Manufacturer	Type/Model Name	Frequency	Description	Standard/Notes	Security
Alien Technology	Higgs 2	860~960 MHz	EPC up to 192 Bits, TID 64 Bits	ISO18000-6c - EPC Gen2	?none?
	Higgs 3	860~960 MHz	EPC up to 480 Bits, TID 64 Bits	ISO18000-6c - EPC Gen2	Dynamic Authentication™ - Enhanced IC security using a non-digital, unique and non-cloneable "finger-print" - Practically eliminates copied tags being applied to counterfeit or goods of higher value. A 64-bit Unique TID for authentication and serialization applications, an extensible EPC memory bank, 512-bits of user memory for distributed data applications, and password protected read and write support capabilities to prevent unauthorized viewing and modifi cation of the tag's 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 write support capabilities to prevent unauthorized viewing and modification of the tag's data.
Inpinj	Monza 3	860~960 MHz	EPC up to 128 Bits	EPC Gen2 - ISO18000-6	?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	?none?
	Monza 4QT	860~960 MHz	EPC up to 128 Bits - User Memory 128 Bits	EPC Gen2 - ISO18000-6	QT technology's 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-tenth of its normal range. So while a reader can always singulate the tag and read its currently exposed identifier (EPC or alternate product identifier) from normal range, any attempts to access the Private Data Profile from a distance will cause the tag to lose power and drop out of its dialog with the reader. The short-range feature ensures that protected information is not readable unless the tag is very close to a reader antenna.
	Monza 5	860~960 MHz	User Memory 128 Bit	EPC Gen2 - ISO18000-6	?none?
	Monza X-2K Dura	860~960 MHz/I2C	EPC up to 128 Bits - User Memory 2176 Bits	EPC Gen2 - ISO18000-6	QT technology's 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-tenth of its normal range. So while a reader can always singulate the tag and read its currently exposed identifier (EPC or alternate product identifier) from normal range, any attempts to access the Private Data Profile from a distance will cause the tag to lose power and drop out of its dialog with the reader. The short-range feature ensures that protected information is not readable unless the tag is very close to a reader antenna.
	Monza X-8K Dura	860~960 MHz/I2C	EPC up to 128 Bits - User Memory 8192 Bits	EPC Gen2 - ISO18000-6	QT technology's 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-tenth of its normal range. So while a reader can always singulate the tag and read its currently exposed identifier (EPC or alternate product identifier) from normal range, any attempts to access the Private Data Profile from a distance will cause the tag to lose power and drop out of its dialog with the reader. The short-range feature ensures that protected information is not readable unless the tag is very close to a reader antenna.
EM-Marin Microelectronic (acquired Sokymat in 2003)	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		none
	EM4022/P4022	Multifrequency	Read only, 64 Bits		none
	EM4025/EM4125	100~150 kHz	Read only, 55 Bits		none
	EM4026	125 kHz	Read only, 64 Bits		none
	EM4033	13.56 MHz	Read only, 64 Bits	ISO15693	none
	EM4034 (same as EM4035 but no crypto)	13.56 MHz	R/W, 448 Bits	ISO15693	Password (block 0) is never readable but written only in Secure mode. Super User Memory, EAS and Lock Block (block2) can be read by all users but written only in Secure mode. Lock block defines which memory blocks are locked against programming. All user memory words (Blocks 3 to 13) are always readable. Write access rights to User Words (blocks 3 to 11) depend on appropriate Lock Block. Secure mode is enabled by Login command. Login proprietary command is E4 and it checks password stored in block0 - password cannot be read - password can be changed only after a succesful login (Secure Mode).
	EM4035 (same as EM4034 & EM4135 but with crypto)	13.56 MHz	R/W, 3.2K Bits	ISO15693	The 3.2k bit EEPROM memory contained in the chip is organized in 50 words of 64 bits, each word can be irreversibly locked [same as EM4034?].
	V4050	125 KHz	R/W, 1024 Bits		The chip contains 1 KBit of EEPROM which can be configured by the user, allowing a write inhibited area, a read protected area, and a read area output continuously at power on. 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).
	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		none
	V4070	125 kHz	R/W, 160 Bits		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	chip-only	ROM, 64 Bits		none
	EM4083	115~140 kHz	R/W, 512 Bits		none
	P4092	100~150 kHz	Base Stations		-
	EM4094	13.56 MHz	Base Station	ISO15693-14443A/B	-
	EM4095 (old P4095)	125 kHz	Booster Circuits		-
	EM4100 (old H4100 - replaced by EM4200)	100~150 kHz	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)	860~960 MHz	Read only, 64 Bits		none
	EM4124	860~960 MHz	R/W, 176 Bits	ISO18000	32 bit Kill Password (block0+block1), and 32 bit Access Password (block2+block3) [default pwds = 0000'0000'0000'0000]
	EM4126	860~960 MHz	R/W, 224 Bits	ISO18000	none
	EM4133	13.56 MHz	R/W, 512 Bits	ISO15693	Password is located at block0 (it is never readable but written only in Secure mode after a successful Login command). Super User Memory, EAS and the Lock Block area (block2) can be read by all users but written only in Secure mode. Lock block bits define which memory blocks are locked against programming/writing operations. All user memory words (Blocks 3 to 13) are always readable and 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).
	EM4135 (same as EM4035 but no crypto)	13.56 MHz	R/W, 2432 Bits	ISO15693	The 2.4k bit EEPROM memory contained in the chip is organized in 38 words of 64 bits, each word can be irreversibly locked [same as EM4034?].
	EM4150/EM4350 (replaced by EM4450/EM4550)	100~150 kHz	R/W, 1K Bits		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).
	EM4170	125 kHz	R/W, 256 Bits		The chip contains an implementation of a crypto-algorithm with 96 Bits of user configurable secret-key contained in EEPROM. Bits 15 and 14 of word 1 are used as Lock-Bits. The memory can only be accessed for writing or erasing if these two bits have the contents "x0" as when they are delivered. The memory can be unlocked by using the PIN-code command; in that case, the lock-bits are reset from the value "x1" to the value "x0". Words 4 through 9 contain the 96 bits of secret key. These bits influence the crypto-algorithm but cannot be read directly. Words 11 and 12 contain the 32 bits of PINCode. These two words can be written when the lock bits are in unlocked state. They cannot be read out as for the secret key.
	EM4200 (replaces EM4100/4102/4005/4105)	125~134.2 kHz	Read only, 64 Bits	ISO11784/85 Compatible	none
	EM4205/EM4305	125~134.2 kHz	R/W, 512 Bits	ISO11784/85 Compatible	Word 2 contains a 32 bit password. The password value can be changed only after a successful Login command.The 32 bit Password word has to be sent to the chip during a Login command to enable password protected operations. The password word can not be read out with a read word command. There is also a "Read Login Bit": When set to logic 1, the reading of all words, except Words 0 and 1 (manufacturer and UID blocks), by using the Read Word command is protected. Reading any of these words using the Read Word command, can be done upon successful execution of a Login command.There is also a "Write Login Bit": when the Write Login bit is set to logic 1, modification of EEPROM content is protected. Writing any word using Write Word command or changing protection using Protect command, can be done upon successful execution of a login command.
	EM4222	300MHz~2GHz	Read only, 64 Bits		none
	EM4223 (replaces EM4035/EM4135)	800MHz	Read only, 128 Bits		none
	EM4233SLIC	13.56 MHz	R/W, 1K Bits	ISO15693	The enhanced 32 bit password (pwd changeable by write password command only in Secure Mode.) security feature permits a flexible administration of the memory access rights which makes it the right solution for advanced theft protection. In Secure mode (logging with password), the write access to the user's data memory depends on Lock bits only. A pair of bits 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 - Changeable in Secure mode by Protect Page command.
	EM4233 2k	13.56 MHz	R/W, 2K Bits	ISO15693	The customer data privacy and security is guaranteed by a powerful and fast crypto engine implemented in the chip associated with a true random generator and a 96 bit secret key. The enhanced on-chip security feature permits a flexible administration of the memory access rights which makes it the right solution for advanced theft protection. Depending on the application requirements, in terms of security, the user can tailor and adjust the security level by selecting either a true mutual authentication process, a login procedure with a 32 bit password or use the chip as a plain text memory (smartcard).
	EM4237SLIC	13.56 MHz	R/W, 1K Bits	ISO15693	Security features based on a 32-bit password - Advanced NVM management access conditions - Memory blocks/pages Locking mechanism - Lock mechanism for AFI, DSFIS and EAS - Password protected EAS and AFI functionality - Destroy function to deactivate the chip forever.
	EM4237	13.56 MHz	R/W, 2K Bits	ISO15693	Chip Security based on Grain128A crypto algorithm - Mutual Authentication based on challenge/response - Secure Messaging - encryption of the RF communication channel - Message Authentication Code (MAC) - Possibility to select security level based on a 32-bit password - Optional Random ID for enhanced security and privacy - EEPROM blocks/pages Locking mechanisms - Destroy function to deactivate the chip forever.
	EM4269	125 kHz	R/W, 512 Bits	ISO FDX-B	Read and write 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 and write protection
	EM4294	13.56 MHz	Front End	ISO15693/ISO 14443A/B	The reader integrates the crypto algorithm of the EM4035 transponder IC associated with 4 secret keys. Each secret key is 96 bit length and it gives access to the EM4035 tag protected memory after a true mutual authentication process between the tag and the reader. The secret key can not be read by an external evice and their integrity is protected by a 32 bit password.
	EM4298	860~960 MHz	Decoder	ISO18000	UHF Decoder/Encoder circuit, iP-X, ISO 18000-6A/B & C compliant
	EM4322	125kHz+6.8MHz	Read only, 64 Bits		none
	EM4324	860~960 MHz	Read only, 1024 Bits	ISO18000	32-bit password-protected Kill command. 32-bit password-protected Access command. Anti-tearing feature to prevent malicious unlocking
	EM4325	860~960 MHz	R/W, 4096 Bits	ISO18000	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).

Manufacturer	Type/Model Name	Frequency	Description	Standard/Notes	Security
	EM4333	13.56 MHz	R/W, 1K System+4K User+64KCode	ISO15693-ISO14443A	Security thanks to Hardware AES-128-Hardware DES/3DES-Hardware Random Number Generator FIPS140-2. New stream cipher Grain128a with 128-bit key. High secure proprietary crypto with 96 bit key. Hardware Random Number Generator. Three pass mutual authentication according to standard ISO 9798-2. Data authenticity protected with 32 bits MAC. The VICC offers three modes of secure modes: Normal mode used by all users / Safe Access mode granted to power users / Administration mode for card personalization. The Safe Access and Administration mode can be protected by different level of security: - Password protection - Mutual authentication with proprietary crypto compliant with EM Microelectronic HF family - Mutual authentication and MAC using new state-of-the-art stream cipher Grain128a The Grain128a stream cipher uses key length of 128 bits and it allows not only mutual authentication but also message authentication code (MAC) of 32 bits to ensure security of all data transfers. Every page in full 4kB memory can be protected against read or write access separately using protection bits. The protected pages can be then accessed or modified only in Safe Access or Administration mode. Symmetric encryption / decryption algorithm can be achieved using AES, DES and Triple DES on chip HW accelerators. The crypto modes can be used in different modes as EBC, CBC and CTR. AES offers state-of-the-art security with 128 bit key length. DES/3DES offers backward compatibility to previous products.
	EM4350/EM4150	100~150 kHz	R/W, 1K Bits		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).
	EM4369	125 kHz	R/W, 512 Bits	ISO FDX-B	32 bit Password read and write protection. Lock feature convert EEPROM words in read only. All EEPROM words can be write protected by setting lock bits which transform them in read-only.
	EM4444	300MHz-2.4GHz	R/W, 512 Bits		7 pages of user programmable and lockable 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 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).
	EM4469/EM4569 (same as EM4469 with extended range)	100~150 KHz	R/W, 512 Bits	ISO11785 Compatible	Read and write 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 and write protection. The 32 bit Password word has to be sent in Login command to enable password protected operations. the Password word can not be read out by Read Word command. The Protection word protects EEPROM words from being written. Every EEPROM word is protected by a pair of bits in Protection word. Once this bit pair is set to 11 the word cannot be written (it becomes read-only).
	EM4522	125kHz+6.8MHz	R/W, 640 Bits		7 pages of user programmable and lockable memory (64-bit pages).
	EM4550/EM4450 (replaces EM4150/EM4350)	125 kHz	R/W, 1024 Bits		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).
	NF4	13.56 MHz	R/W, 8K/32K/64K Bytes	ISO14443A	The chip security features are based on AES-128 cryptography. In order to enforce the confidentiality level of the data exchanged between the reader and the NF4 chip, the contactless communication can be optionally encrypted including also a Message Authentication Code (MAC). Optional Secure Messaging (SM). Encryption of the RF communication channelThe chip maximizes flexibility in terms of access conditions to memory data.
Atmel (acquired Temic Semiconductor's Integrated Circuit Business in 1998)	TK5530	125 kHz	Read only, 126 Bits		none
	TK5551	125 kHz	R/W, 264 Bits	ISO11784, 11785	The AOR mode is an anti-collision procedure for transponders to read, e.g., ten transponders in the field during 500ms (RF/32, maxblock 2). The number of transponders and the time to read out are dependent on the application. If the AOR mode has been configured by AOR bit at block 0, the transponder remains in sleep mode while putting it into the field. If the specified AOR wake-up command is sent, the dedicated transponder generates an internal RESET (see section “OP Code Formats” in the Atmel e5551 datasheet). Due to the RESET the transponder is woken up. That means, the transponder is able to modulate the field (read mode). The AOR wake-up command consists of the OP code and the 32-bit password. The time duration to send the AOR wake-up sequence is between 8.7ms and 27.5ms according to Figure 10-1. The time duration is dependent on the minimum/maximum values of the measured write-time frames and the content of the password. To select another transponder in the field, it is necessary to end the stop OP code to stop the modulation of the transponder. The blocks can be protected against overwriting by using lock bits.
	e5561	125 kHz	36 Bytes	none	The blocks can be protected against overwriting by using lock bits. One block is reserved for setting the operation modes of the IC: the crypto circuit uses the certified AUT64 algorithm to encrypt the challenge which is written to the e5561. The computed result can be read out by the base station. Comparing the encryption results of the base station and the e5561, a high-security authentification procedure is established. This procedure requires the crypto key of the e5561 and the base station to be equal. The crypto key is stored in blocks 5 to 8 of the EEPROM and can be locked by the user to avoid read out or changes. Another block contains a password to prevent unauthorized writing: If the password (saved at block9) protection is enabled, the e5561 remains in ID mode even if it has received a correct write sequence. The only possible operation is to modify the content of block 9 by sending the correct password bits. In all other cases, an error handling procedure is started and the e5561 enters ID mode. A lock-bit is a physical part of the EEPROM's content and is under user control. The lock-bit protection mechanism has two different effects: • Avoid programming (modifying data) of the EEPROM's blocks • Avoid reading out the crypto key from the EEPROM using the direct-access mode If the base station tries to read out the crypto key and the corresponding lock-bit is set, the e5561 will enter ID mode immediately. Once the crypto key lock-bit is set, the crypto key can not be modified or read out any more. There are several lock-bits available, each affecting a special data region of the EEPROM. The main groups of lock-bits are: • Lock-bits to inhibit programming of the specified blocks of the EEPROM • Lock-bits to inhibit programming of the specified blocks of a specific address range In both cases, an attempt to modify a data region protected by a lock-bit will cause an error handling procedure (i.e., the e5561 enters ID mode).
	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 obtain a password to prevent unauthorized writing
	ATA5551	125 KHz	R/W, 264 Bits		The AOR mode is an anti-collision procedure for transponders to read, e.g., ten transponders in the field during 500ms (RF/32, maxblock 2). The number of transponders and the time to read out are dependent on the application. If the AOR mode has been configured by AOR bit at block 0, the transponder remains in sleep mode while putting it into the field. If the specified AOR wake-up command is sent, the dedicated transponder generates an internal RESET (see section “OP Code Formats” in the Atmel e5551 datasheet). Due to the RESET the transponder is woken up. That means, the transponder is able to modulate the field (read mode). The AOR wake-up command consists of the OP code and the 32-bit password. The time duration to send the AOR wake-up sequence is between 8.7ms and 27.5ms according to Figure 10-1. The time duration is dependent on the minimum/maximum values of the measured write-time frames and the content of the password. To select another transponder in the field, it is necessary to end the stop OP code to stop the modulation of the transponder. The blocks can be protected against overwriting by using lock bits.
	T/TK/5552	125 KHz	R/W, 1024 Bits	ISO11784, 11785	Bit 0 of every block is the lock bit for that block. Once locked, the block (including the lockbit itself) cannot be field-reprogrammed.
	T5554	100-150 KHz	R/W, 264 Bits	ISO11784, 11785	Blocks 1 to 6 are freely programmable. Block 7 may be used as a password. If password protection is not required, it may be used for user data. When password mode is on (usePWD = 1), the first 32 bits after the OP-code are regarded as the password. They are compared bit-by-bit with the contents of block 7, starting at bit 1. If the comparison fails, the IC will not program the memory, but restart in read mode at block 1 once writing has completed. Notes: (1) If PWD is not set, but the IC receives a write datastream containing any 32 bits in place of a password, the IC will enter programming mode. (2) In password mode, MAXBLK should be set to a value below 7 to prevent the password from being transmitted by (3) Every transmission of 2 OP-code bits, 32 password bits, one lock bit, 32 data bits and 3 address bits (= 70 bits) needs about 35 ms. Testing all 232 possible combinations (about 4.3 billion) takes about 40,000 h, or over four years. This is a sufficient password protection for a general-purpose IDIC. Bit 0 of every block is the lock bit for that block. Once locked, the block (including the lockbit itself) cannot be field-reprogrammed.
	T5556	125 KHz	R/W, 256OTP+224 Bits		Bit 0 of every block is the lock bit for that block. Once locked, the block (including the lockbit itself) cannot be modified again during configuration.
	ATA5557	100-150 KHz	R/W, 330 Bits		In password mode (PWD bit set), the direct access to a single block needs the valid 32-bit password to be transmitted. Bit 0 of every 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 again.
	ATA5558	125 kHz	1344 Bits (1024+320)	ISO11784, 11785	Password Protection - The user memory is subdivided into continuous page areas which can be configured so that write or read/write operations on blocks within these pages can only be carried out after the appropriate password has been transmitted to the tag (LoginRead or LoginWrite command). The read and write password protections are independent and user definable. The read and write passwords are found in blocks 54 and 55 and the page security levels are defined in the Page Security register of block 62. - Lock Bit - Each memory block, consists of 32 data bits and an associated lock bit. Once a block is locked (lock bit = 1), the entire block including the lock bit itself can no longer be reprogrammed. - Master Key - The Master Key controls various operating modes as described in Table 2-2. For production test purposes, other Master Key codes are used, but once the Configuration block has been double locked these test functions can never be reactivated. If the Master Key is set to 0110, the blocks within the system memory section have different access protection (see Figure 2-5 on page 7). These access rights are fixed and not influenced by the Page Security Register. Access to password protected system memory blocks can only be performed after the corresponding LoginWrite or LoginRead has been successfully executed. The password blocks themselves are non-readable. Traceability and configuration can always be read but the traceability data cannot be altered. A new ATA5558 device, when received by the customer can be considered as being unprogrammed (all 0 state), the only exception to this being the preprogrammed non-alterable traceability information. For the tag manufacturer to be able to easily set up the tag passwords, it is possible to provisionally switch the password protection off. i.e Master Key = 0. In this state, it is possible to read and write all non-locked (lock bits = 0) memory blocks irrespective of the page security. In this way, new tag passwords or Tag ID’s can be defined and written. Blocks, which have once been locked (block lock bit = 1) can however not be rewritten. When the customer has completed the tag configuration, the Master Key is set to the “safe” state (= 6) thus enabling the full password protection, and then finally the configuration block itself may be locked. In this double locked condition, the configuration and all other locked blocks are irreversibly set and cannot be changed. This applies to both the user and the majority of the system memory blocks.
	TK5561A-PP	125 kHz	128 bits	ISO11784, 11785	The on-chip non-volatile memory of the 320-bit EEPROM (10 blocks, 32 bits each) can be read and written blockwise by a read/write base station, e.g. based on the U2270B. Up to four blocks consisting of the user programmable ID code, the crypto key and configurations are stored in six blocks. The crypto key and the ID code can be individually protected against overwriting.
	ATA5567 (upgraded version of ATA5557)	100-150 KHz	R/W, 330 Bits		In password mode (PWD bit set), the direct access to a single block needs the valid 32-bit password to be transmitted. Bit 0 of every 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 again). In Temic datasheet a diagram mention the word "password" but it should be an error/typo.
	ATA5570	125 kHz	RW, 330 Bits	ISO11784, 11785	In password mode (PWD bit set), the direct access to a single block needs the valid 32-bit password to be transmitted. Bit 0 of every 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 again.
	ATA5577 (replaces ATA5567/T5557/TK5551)	125 KHz	R/W, 363 Bits	ISO11784/85 Compatible	Password - When password mode is active (PWD = 1), the first 32 bits after the opcode are regarded as the password. They are compared bit by bit with the contents of block 7, starting at bit 1. If the comparison fails, the ATA5577 will not program the memory, instead it will restart in regular- read mode once the command transmission is finished. Note: In password mode, MAXBLK should be set to a value lower than 7 to prevent the password from being transmitted by the ATA5577. Each transmission of the direct access command (two opcode bits, 32-bit password, '0' bit plus 3 address bits = 38 bits) needs about 18 ms. Testing all possible combinations (about 4.3 billion) would take about two years. Each block includes a single Lock bit (bit0) which is responsible for write-protecting the associated block. Once locked, the block (including the lock bit itself) is not re-programmable via the RF field - OTP Functionality - If the OTP bit is set to 1, all memory blocks are write protected and behave as if all lock bits are set to 1. If, in addition, the master key is set to 6, the ATA5577 mode of operation is locked forever (one-time-programming functionality). If the master key (bits form b1 to b4) is set to 9, the test-mode access allows the re-configuration of the tag.
	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 byte (byte 16) and are able to prevent the whole memory of the Atmel ATA5575M1 from reprogramming. As long as the lock bits are set to '00000b' the memory is alterable and the device can be programmed by the customer. In this case the Atmel ATA5575M1 sends out dummy data (UNIQUE format with header and all digits set to '0'; By setting the lock bits to '01101b' the whole memory is locked and cannot be altered. After Reset the Atmel ATA5575M1 enters regular read mode and sends out the programmed user data. Consequently the user of a Transponder with an Atmel ATA5575M1 can be sure that the device is locked if the programmed data are read out after reset. In delivery state the lock bits are programmed to '00000b'. All other combinations of bit 1 - bit 5 are not defined and may lead to malfunction of the IC.
	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 byte (byte 16) and are able to prevent the whole memory of the Atmel ATA5575M1 from reprogramming. As long as the lock bits are set to '00000b' the memory is alterable and the device can be programmed by the customer. In this case the Atmel ATA5575M1 sends out dummy data (UNIQUE format with header and all digits set to '0'; By setting the lock bits to '01101b' the whole memory is locked and cannot be altered. After Reset the Atmel ATA5575M1 enters regular read mode and sends out the programmed user data. Consequently the user of a Transponder with an Atmel ATA5575M1 can be sure that the device is locked if the programmed data are read out after reset. In delivery state the lock bits are programmed to '00000b'. All other combinations of bit 1 - bit 5 are not defined and may lead to malfunction of the IC.

Manufacturer	Type/Model Name	Frequency	Description	Standard/Notes	Security
	AT88RF001	13.56 MHz	R/W, 256 Bits	ISO14443B	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 password validation. The bits within the LockBits field correspond to the pages within 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 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 command is permitted.
	AT88RF020	13.56 MHz	256 Bytes	ISO14443B	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 password validation. The bits within the LockBits field correspond to the pages within 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 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 command is permitted.
	AT88RF256	125kHz	R/W, 32 Bytes		Password and Write Lock Protection. ID lenght programmable (4-19 bytes)
	AT88SC0104CRF CRYPTO	13.56 MHz	128 Bytes	ISO14443B	- Symmetrical Dynamic Mutual Authentication with 64-bit Cryptographic Keys ((under exclusive patent license from ELVA)) - Encrypted Passwords with Attempts Counters - Stream Encryption Ensures Data Privacy - Four Key Sets for Authentication and Encryption - Eight Sets of two 24-bit Passwords - Selectable Access Rights by Zone - Write Lock Mode - Tamper Sensors
	AT88SC0204CRF CRYPTO	13.56 MHz	256 Bytes	ISO14443B	
	AT88SC0404CRF CRYPTO	13.56 MHz	512 Bytes	ISO14443B	
	AT88SC0808CRF CRYPTO	13.56 MHz	1024 Bytes	ISO14443B	
	AT88SC1616CRF CRYPTO	13.56 MHz	2048 Bytes	ISO14443B	
	AT88SC3216CRF CRYPTO	13.56 MHz	4096 Bytes	ISO14443B	
	AT88SC6416CRF CRYPTO	13.56 MHz	8192 Bytes	ISO14443B	
NXP (Philips)	MIFARE Ultralight (MF0ICU1)	13.56 MHz	R/W, 64 Bytes	ISO14443A	Lock bytes (block2) - 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 - 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.
	MIFARE Ultralight EV1 (MF0ULx1)	13.56 MHz	R/W, 128 Bytes	ISO14443A	3 independent 24-bit true one-way counters - Field 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 unintended memory operations.
	MIFARE Ultralight C (MF0ICU2)	13.56 MHz	R/W, 192 Bytes	ISO14443A	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 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. 3DES Authentication proves that two entities have the same secret and each entity can be seen as a reliable partner for the coming communication. The applied encryption algorithm ek() is 2 key 3DES encryption.
	MIFARE Mini (MF1ICS20)	13.56 MHz	R/W, 320 Bytes	ISO14443A	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 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 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 - AES-128 used for authenticity and integrity - Anti-tearing mechanism for writing AES keys - Keys can be stored as MIFARE
	MIFARE Plus S 4K (MF1SPLUS8001/8011/8031)	13.56 MHz	R/W, 4K Byte; UID: 7Bytes	ISO14443A / AES encryption	
	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 - AES-128 used for authenticity and integrity - Anti-tearing mechanism for writing AES keys - Keys can be stored as MIFARE
	MIFARE Plus X 4K (MF1PLUS8001/8011/8031)	13.56 MHz	R/W, 4K Byte; UID: 7Bytes	ISO14443A / AES encryption	
	MIFARE Classic S50 (MF1ICS50)	13.56 MHz	R/W, 1K Bytes	ISO14443A	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 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 S70 (MF1ICS70)	13.56 MHz	R/W, 4K Bytes	ISO14443A	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 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	Manufacturer programmed 7-byte UID or 4-byte NUID identifier for each device - Random ID support - Mutual three pass authentication (ISO/IEC DIS 9798-2) - • 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 authentication (ISO/IEC DIS 9798-2) - • Individual set of two keys per sector to support multi-application with key hierarchy
	MIFARE DESFire V0.6 (MF3ICD40)	13.56 MHz	R/W, 4K Bytes	ISO14443A	- 3DES w/ 112-bit key for authentication and data encryption - 14 keys per application + 1 master key - Access rights on file level - Based on asynchronous 8051 w/ 3DES engine - Analytical attacks not possible but Side-channel attacks are possible - 3-pass mutual authentication based on the crypto used. - Confidentiality En/Decryption based on crypto used.
	MIFARE DESFire EV1 (MF3ICD21/MF3ICD41/MF3ICD81) (MF31CDH21/MF31CDH31/MF31CDH41)	13.56 MHz	R/W, 2K/4K/8K Bytes	ISO14443A	- 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. - 3-pass mutual authentication based on the crypto used. - Confidentiality En/Decryption based on crypto used.
	MIFARE ProX P8RF6x	13.56 MHz	R/W, 4-16 KBytes+OS	ISO7816+ISO14443A	
	SmartMX P5Sxxxx	13.56 MHz	R/W, 10-72 KBytes+OS	ISO7816+ISO14443A	
	SmartMX P5Cxxx	13.56 MHz	R/W, 10-72 KBytes+OS	ISO7816+ISO14443A	
	I.CODE1 (SL1ICS30)	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 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.
	I.CODE1 (SL1ICS31)	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 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.
	I.CODE UID (SL2ICS11)	13.56 MHz	R/W, 192 Bits		none
	I.CODE SLI (SL2ICS20)	13.56 MHz	R/W, 1024 Bits	ISO15693	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 never be written to from this moment on.
	I.CODE SLI – L (SL2ICS50)	13.56 MHz	R/W, 512 Bits	ISO15693	Password protected Label Destroy: With the 32-bit destroy password an addressed label can be destroyed with the Destroy command. 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 Mode 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 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 user memory block (write protection).
	I.CODE SLI – L HC (SL2ICS51)	13.56 MHz	R/W, 512 Bits	ISO15693	Password protected Label Destroy: With the 32-bit destroy password an addressed label can be destroyed with the Destroy command. 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 Mode 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 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 user memory block (write protection).
	I.CODE SLI – S (SL2ICS53)	13.56 MHz	R/W, 2048 Bits	ISO15693	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 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 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 Mode 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 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 user memory block (write protection).
	I.CODE SLI – S HC (SL2ICS54)	13.56 MHz	R/W, 2048 Bits	ISO15693	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 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 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 Mode 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 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 user memory block (write protection).
	I.CODE SLIX (SLS2002/SLS2102)	13.56 MHz	R/W, 1024 Bits	ISO15693/ISO18000-3	Password protected EAS and AFI functionality: The 32-bit EAS/AFI password enables the addressed label to be set in a mode where 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).
	I.CODE SLIX-L (SLS5002/SLS5102)	13.56 MHz	R/W, 512 Bits	ISO15693/ISO18000-3	Password protected Label Destroy: The 32-bit Destroy password enables an addressed label to be destroyed with the DESTROY SLIX-L command. That status is irreversible 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 PRIVACY command. In 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 protected EAS and AFI functionality: The 32-bit EAS/AFI password enables the addressed label to be set in a mode where 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).

Manufacturer	Type/Model Name	Frequency	Description	Standard/Notes	Security
	I.CODE SLIX-S (SLS5302/SLS5402)	13.56 MHz	R/W, 512 Bits	ISO15693/ISO18000-3	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 counterfeiting) - Password protected Label Destroy: The 32-bit Destroy password enables an addressed label to be destroyed with the DESTROY SLIX-S command. That status is irreversible 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 PRIVACY command. In 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 protected EAS and AFI functionality: The 32-bit EAS/AFI password enables the addressed label to be set in a mode where the EAS status, the EAS ID and/or 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).
	I.CODE 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 each user memory block (write protection).
	I.CODE ILT-M (SL2S1412/1512/1612)	13.56 MHz	R/W, 510 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. The user memory can be write locked, permanently write locked, unlocked, permanently unlocked or block permalocked.
	I.CODE EPC (SL2ICS10)	13.56 MHz	R/W, 136 Bits	EPC	Lock mechanism for each user memory block (write protection).
	I.CODE UID (SL2ICS11)	13.56 MHz	R/W, 192 Bits	EPC	Label destroy command with 24 bit destroy code protection.
	I.CODE UID-OTP (SL2ICD12)	13.56 MHz	R/W, 192 Bits	EPC	Memory is OTP. Label destroy command with 24 bit destroy code protection.
	HITAG1 HT1ICS30 (Vegas)	125 KHz	R/W, 256 Bytes		Encryption, authentication, 2x32 Bit passwords.Parts of memory can be write protected by the user.
	HITAG1 HT1DC20S30	125 KHz	R/W, 2048 Bits		Encryption, authentication, 2x32 Bit passwords.Parts of memory can be write protected by the user.
	HITAG2 HT2ICS20	125 KHz	R/W, 32 Bytes	ISO11784/11785	Encryption, authentication, 16 Bit KeyHigh and 48 Bit KeyLow; 2 passwords (32 and 24 Bit); 5 Modes: Crypto = r/w using crypted transmission; Password = r/w in plain text previous password check; A = EM4100 - B = Animal ID; C = PCF793x. HITAG 2 is the name 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 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 Generation Crypto Code" for this type of transponder.
	HITAG2 HT2DC20S20	125 kHz	R/W, 32 Bytes	ISO11784/11785	Encryption, authentication, 16 Bit KeyHigh and 48 Bit KeyLow; 2 passwords (32 and 24 Bit); 5 Modes: Crypto = r/w using crypted transmission; Password = r/w in plain text previous password check; A = EM4100 - B = Animal ID; C = PCF793x.
	HITAG S HTSICH32	125 kHz	Read Only, 32 Bits	ISO11784/11785	none
	HITAG S HTSICH56	125 kHz	R/W, 256 Bits	ISO11784/11785	32 Bit Unique Identification Number (UID); 48 Bit secret key based encrypted authentication. Secure Memory Lock (r/w) functionality.
	HITAG S HTSICH48	125 kHz	R/W, 2048 Bits	ISO11784/11785	32 Bit Unique Identification Number (UID); 48 Bit secret key based encrypted authentication. Secure Memory Lock (r/w) functionality.
	HITAG µ HTMS1001	125 KHz	R/W, 128 Bits	ISO14223	Memory Lock functionality - 32-bit password feature.
	HITAG µ Advanced HTMS1001	125 KHz	R/W, 512 Bits	ISO14223	Memory Lock functionality - 32-bit password feature.
	HITAG µ Advanced+ HTMS1x01/HTMS8x01	125 KHz	R/W, 1760 Bits	ISO14223	Memory Lock functionality - 32-bit password feature.
	HITAG RO HTCICC640x	125 kHz	Read only, 64 Bits	ISO11784/11785	none
	PCF7900/PCH7900	315/434/869/915 MHz			Fractional-N Transmitter IC (FraNTIC).
	PCF7930	125 kHz	R/W, 1024		Write lock mechanism (reversible) [excluded block1]. Password (56 bits) to protect from writing (may be readable or not). This 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. Because of this, almost all car manufacturers have implemented their own scheme.
	PCF7931	125 KHz	R/W, 1024		Write lock mechanism (reversible) [excluded block1]. Password (56 bits) to protect from writing (may be readable or not). This 1st generation type transponder implements the read capabilities of the PIT protocol. As this transponder is OTP, there is no option of using a synchronization code scheme.
	PCF7935	125 KHz	R/W, 1152		Write lock mechanism (reversible) [excluded block1]. Password (56 bits) to protect from writing (may be readable or not). Additional shadow memory (not present in PCF731). It implements the SECT protocol which is a simple challenge/response protocol, using a not specified cipher.
	PCF7936 (Hitag2)	125 KHz	?		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 HITAG2 transponder and does not have any UHF capabilities. Hence, it is used solely for immobilizers. UID scheme: XX XX XX 1X.
	PCF7937 (Hitag2 Extended)	?	?		?
	PCF7938 (HITAG-Pro)	?	R/W, 448 Bytes		96-bit secret key.
	PCF7939 (HITAG-Pro)	?	?		AES-128-Bit.
	PCF7941/21 (Hitag2)	Remote keyless entry	?		This transponder includes UHF capabilities and a RISC Controller with a 4 kB ROM that is used to program keyless entry features. Transponders of this type are also termed "STARC lite" (Security Transponder and RISC Controller).
	PCF7942/43/44 (Hitag2)	?	?		PCF7942/43/44 This transponder includes UHF capabilities and a RISC Controller with an 8 kB ROM for programming keyless entry features. Transponders of this type are also called "STARC" (Security Transponder and RISC Controller). UID scheme: XX XX XX 4X.
	PCF7945 (Hitag2)	Remote keyless entry	?		This transponder uses an updated protocol version (in comparison with PCF7941/42) to communicate via UHF for keyless entry purposes. The immobilization features are the same as above.
	PCF7946/47 (Hitag2)	?	?		In contrast to the STARC based transponders, this transponder does not have a RISC controller and instead features a built-in rolling code generator for keyless entry. UID scheme: XX XX XX 2X.
	PCF7952 (HITAG-Pro)	Keyless entry/go	?		This transponder is the first for keyless-go applications and again offers a RISC controller. UID scheme: XX XX XX 7X.
	PCF7953 (Hitag2)	Keyless entry/go	?		?
	PCF7961/22 (Hitag2)	Remote keyless entry	?		?
	NCF2940	Remote keyless entry	?		?
	NCF2950	Keyless entry/go	?		?
	NCF2970	Keyless entry/go	?		?
	UCode HSL (SL3ICS3001)	860~960MHz/2.45GHz	R/W, 256 Bytes	ISO18000	Lock mechanism (write protection) for each byte
	UCode EPC v1.19 (SL3ICS10)	860~960MHz/2.45GHz	R/W, 96+256 Bits	ISO18000	32-bit access password - 32-bit kill password
	UCode EPC G2 (SL3ICS10)	860~960 MHz	R/W, 64 Bytes	ISO18000	32-bit kill password to permanently disable the tag - 32-bit access password to allow a transition into the secured transmission state. Lock mechanism (write protection) for individual passwords and individual memory banks allow for permanent lock (permalock) status of a password or memory bank.
	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.
	UCode G2iM/+ (SL3S1003/1013)	840~960 MHz	R/W, 256 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.
	UCode G2XM (SL3ICS1002)	860~960 MHz	R/W, EPC 240 Bit, TID 64 Bits	ISO18000-6	- Read Protect: protects all memory content including CRC16 from unauthorized reading. - 32-bit kill password to permanently disable the tag - 32-bit access password to allow a transition into the secured transmission state.
	UCode G2XL (SL3ICS1202)	860~960 MHz	R/W, 64+240 Bits	ISO18000-6	- Read Protect: protects all memory content including CRC16 from unauthorized reading. - 32-bit kill password to permanently disable the tag - 32-bit access password to allow a transition into the secured transmission state.
	UCode 7 (SL3S1204)	860~960 MHz	none	ISO18000-6	32-bit kill password to permanently disable the tag - 32-bit access password.
	UCode I2C (SL3S4011/4021)	860~960 MHz/I2C	R/W, 3328 Bits	ISO18000-6	Memory read protection - 32-bit KILL password to permanently disable the tag - 32-bit ACCESS password to allow a transition into the secured transmission state.
	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.
	NTAG210	13.56 MHz	R/W, 80 Bytes	ISO14443A	Capability container with one time programmable bits - Field 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.
	NTAG212	13.56 MHz	R/W, 164 Bytes	ISO14443A	Capability container with one time programmable bits - Field 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.
	NTAG213	13.56 MHz	R/W, 180 Bytes	ISO14443A	Field programmable read-only locking function per page for the first 16 pages - Field programmable read-only locking function above the first 16 pages per double page.
	NTAG215/215F	13.56 MHz	R/W, 540 Bytes	ISO14443A	Field programmable read-only locking function per page for the first 16 pages - Field programmable read-only locking function per 16 pages. Configurable password protection with optional limit of unsuccessful attempts - Anti-tearing support for capability container (CC) and lock bits - ECC supported originality check.
	NTAG216/216F	13.56 MHz	R/W, 924 Bytes	ISO14443A	Field programmable read-only locking function per page for the first 16 pages - Field programmable read-only locking function per 16 pages. Configurable password protection with optional limit of unsuccessful attempts - Anti-tearing support for capability container (CC) and lock bits - ECC supported originality check.
	NTP3xxx	13.56 MHz	???	ISO14443A	Activison game item (ex. Skylanders)
LEGIC	Prime MIM256	13.56 MHz	R/W, 256 Bytes	LEGIC RF Standard (failed ISO14443F)	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 cryptography.
	Prime MIM1024	13.56 MHz	R/W, 1024 Bytes	LEGIC RF Standard (failed ISO14443F)	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 cryptography.
	ATC128MV	13.56 MHz	R/W, 128 Bytes	ISO15693	3DES, DES, LEGIC encryption; 96 Bit cryptographic authentication.
	ATC256MV	13.56 MHz	R/W, 256 Bytes	ISO15693	3DES, DES, LEGIC encryption; 96 Bit cryptographic authentication.
	ATC512MV	13.56 MHz	R/W, 512 Bytes	ISO15693	3DES, DES, LEGIC encryption; 64 Bit cryptographic authentication.
	ATC1024MV	13.56 MHz	R/W, 1024 Bytes	ISO15693	3DES, DES, LEGIC encryption; 64 Bit cryptographic authentication.
	ATC2048MV	13.56 MHz	R/W, 2048 Bytes	ISO15693	3DES, DES, LEGIC encryption; 64 Bit cryptographic authentication.
	ATC4096MV	13.56 MHz	R/W, 4096 Bytes	ISO15693	3DES, DES, LEGIC encryption; 64 Bit cryptographic authentication.
	ATC512MP	13.56 MHz	R/W, 512 Bytes	ISO14443	3DES, DES, LEGIC encryption; 64 Bit cryptographic authentication.
	ATC1024MP	13.56 MHz	R/W, 1024 Bytes	ISO14443	3DES, DES, LEGIC encryption; 64 Bit cryptographic authentication.
	ATC2048MP	13.56 MHz	R/W, 2048 Bytes	ISO14443	3DES, DES, LEGIC encryption; 64 Bit cryptographic authentication.
	ATC4096MP	13.56 MHz	R/W, 4096 Bytes	ISO14443	3DES, DES, LEGIC encryption; 64 Bit cryptographic authentication.
	AFS4096JP	13.56 MHz	R/W, 4096 Bytes	ISO14443A	AES (128/256 Bit), 3DES, DES, LEGIC encryption. 112 Bit cryptographic authentication.
	CTC4096MP	13.56 MHz	R/W, 1002/2984 Bytes	ISO14443A/LEGIC RF Standard	AES (128/256 Bit), 3DES, DES, LEGIC encryption. 112 Bit cryptographic authentication.
Infineon	SLE 44R35/T/S	13.56 MHz	R/W, 1K Bytes	ISO14443A	Mifare compatible

Manufacturer	Type/Model Name	Frequency	Description	Standard/Notes	Security
	SLE 55R01	13.56 MHz	R/W, 160 bytes	ISO14443A	- 2-way authentication with 64-bit secret key between reader and card - 2 keys for each sector allow hierarchical key management - 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) - Access protection of EEPROM by transport keys on chip delivery
	SLE 55R04	13.56 MHz	R/W, 770 bytes	ISO14443A	- 2-way authentication with 64-bit secret key between reader and card - 2 keys for each sector allow hierarchical key management - 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) - Access protection of EEPROM by transport keys on chip delivery
	SLE 55R04E my-d™ prox-enhanced	13.56 MHz	R/W, 6160 Bits	ISO14443A	- 2-way authentication with 64-bit secret key between reader and card - 2 keys for each sector allow hierarchical key management - 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) - Access protection of EEPROM by transport keys on chip delivery
	SLE 55R08	13.56 MHz	R/W, 1280 bytes	ISO14443A	- 2-way authentication with 64-bit secret key between reader and card - 2 keys for each sector allow hierarchical key management - 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) - Access protection of EEPROM by transport keys on chip delivery
	SLE 55R16	13.56 MHz	R/W, 2560 bytes	ISO14443A	- 2-way authentication with 64-bit secret key between reader and card - 2 keys for each sector allow hierarchical key management - 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) - Access protection of EEPROM by transport keys on chip delivery
	SLE 55R16E my-d™ prox-enhanced	13.56 MHz	R/W, 20480 Bits	ISO14443A	"- 2-way authentication with 64-bit secret key between reader and card - 2 keys for each sector allow hierarchical key management - 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) - 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	Individual locking of blocks / pages (read only) - State-of-the-art challenge and response security algorithm (mutual authentication) - 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 code (MAC) verifying data access - Transport Key at chip delivery.
	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	ISO15693	
	SRF 55V02S HC my-d™ vicinity secure	13.56 MHz	R/W, 256 bytes	ISO15693	
	SRF 55V10P my-d™ vicinity	13.56 MHz	R/W, 1024 bytes	ISO15693	
	SRF 55V10P HC my-d™ vicinity	13.56 MHz	R/W, 1024 bytes	ISO15693	
	SRF 55V10S my-d™ vicinity secure	13.56 MHz	R/W, 1024 bytes	ISO15693	
	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	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)	13.56 MHz	R/W, 152 Bytes	ISO14443A	• 32 bit of One Time Programmable (OTP) memory area • Locking mechanism for each block • Block Lock mechanism • Optional 32 bit Password for Read/Write or Write access • Optional Password Retry Counter • Optional 16 bit Value Counter
	SLE 66R01P/PN my-d™ move (PN is already NFC initialized)	13.56 MHz	R/W, 152 Bytes	ISO14443A	
	SLE 66R04P my-d™ NFC	13.56 MHz	R/W, 616 Bytes	ISO14443A	
	SLE 66R16P my-d™ NFC	13.56 MHz	R/W, 2048 Bytes	ISO14443A	
	SLE 66R32P my-d™ NFC	13.56 MHz	R/W, 4096 bytes	ISO14443A	
	SLE 66R04S my-d™ proximity 2	13.56 MHz	R/W, 512 bytes	ISO14443A	- State-of-the-art challenge and response security algorithm - 2-way mutual authentication with 64-bit secret key between reader and card for basic security - 2 keys for each sector enable hierarchical key management - Multi-level security structure possible
	SLE 66R16S my-d™ proximity 2	13.56 MHz	R/W, 2048 bytes	ISO14443A	
	SLE 66R32S my-d™ proximity 2	13.56 MHz	R/W, 4096 bytes	ISO14443A	
	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 - 48-bit key length - 2 keys per sector enabling key management - Transport key at chip delivery - Selective memory access secured by authentication and access conditions - Suited to multifunctional applications: individual key sets for each EEPROM sector
	SLE 66R35I (Mifare compatible 4Bytes non-unique UID)	13.56 MHz	R/W, 1K Bytes	ISO14443A	
	SLE 66R35R (Mifare compatible 4Bytes Reused UID)	13.56 MHz	R/W, 1K Bytes	ISO14443A	
	SLE 66R35E7 (Mifare compatible 7Bytes UID)	13.56 MHz	R/W, 1K Bytes	ISO14443A	
	SLE 66CLXXPE (security IC / Crypto)	13.56 MHz	R/W, 4K/8K/16K/18K/36K/78K/80K Bytes	ISO14443A/B+contact	- Certified True Random Number Generator with firmware test function supporting AIS-31 requirements - Dual Key Triple DES (DDES) Accelerator - 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) - Elliptic 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 prevent unauthorised write to memory
	SRF66V10ST	13.56 MHz	R/W, 10K Bits	ISO/IEC 18000-3 Mode 2	
	SRF66V01ST	13.56 MHz	R/W, 1280 Bits	ISO/IEC 18000-3 Mode 2	?
ST Microelectronics	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.
	SRI512	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 protected counter block behaves like a ROM block).
	SRIX512	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. Possible mutual authentication with specific reader (provided with CRX14 chip - proprietary algorithm). 2 Count-Down Binary Counters (blocks 5 and 6) with automated anti-tearing protection (a protected counter block behaves like a ROM block).
	SRI2K	13.56 MHz	R/W, 1024 Bits	ISO14443B	Blocks from 7 to 15 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 (7 to 15) cannot be unprotected. 2 Count-Down Binary Counters with automated anti-tearing protection.
	SRI4K	13.56 MHz	R/W, 4096 Bits	ISO14443B	Blocks from 7 to 15 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 (7 to 15) cannot be unprotected. 2 Count-Down Binary Counters with automated anti-tearing protection.
	SRIX4K	13.56 MHz	R/W, 4096 Bits	ISO14443B	Blocks from 7 to 15 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 (7 to 15) cannot be unprotected. Possible mutual authentication with specific reader (provided with CRX14 chip - proprietary algorithm). 2 Count-Down Binary Counters with automated anti-tearing protection.
	SRT512	13.56 MHz	R/W, 512 Bitss	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 protected counter block behaves like a ROM block). [Differences from SRI512: SRT512 is not provided with resettable OTP area].
	LRI64	13.56 MHz	R/W, 120 Bits (UID)	ISO15693 with WORM User Area	Blocks from 10 to 14 are write-once read-many (WORM) memory. It is possible to write to each of them once; after the first valid write access, the block is automatically locked, and only read commands are possible.
	LRIS64K	13.56 MHz	R/W, 64K+120 Bits (UID)	ISO15693 with WORM User Area	Each sector can be individually read and/or write protected by one out of three available passwords. A sector provides 32 blocks of 32 bits; each read and write access are done by block. Read and write block accesses are controlled by a Sector Security Status byte that defines the access rights to all the 32 blocks contained in the sector. If the sector is not protected, a Write command updates the complete 32 bits of the selected block. Each memory sector of the LRIS64K is assigned with a Sector security status byte including a Sector Lock bit, two Password Control bits and two Read/Write protection bits; the protection of a locked sector cannot be changed.on delivery, the three default password values are set to 0000 0000h and are activated.
	LRI1K	13.56 MHz	R/W, 1024 Bits	ISO15693	Lock Block command to permanently locks the selected block. Kill command available.
	LRI2K	13.56 MHz	R/W, 2048 Bits	ISO15693	Lock Block command to permanently locks the selected block. Kill command available.
	LRIS2K	13.56 MHz	R/W, 2048 Bits	ISO15693	Each sector can be individually read and/or write protected by one out of three available passwords. A sector provides 32 blocks of 32 bits; each read and write access are done by block. Read and write block accesses are controlled by a Sector Security Status byte that defines the access rights to all the 32 blocks contained in the sector. If the sector is not protected, a Write command updates the complete 32 bits of the selected block. Each memory sector of the LRIS64K is assigned with a Sector security status byte including a Sector Lock bit, two Password Control bits and two Read/Write protection bits; the protection of a locked sector cannot be changed.on delivery, the three default password values are set to 0000 0000h and are activated.
	ST13 family replaced by ST21 family	13.56+contact		ISO14443B	?
	ST16R820	13.56MHz	R/W, 576 Bytes	ISO14443B	Protected One Time Programmable block (32 or 64 bytes)
	ST16RF52	13.56 MHz	R/W, 2Kb	ISO14443B	Protected One Time Programmable block (32 or 64 bytes)
	ST16RF58	13.56 MHz	R/W, 8Kb	ISO14443B	Protected One Time Programmable block (32 or 64 bytes)
	ST19WR02 (ST19 family replaced by ST23 family)	13.56+contact	R/W, 2Kb	ISO14443B/B'	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.U.N. registers (Generators of Unpredictable Number).
	ST19XR04	13.56+contact	R/W, 4Kb	ISO14443B/B'	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.U.N. registers (Generators of Unpredictable Number).
	ST19XR08/ST19WR08	13.56+contact	R/W, 8Kb	ISO14443B/B'	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.U.N. registers (Generators of Unpredictable Number).

Manufacturer	Type/Model Name	Frequency	Description	Standard/Notes	Security
	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.U.N. registers (Generators of Unpredictable Number). Enhanced NESCRYPT crypto-processor for public key cryptography.
	ST19XR34	13.56+contact	R/W, 34Kb	ISO14443B/B'	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.U.N. registers (Generators of Unpredictable Number). 1088 Bit Modular arithmetic processor with library support for asymmetrical algorithms - Fast modular multiplication and squaring using Montgomery method - Software Crypto libraries in separate ST ROM area for efficient algorithm coding using a set of advanced functions - Software selectable operand length up to 2176 bits.
	MR31	13.56+contact	R/W, 16K, 22K, 38K, 52K Bytes	ISO14443A/B/B'	- Three-key Triple DES accelerator - AES accelerator - NESCRYPT coprocessor for public key cryptography algorithm - Protection against multiple attacksThe SR31Z052 features 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 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'	
	M24LR04/16/64E-R	13.56+I2C	R/W, 4K, 16K, 64K Bytes	ISO15693	Lock-sector command sets the access rights and permanently locks the selected sector (1 sector = 32 blocks). Multiple password protection in RF mode - 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.
	M24LR64-R	13.56+I2C	R/W, 65536 Bits	ISO15693	"Lock-sector command sets the access rights and permanently locks the selected sector (1 sector = 32 blocks). Multiple password protection in RF mode - 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."
	XRA00	866-928 MHz	R/W, 128 Bits, 96-bit EPC code	EPC Class 1b	8-bit destruct code - 8-bit lock code.
	XRAG2	866-928 MHz	R/W, 432 Bits	EPC Gen2	Kill Command - Access Password - Lock mechanism.
Sony	RC-S919	13.56 MHz	R/W, 576 Bytes	ISO/IEC 18092	?
	RC-S962/1	13.56 MHz	R/W, 2464 Bytes	ISO/IEC 18092-FeLiCa (failed ISO14443C)	The access key is generated from the area key and service key of the area and service to be accessed. Mutual authentication is a 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 encrypted.
	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 authenticity of the card can be verified by the reader. Supports only non-encrypted commands.
	RC-S966 (Lite-S)	13.56 MHz	R/W, 432 Bytes FRAM	ISO/IEC 18092-FeLiCa Lite-S	- Mutual authentication (Internal Authentication/External Authentication) - MAC generation, addition, and verification functions - Tamper-resistance function. - Read Only Access - Read / Write Access - Read After Authentication - Write After Authentication - Write With MAC
	RC-SA00	13.56 MHz	R/W, 6K Bytes	ISO/IEC 18092	AES and DES encryption; AES-encrypted commands; DES-encrypted commands; Non-encrypted commands
	RC-SA01	13.56 MHz	R/W, 4K Bytes	ISO/IEC 18092	AES encryption; AES-encrypted commands; Non-encrypted commands
	RC-S888	13.56 MHz	R/W, 4K Bytes	ISO/IEC 18092	Embedded IC chip (RC-S962) with superior tamper resistant characteristics
	RC-S889	13.56 MHz	R/W, 9K Bytes	ISO/IEC 18092	Embedded IC chip (RC-S960) with superior tamper resistant characteristics
	RC-S860	13.56 MHz	R/W, 4K Bytes	ISO/IEC 18092	riple-DES 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.
FUJITSU	MB89R118	13.56 MHz	R/W, 2K Bytes FRAM	ISO/IEC 15693	Lock (disable to write) the requested 1 block in the user area.
	MB89R119	13.56 MHz	R/W, 256 Bytes FRAM	ISO/IEC 15693	Lock (disable to write) the requested 1 block in the user area.
Sokymat Automotive (acquired in 2003 by EM Microelectronic - sold in 2008 to SMARTRAC Technology GmbH)	UNIQUE (EM4102)	125 KHz	Read only, 64 Bits		none
	T5/Nova (JMA TP05)	130 kHz	R/W, 160 Bits (64 or 128 selectable)		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		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).
	TagCoder Lite	125 KHz	R/W, 512 Bits		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 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; 32 Bit customer key.
	TagCoder (as the previous IC but with integrated remote logic)	125 KHz	R/W, 512 Bits		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 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; 32 Bit customer key.
	TagAccess	125 KHz/Serial	R/W, 4096 Bits		TagAccess combines the functionality of a 125 kHz crypto transponder together with an SPI serial interface. This unique combination allows for the sharing of EEPROM and crypto operations between TagAccess and a microcontroller. It is possible to access the EEPROM of TagAccess via a simple serial protocol or via 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. Different types of read/write protection of the EEPROM are also implemented.
	AES-Tag	125 kHz	R/W, 10240 Bits		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 in all authentication 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-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.
???	Zodiac (EM4102) Zodiac (EM4102) [probably a Sokymat product]	134.2 KHz	Read only, 128 Bits	ISO11784	none
	RI-TRP-B*	134.2 KHz	R/W, 88 Bits		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 followed 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 EEPROM. When the challenge has been 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*	134.2 KHz	R/W, 1360 Bits		? (probably DST40). 24 Bits selective Address width.
	RI-TRP-M*	134.2 KHz	R/O, 30 Bits+R/W 208 Bits		? (probably DST40).
	RI-TRP-R*/0*	134.2 KHz	Read only, 64 Bits		none
	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	134.2 KHz	R/W, 80 Bits		80-bit key length, 4-byte or 5-byte challenge, 3-byte signature (DST80).
	RI-TH1-CB1A (based on TagIt) [obsolete]	13.56 MHz	R/W, 2 KBit	ISO15693	Each block is separately programmable by the user and can be locked to protect data from modification. Once the data has been ‘locked’ 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” Byte defined in ISO 15693-3 is used to store the Factory Lock Status of the Block. Block locking irreversibly protects the locked data from any further reprogramming.
	RI-TH1-CB2A (based on TagIt)	13.56 MHz	R/W, 2 KBit	ISO15693	
	RI-TH1-CB3A (based on TagIt)	13.56 MHz	R/W, 2 KBit	ISO15693+Magnetic Stripe	
	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 ‘locked’ 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” Byte defined in ISO 15693-3 is used to store the Factory Lock Status of the Block. Block locking irreversibly protects the locked data from any further reprogramming.
	Tag-it HF-I Pro	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 locked, it can only be changed by the password protected write command. 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” byte defined in ISO 15693-3 is used to store the Factory Lock Status of the Block. Factory Block locking irreversibly protects the locked data from any further reprogramming. User locked blocks can be reprogrammed by use of the password protected write command. Kill command available.
	Tag-it HF-I Plus	13.56 MHz	R/W, 2048 Bit	ISO15693	Each block with 32 bit is user programmable and can be locked individually to protect data from modification. Once set, the lock bit cannot be reset. The user memory is field programmable per block. 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” Byte defined in ISO 15693-3 is used to store the Factory Lock Status of the Block. Block locking irreversibly 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	?
Inside Secure	PicoPass 2KS	13.56 MHz	R/W, 2K Bit	ISO14443A/ISO14443B/ISO15693	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 personalization phase.
	PicoPass 16KS	13.56 MHz	R/W, 16K Bit	ISO14443A/ISO14443B/ISO15693	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 personalization phase.

Manufacturer	Type/Model Name	Frequency	Description	Standard/Notes	Security
	PicoPass 32KS	13.56 MHz	R/W, 32K Bit	ISO14443A/ISO14443B/ISO15693	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 personalization phase.
GOLDKEY Technology	GK4001 (same as EM4001)	125 KHz	R/W, 64 Bit		none
HID Global	Prox (1xxxxxxx)	125 KHz	Read only, 44 Bit	ISOProx has only 125KHz chip. Duo option adds a Magnetic Stripe (1336/1536). Contact chip options are available. Refer to the Logical Access HTOG.	none
	iClass (2xxxxxxxx)	13.56 MHz	R/W, 2k, 16k, 32k	ISO14443A/B and ISO15693 Has a Magnetic Stripe option (200/210/202/212/204/232/242/252/2 Contact chip options are available. Refer to the Logical Access HTOG.	The authentication for secure mode communication between reader and card is done both-ways using the 16 byte 3DES 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 Application.
	iClass SE (3xxxxxxxx)	13.56 MHz	R/W, 2k, 16k, 32k MIFARE 1k, 4k DESFire EV1 8k Seos 16k	ISO14443A/B and ISO15693 Has a Magnetic Stripe option. Contact chip options are available. Refer to the Logical Access HTOG.	iCLASS SE smart cards feature multiple securely separated application areas that are each protected by 64-bit diversified read/write 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 read/write capabilities.
	iClass dual technology cards.	125 KHz + 13.56 MHz	Combinations of the HID formats above	ISO14443A/B and ISO15693 (optional magnetic band)	Combination of the iClass SE formats above.
Fudan Microelectronics	FM11RF005M	13.56 MHz	R/W, 512 Bit	ISO14443A	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.
	FM11RF005SH	13.56 MHz	R/W, 512 Bit	ISO14443A	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 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	ISO14443A	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.
	FM11RF08SH	13.56 MHz	R/W, 1024 Bit	ISO14443A	Transfer key protection. Individual set of keys for each block. User definable access condition for each block. Encryption Algorithm compatible with Shanghai local standard.
	FM11RF32M (Mifare 4K clone)	13.56 MHz	R/W, 1024 Bit	ISO14443A	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	ISO14443A	Transfer key protection. Individual set of keys for each block. User definable access condition for each block. Encryption Algorithm compatible with Shanghai local standard.
	FM1208	13.56 MHz	R/W, 32K ROM+8K EEPROM	ISO14443A	High security level data communication (mutual three pass authentication, Access right control - auth command is [60])
	FM1208M01 (Mifare compatible command set)	13.56 MHz	R/W, 32K ROM+8K EEPROM	ISO14443A	3DES, single-DES processor; SPA/DPA resistenat controller. Memory data encryption (ROM, EEOPROM, RAM). ROM code reverse resistant. Encryption Algorithm compatible with Mifare 1K.
	FM1208SH01	13.56 MHz	R/W, 32K ROM+8K EEPROM	ISO14443A	3DES, single-DES processor; SPA/DPA resistenat controller. Memory data encryption (ROM, EEOPROM, RAM). ROM code reverse resistant. Encryption Algorithm compatible with Shanghai local standard.
	FM12AG08M01	13.56 MHz	R/W, 32K ROM+8K EEPROM	ISO14443A	3DES, SM1, compatible with Mifare 1K.
	FM1208M04	13.56 MHz	R/W, 32K ROM+8K EEPROM	ISO14443A	3DES, compatible with Mifare 4K.
Angstrom (russian company)	КБ5004ХК2	125 KHz	Read only, 64 Bits		none
	КБ5004ХК1	13.56 MHz	Read only, 64 Bits		none
	КБ5004ХК3 (Mifare 1K clone?)	13.56 MHz	R/W, 1024 Bits	ISO14443A	48 Bit cyptographic key to access each of the 16 sectors.
	К563РТ1У	2 GHz	R/W, 1563 Bits		?none?
	КИБИ-001	125 kHz	Read only, 64 Bits		none
	КИБИ-001МТ	125 kHz	Read only, 64 Bits		none
	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	13.56 MHz	Read only, 64 Bits		none
	КИБИ-D	13.56 MHz	Read only, 64 Bits		none
	Transponder G2	860 MHz	?		?
Tatwah Design	TK4100 (EM4100 clone)	125 kHz	Read only, 64 Bits		none
Quanray	QR2213 (Mifare Ultralight clone)	13.56 MHz	R/W, 64 Bytes	ISO14443A	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 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. 3DES Authentication proves that two entities have the same secret and each entity can be seen as a reliable partner for the coming communication. The applied encryption algorithm ek() is 2 key 3DES encryption.
	QR2217 (Mifare 1K clone)	13.56 MHz	R/W, 1024 Bytes	ISO14443A	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 Ciphering protects data transmission.
	QR2272	13.56 MHz	R/W, 1024 Bytes	ISO14443A	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 Ciphering protects data transmission. 128bit TEA encryption. 38bit random number generator.
Shanghai Huahong Integrated Circuit Co (SHIC)	SHC1101 (Mifare 1K clone)	13.56 MHz	R/W, 1024 Bytes	ISO14443A	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.
	SHC1102 (Mifare Ultralight clone)	13.56 MHz	R/W, 512 Bits	ISO14443A	none
	SHC1104 (Mifare 1K clone)	13.56 MHz	R/W, 1024 Bits	ISO14443A	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.
	SHC1112	13.56 MHz	?	ISO14443A	?
	SHC1124	13.56 MHz	R/W, 72K Bytes / ARM SC100 core CPU	ISO14443A	- Supports 1024bit Modular Arithmetic - Supports Modular Exponentiation and Modular Multiplication operation - Supports hardware accelerated key pair generation - Supports SPA/DPA resistant - Co-processors for public and secret key encryption to support RSA, ECC and DES/3DES. Generates true random number.
	SHC1302	13.56 MHz+contact	R/W, 48K Bytes / ARM SC100 core CPU	ISO14443-ISO/IEC7816	- Supports 2048bit Modular Arithmetic for RSA - Supports Modular Exponentiation and Modular Multiplication operation - 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 number.
Maxim Integrated	MAX66040E	13.56 MHz	R/W, 1K Bits	ISO14443B	Block Lock Feature; 512-Bit SHA-1 Engine to Compute 160-Bit MAC and to Generate Secrets.
	MAX66040K	13.56 MHz	R/W, 1K Bits	ISO14443B	Block Lock Feature; 512-Bit SHA-1 Engine to Compute 160-Bit MAC and to Generate Secrets.
	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.
Verayo	M1HW	13.56 MHz	R/W, 1K Bits	ISO14443A	PUF Circuit (unique and random silicon fabrication process variations): unclonable.
	M4H	13.56 MHz	R/W-OTP, 2K Bits	ISO14443A	PUF Circuit (unique and random silicon fabrication process variations): unclonable.
	X5122H	13.56 MHz	R/W-OTP, 512 Bits	ISO14443A	PUF Circuit (unique and random silicon fabrication process variations): unclonable.
Kovio	Kovio Tag	13.56 MHz	Read Only, 128 Bits	ISO14443A	none
	Kovio 2Kb	13.56 MHz	R/W, 2K Bits	ISO14443A	Possible blocks permalock.
OTI, ISO 14443 Type D / Cubic, ISO 14443 Type E					