated remote logic) | 125 KHz | R/W, 512 Bits | | The advantage of how way suthencication over conventional cryptographic transponders is that only a value intercogation of the transponder can result in the return of the cryptographic reply that is sent back to the vehicle reader. The first authentication takes place within the transponder; the second authentication is carried out within the transponder unit. Itself. Due to this how way authencication method and the 95 bit Secret Key | | | |
| 2003 by EM Microelectronic - sold in 2008 to SMARTRAC Technology | | | | | carried out within the transponder unit itself. Due to this two way authentication method and the 96 bit Secret Key one of the highest security level available for automotive transponders on the market is reached. 32 Bit password; 2 lock bits; 32 Bit customer key. | | | |
| GmbH) | | | | | | | | |
| | | | | | with an SPI serial interface. This unique combination allows for the sharing of EEPROM and crypto operations between TagAccess and a microcontroller. It is | | | |
| | TaqAccess | 125 KHz/Serial | R/W, 4096 Bits | | possible to access the EEPROM of TagAccess via a simple serial protocol or via | | | |
| | TagAccess | 125 Ki12/ Selidi | N/W, 4050 BIG | | the 125 kHz transponder link from the vehicle immobilizer base station. EEPROM is used to store device configuration, the user programmable secret | | | |
| | | | | | keys (not readable via SPI), 32 bit unique Device Identification, 32 bit password, as well as 3,726 bits of freely programmable user memory. | | | |
| | | | | | | | | |
| | | | | | cryptographic Read/Write Transponder containing the NISTproven public encryption algorithm AES (Advanced Encryption Standard). The performance optimised implementation is based on 128 bit secret key with multiple authentication methods and security levels. Due to a patented protocol concept extremely short timings are selectable | | | |
| | AES-Tag | 125 kHz | R/W, 10240 Bits | | automication methods and security levels. Job to a patentic protocol concept extremely short chinings and security in all automication modes single, mutual and mutual ISO. Random number generation is supported via an embedded TRNG. The transponder also contains a 32 bit identification number as well as multiple configuration and lock- | | | |
| | | | | | TRNG. The transponder also contains a 32 bit identification number as well as multiple configuration and lock- mechanisms. Various protections mechanisms for the user-memory can be configured on customer's choice and | | | |
| | | | | | mechanisms. Various protections mechanisms for the user-memory can be configured on customer's choice and preference. A special increment-counter in ring-bufferarchitecture completes the outstanding feature list of this product. 128 bit secret keys (3x) - 32 bit customer key - 6 lock bits - 32 bit password. | | | |
| 222 | Zodiac (EM4102) Zodiac (EM4102) [probably a Sokymat product] | 134.2 KHz | Read only, 128 Bits | ISO11784 | | | | |
| | | | | | Page 1, 2, 4 R/W; Page 3 R/O; Page 4 (encrypted); 8 bit password, In the encryption mode the interrogator sends (writes) the encryption command in the write address bolowed by a 40-bit random number (challenge) to the transponder. The challenge is shifted into the encryption logic, which is also initialized with the 40-bit encryption key stored in EERPKON. When the challenge has been | | | |
| | RI-TRP-B* | 124.2 KHz | DOM 99 Bits | | into the encryption logic, which is also initialized with the 40-bit encryption key stored in EEPROM. When the challenge has been excepted as the encryption logic, which is also initialized with the 40-bit encryption key stored in EEPROM. When the challenge has been | | | |
| | KI-1KP-D* | 134.2 KHz | R/W, 88 Bits | | completely received, a block cipher algorithm is executed using both the challenge and the encryption key. If fewer or more bits are received, a discharge is executed in the subsequent read phase (no response). Once it detects the end of the encryption phase, the | | | |
| | | | | | transponder responds by sending the 24 bit serial number stored in the EEPROM and a 24 bit response (signature) that was generated by the block cipher algorithm (DST40). | | | |
| | RI-TRP-D* | 134.2 KHz | R/W, 1360 Bits | | ? (probably DST40). | | | |
| | RI-TRP-I* RI-TRP-M* | 134.2 KHz 134.2 KHz | R/W, 1360 Bits R/O, 30 Bits+R/W 208 Bits | | ? (probably DST40). 24 Bits selective Address width. ? (probably DST40) | | | |
| | RI-TRP-R*/0* | 134.2 KHz | Read only, 64 Bits | | 000 | | | |
| | RI-TRP-V* | 134.2 KHz | R/W, 50 Bytes | | Lock bits; TI Challenge/Response principle, Single Encryption or Mutual Authentication; TI Random Challenge/Response; 40-bit Mutual Authentication and Issuer Keys; 24 bit signature (DST+). | | | |
| | RI-TRP-W* | 134.2 KHz | R/W, 80 Bits | | none | | | |
| | TMS37134 | 134.2 KHz | | | TI Challenge/Response, Mutual Authentication, Secure Issuer Access Mode; Encryption, Mutual Authentication, Issuer Key Each 40 bit; Encryption response (signature) 24 bit (DST+). | | | |
| | TMS37145 RI-TH1-CB1A (based on TagIt) [obsolete] | 134.2 KHz 13.56 MHz | R/W, 80 Bits R/W, 2 KBit | ISO15693 | 80-bit key length, 4-byte or 5-byte challenge, 3-byte signature (DST80). Each block is separately programmable by the user and can be locked to protect data from modification. Once the data has been Tocked then it cannot be changed. Two levels of block locking are supported: Individual block locking by the user (U) or individual | | | |
| | RI-TH1-CB2A (based on TagIt) | 13.56 MHz | R/W, 2 KBit | ISO15693 | Tocked' then it cannot be changed. Two levels of block locking are supported: Individual block locking by the user (U) or individual block locking of factory programmed data (F) during manufacturing. Bit 2 of the "Block Security Status" Rute defined to ISO 3 to | | | |
| | RI-TH1-CB3A (based on TagIt) | 13.56 MHz | R/W, 2 KBit | ISO15693+Magnetic Stripe | bocke tries in calificities of background and the second s | | | |
| | Tag-it HF-I Standard | 13.56 MHz | R/W, 256 Bit | ISO15693 | Each block is separately programmable by the user and can be locked to protect data from modification. Once the data has been focked then it cannot be changed. Two levels of block locking are supported. Individual block locking by the user (10) or individual block locking relatory programmed data (7) during manufacturing. Bit 2 of the 'Block Security Shatus' Byte defined in ISO 15693-3 is | | | |
| | | | | | used to store the Factory Lock Status of the Block. Block locking interestibly protects the locked data from any further reprogramming. | | | |
| | | | | | block looking in lacking page and the start of block floating that start is the store rescuring data by the energy manual and a start be first store of the start of block. Store kooking reveals by notes the store data store modification. Once the data has been looked, it can only be thanged by the passer and can be looked to protect data from modification. Once the data has been looked, it can only be user (in a can be looked to protect and the context to protect the store data from the store looked, it can only be user (in a can be looked to protect and the context to protect the store looked in the store of the store of the store the store (in a can be looked to protect the store looked to be user (i) or indicata book looking of factory programmed data (i) during manufactures, Bit 2 of the tibols. Store the store to be the store (in a context of the looked to be the P store). Technologic book looked to be the looked to be the P store). Technologic book is store to be the store (in a context of the looked to be the P store). Technologic book is store to be store to be store to be store P store). Technologic book is store to be store to be store). Technologic book is store to be store to be store to be store to be store to be store). Technologic book is store to be store to be store to be store to be store to be store). Technologic book is store to be store to be store to be store to be store to be store) to be store to b | | | |
| | Tag-it HF-I Pro | 13.56 MHz | R/W, 256 Bit | ISO15693 | locking by the user (U) or individual block locking of factory programmed data (F) during manufacturing. Bit 2 of the "Block Security Status" byte defined in ISO 15693-3 is used to store the Factory Lock Status of the Block. Factory Block locking irreversibly protects | | | |
| | | | | | command kill command available | | | |
| | | | | | Each block with 32 bit is user programmable and can be locked individually to protect data from modification. Once set, the lock bit | | | |
| | Tag-it HF-I Plus | 13.56 MHz | R/W, 2048 Bit | ISO15693 | cannot be reset. The user memory is field programmable per block. Two levels of block locking are supported: trividival block locking of factory programmed data (F) during manufacturing. Bit 2 of the "Block Security Status" Byte defined in ISO 15693-3 is used to store the Factory Lock Status of the Block. Block locking inversibly protects the locked data | | | |
| | | | | | Byte defined in ISO 1693-3 is used to store the Factory Lock Status of the Block. Block locking intervensibly protects the locked data from any further reprogramming. | | | |
| | RI-UHF-* | 860-960 MHz | R/W, 96 Bits EPC+32 Bits UID | EPC Gen2 - ISO18000-6 | ? Cryptographic security for data protection and chip authentication. Two unique secret keys are used to protect two different applications | | | |
| | PicoPass 2KS | 13.56 MHz | R/W, 2K Bit | IS014443A/IS014443B/IS015693 | or to manage crediting and debiting of a secure stored value area. Cryptographic security protections can be disabled during | | | |
| Inside Secure | PicoPass 16KS | 13.56 MHz | R/W. 16K Bit | 150144434/150144428/1501502 | personalization phase. Cryptographic security for data protection and chip authentication. Two unique secret keys are used to protect two different applications or to manage credition and debition of a secure stored value area. Comborranhic security protections can be fisiabled during | | | |
| | 100 035 2010 | 13.33 PH 12 | iy iiy zoc bit | 12014499012014442012012032 | or programma sectors no data procedure and any building and the procedure and any sector of a sector of the sector | | | |
| | | | | | | | | |

| Manufacturer | Type/Model Name | Frequency | Description | Standard/Notes | Security | | | | | |
|---|--|------------------------|--|---|---|------|------|-------|---|--|
| Hundractarer | PicoPass 32KS | 13.56 MHz | R/W, 32K Bit | 150144424/150144428/15015602 | Cryptographic security for data protection and chip authentication. Two unique secret keys are used to protect two different applications or to manage crediting and debiting of a secure stored value area. Cryptographic security protections can be disabled during | | | | | |
| | | | | 130144430(130144430)(13013053 | personalization phase. | | | | | |
| GOLDKEY Technology | GK4001 (same as EM4001) | 125 KHz | R/W, 64 Bit | | none | | | | | |
| | | | | ISOProx has only 125KHz chip. | | | | | | |
| | Prox (1xxxxxxx) | 125 KHz | Read only, 44 Bit | Duo option adds a Magnetic Stripe (1336/1536). | none | | | | | |
| | | | | Contact chip options are available. Refer to the Logical Access HTOG. | | | | | | |
| | | | | ISO14443A/B and ISO15693 | The authentication for secure mode communication between reader and card is done both-ways using the 16 byte 3DES | | | | | |
| HID Global | iClass (2xxxxxxxx) | 13.56 MHz | R/W, 2k, 16k, 32k | (200/210/202/212/204/232/242/252/ Contact chin ontions are available | keys KCUR (Custom Read Key) and KCUW (Custom Write Key). One needs to sign a NDA with HID to receive these two keys from HID. The control of these keys by HID limits the group of people with read access to the HID Access Control | | | | | |
| | | | R/W, 2k, 16k, 32k | Refer to the Logical Access HTOG. | Application. | | | | | |
| | iClass SE (3xxxxxxxx) | 13.56 MHz | MIFARE 1k, 4k | Has a Magnetic Stripe option. | ICLASS SE smart cards feature multiple securely separated application areas that are each protected by 64-bit diversified readwrite keys that allow complex applications and provide for future expansion. ICLASS SE smart card technology provides secure access control and increases performance with mutual authentication, encrypted data transfer, and 64-bit diversified keys for readwrite | | | | | |
| | | | DESFire EV1 8k Seos 16k | Contact chip options are available. Refer to the Logical Access HTOG. ISO14443A/B and ISO15693 (optiona | control and increases performance with mutual authentication, encrypted data transfer, and 64-bit diversified keys for read/write capabilities. | | | | | |
| | iClass dual technology cards. | 125 KHz + 13.56 MHz | Combinations of the HID formats above | ISO14443A/B and ISO15693 (optiona magnetic band) | | | | | | |
| | FM11RF005M | 13.56 MHz | R/W, 512 Bit | IS014443A | High security level data communication (mutual three pass authentication); security level control; Encryption Algorithm compatible with Mifare 1K. Without authentication blocks from 8 to 15 cannot be read/write and from 2 to 7 | | | | | |
| | | | | | can only be read. Blocks 0 and 1 can never be written. High security level data communication (mutual three pass authentication); security level control; Encryption Algorithm compatible with Shanghai local standard. Without authentication blocks from 8 to 15 cannot be read/write | | | | | |
| | FM11RF005SH | 13.56 MHz | R/W, 512 Bit | ISO14443A | Algorithm compatible with Shanghai local standard. Without authentication blocks from 8 to 15 cannot be read/write and from 2 to 7 can only be read. Blocks 0 and 1 can never be written. | | | | | |
| | FM11RF08 (Mifare 1K clone) | 13.56 MHz | R/W, 1024 Bit | IS014443A | and from 2 to 7 can only be read. Blocks 0 and 1 can never be written. 3 pass mutual authentication (ISO IECDIS979-2) - All data should be encrypted after authentication to prevent signal interception - Transfer key protection. Individual set of keys for each block. User definable access condition for | | | | | |
| | | | | | each block. Transfer key protection. Individual set of keys for each block. User definable access condition for each block. | | | | | |
| | FM11RF08SH | 13.56 MHz | R/W, 1024 Bit | IS014443A | Encryption Algorithm compatible with Shanghai local standard. | | | | | |
| Fudan Microelectronics | FM11RF32M (Mifare 4K clone) | 13.56 MHz | R/W, 1024 Bit | IS014443A | 3 pass mutual authentication (ISO IECDIS9798-2) - All data should be encrypted after authentication to prevent signal interception - Transfer key protection. Individual set of keys for each block. User definable access condition for each block. | | | | | |
| | FM11RF32SH | 13.56 MHz | R/W, 1024 Bit | IS014443A | Transfer key protection. Individual set of keys for each block, User definable access condition for each block. | | | | | |
| | FM1208 | 13.56 MHz | R/W, 32K ROM+8K EEPROM | IS014443A | Encryption Algorithm compatible with Shanghai local standard. High security level data communication (mutual three pass authentication, Access right control - auth command is | | | | | |
| | FM1208M01 (Mifare compatible command set) | 13.56 MHz | R/W, 32K ROM+8K EEPROM | IS014443A | [60]) 3DES, single-DES processor: SPA/DPA resistenat controller, Memory data encryption (ROM, EEOPROM, RAM), ROM code reverse | | | | | |
| | FM1208H01 (Mirare compatible command set) FM1208SH01 | 13.56 MHz | R/W, 32K ROM+8K EEPROM | IS014443A | resistant. Encryption Agorithm compatible with Mare 1K. 30ES, single-DES processor, SPA/DPA resistenat controller. Memory data encryption (ROM, EEOPROM, RAM). ROM code reverse resistant. Encryption Algorithm compatible with Shanghai local standard. | | | | | |
| | FM12085H01 FM12AG08M01 | 13.56 MHz | R/W, 32K ROM+8K EEPROM | IS014443A | resistant. Encryption Algorithm compatible with Shanghai local standard. 3DES, SM1, compatible with Mifare 1K. | | | | | |
| | FM1208M04 | 13.56 MHz | R/W, 32K ROM+8K EEPROM | IS014443A IS014443A | 3DES, compatible with Mifare 4K. | | | | | |
| | K55004XK2 | 125 KHz | Read only, 64 Bits | | none | | | | | |
| | K65004XK1 | 13.56 MHz | Read only, 64 Bits | | none | | | | | |
| | K65004XK3 (Mifare 1K clone?) | 13.56 MHz | R/W, 1024 Bits | IS014443A | 48 Bit cyptographic key to access each of the 16 sectors. | | | | | |
| | К563РТ1У КИБИ-001 | 2 GHz 125 kHz | R/W, 1563 Bits Read only, 64 Bits | | ?none? | | | | | |
| | KNEW-001 KNEW-001MT | 125 kHz | Read only, 64 Bits | | none | | | | | |
| Angstrom (russian company) | КИБИ-002 | 13.56 MHz | Read only, 64 Bits | | none | | | | | |
| | КИБИ-002МТ | 13.56 MHz | Read only, 64 Bits | | none | | | | | |
| | БИД-002 | 13.56 MHz | Read only, 64 Bits | | none | | | | | |
| | ммбит-002 киби-D | 13.56 MHz 13.56 MHz | Read only, 64 Bits Read only, 64 Bits | | none | | | | | |
| | Transponder G2 | 860 MHz | ? | | none2 | | | | | |
| Tatwah Design | TK4100 (EM4100 clone) | 125 kHz | Read only, 64 Bits | | none | | | | | |
| | | | | | Lock bytes - They enable the user to lock parts of the complete memory area for writing. A Read from user memory area cannot be restricted via lock bytes functionality. OTP bytes - Page 03h is the OTP page and it is preset so that all | | | | | |
| | QR2213 (Mifare Ultralight clone) | 13.56 MHz | R/W, 64 Bytes | IS014443A | area cannot be restricted via lock bytes functionality. OTP bytes - Page 03h is the OTP page and it is preset so that all bits are set to logic 0 after production. These bytes can be bitwise modified using the WRITE command. The WRITE command bytes and the current contents of the OTP bytes are bitwise are bitwise suit is the new OTP byte | | | | | |
| | ·, | | | | contents. This process is irreversible and if a bit is set to logic 1, it cannot be changed back to logic 0. 3DES Authentication proves that two entities have the same secret and each entity can be seen as a reliable partner for the | | | | | |
| Quanray | | | | | coming communication. The applied encryption algorithm ek() is 2 key 3DES encryption. | | | | | |
| | QR2217 (Mifare 1K clone) | 13.56 MHz | R/W, 1024 Bytes | IS014443A | 3-pass authentication: ISO/ IEC DIS9798-2 - All data are encrypted in communication to prevent being intercepted - Individual set of two keys per sector (per application) to support multi-application with hierarchical security control - | | | | | |
| | | | | | Stream Cablering protects data transmission. - pass authentication: ISO/ IEC DIS9798-2. All data are encrysted in communication to prevent being intercepted Individual set of two keys per sector (per application) to support multi-application with hierarchical security control - Individual set of two keys per sector (per application) to support multi-application with hierarchical security control - termination of the sector of the sector (per application) to support multi-application with hierarchical security control - termination of the sector of the sector (per application) to support multi-application with hierarchical security control - termination of the sector of the | | | | | |
| | QR2272 | 13.56 MHz | R/W, 1024 Bytes | IS014443A | Individual set of two keys per sector (per application) to support multi-application with interactical security control - Stream Ciphering protects data transmission. 128bit TEA encryption. 38bit random number generator. 3 pass mutual authentication (ISO IECDIS9798-2) - All data should be encrypted after authentication to prevent | | | | | |
| | SHC1101 (Mifare 1K clone) | 13.56 MHz | R/W, 1024 Bytes | IS014443A | 3 pass mutual authentication (ISO IECDIS9798-2) - All data should be encrypted after authentication to prevent signal interception - Transfer key protection. Individual set of keys for each block. User definable access condition for | | | | | |
| | SHC1102 (Mifare Ultralight clone) | 13.56 MHz | R/W. 512 Bits | IS014443A | each block. | | | | | |
| | | | | | 3 pass mutual authentication (ISO IECDIS9798-2) - All data should be encrypted after authentication to prevent | | | | _ | |
| | SHC1104 (Mifare 1K clone) | 13.56 MHz | R/W, 1024 Bits | IS014443A | signal interception - Transfer key protection. Individual set of keys for each block. User definable access condition for each block. | | | | | |
| | SHC1112 | 13.56 MHz | ? | IS014443A | ? - Supports 1024bit Modular Arithmetic | | | | | |
| Shanghai Huahong Integrated Circuit Co (SHIC) | | | | | - Supports Tozaron Hodular Antimient - Supports Modular Exponentiation and Modular Multiplication operation - Supports hardware accelerated key pair generation | | | | | |
| circuit co (Shic) | SHC1124 | 13.56 MHz | R/W, 72K Bytes / ARM SC100 core CPU | ISO14443A | - Supports SPA/DPA resistant | | | | | |
| | | | | | Co-processors for public and secret key encryption to support RSA, ECC and DES/3DES. Generates true random number. | | | | | |
| | | | | | Supports 2048bit Modular Arithmetic for RSA Supports Modular Exponentiation and Modular Multiplication operation | | | | | |
| | SHC1302 | 13.56 MHz+contact | R/W, 48K Bytes / ARM SC100 core CPU | ISO14443-ISO/IEC7816 | - Supports hardware accelerated key pair generation - Supports 256bit ECC key length | | | | | |
| | | | | | - Supports SPA/DPA resistant Co-processors for public and secret key encryption to support RSA, ECC and DES/3DES. Generates true random | | | | | |
| | MAX66040E | 13.56 MHz | R/W, 1K Bits | IS014443B | number. Block Lock Feature; 512-Bit SHA-1 Engine to Compute 160-Bit MAC and to Generate Secrets. | | | | | |
| | MAX66040E MAX66040K | 13.56 MHz | R/W, 1K Bits | IS014443B | Block Lock Feature; 512-Bit SHA-1 Engine to Compute 160-Bit MAC and to Generate Secrets. Block Lock Feature; 512-Bit SHA-1 Engine to Compute 160-Bit MAC and to Generate Secrets. | | | | | |
| Maxim Integrated | MAX66140E | 13.56 MHz | R/W, 1K Bits | ISO15693/ISO18000-3 | Block Lock Feature; 512-Bit SHA-1 Engine to Compute 160-Bit MAC and to Generate Secrets. | | | | | |
| | MAX66140K | 13.56 MHz | R/W, 1K Bits | ISO15693/ISO18000-3 | Block Lock Feature; 512-Bit SHA-1 Engine to Compute 160-Bit MAC and to Generate Secrets. | | | | | |
| Broadcom (previously Innovision, acquired in 2010) | BCM20203T512 (Topaz, probably old Jewel IC) | 13.56 MHz | R/W, 96 or 512 Bytes | ISO14443A/ISO18000-3 | Permanent Block Lock Feature. | | | | | |
| | M1HW | 13.56 MHz | R/W, 1K Bits | IS014443A | PUF Circuit (unique and random silicon fabrication process variations): unclonable. | | | | | |
| Verayo | M4H | 13.56 MHz | R/W-OTP, 2K Bits | IS014443A | PUF Circuit (unique and random silicon fabrication process variations): unclonable. | | | | _ | |
| | X5122H Kovio Tag | 13.56 MHz 13.56 MHz | R/W-OTP, 512 Bits Read Only, 128 Bits | IS014443A IS014443A | PUF Circuit (unique and random silicon fabrication process variations): unclonable. | | | | | |
| Kovio | Kovio 2Kb | 13.56 MHz | R/W, 2K Bits | IS014443A | Possible blocks permalock. | | | | | |
| | | | | | | | | | | |
| | | | | | | | | _ | | |
| OTI, ISO 14443 Type D / | | | | | | | | | | |
| Cubic, ISO 14443 Type E | | | | | | | | _ | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | _ | |
| | | | | | | | | | | |