MagneSafe
Encryption and Decryption

Overview

December 10, 2014

Manual Part Number: D998200029-11

REGISTERED TO ISO 9001:2008

Table 0.1 - Revisions

Rev Number	Date	Notes
11	December 10, 2014	Initial Release

Contents

Bibliography

Wikipedia. (2014). *3 DES*. Retrieved from Wikipedia: http://en.wikipedia.org/wiki/Triple_DES

Wikipedia. (2014). *DUKPT*. Retrieved from Wikipedia: http://en.wikipedia.org/wiki/Derived_unique_key_per_transaction

Wikipedia. (2014). *Hardware Security Module*. Retrieved from Wkipedia: http://en.wikipedia.org/wiki/Hardware_security_module

MagneSafe™ Security Architecture

MagneSafe Security Architecture is a foundation you can build on. The MagneSafe Security Architecture (MSA) has evolved exponentially from its inception in 2006 when MagTek delivered the industry's first Secure Card Reader Authenticators (SCRAs) for secure electronic transactions.

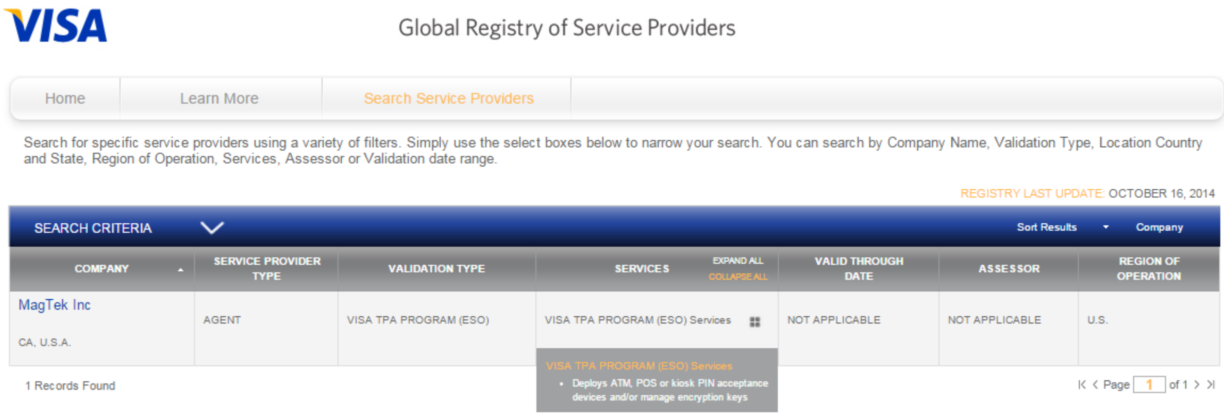
The MSA is a digital identification and authentication architecture that safeguards consumers and their personal data. Designed to exceed PCI regulations, MSA leverages strong encryption, secure tokenization, counterfeit detection, tamper recognition, data relevance and integrity, and dynamic digital transaction signatures, which together validate and protect the entire transaction and each of its components.

A key feature of the MSA is MagnePrint® card authentication, a patented, proven technology which reliably identifies counterfeit credit cards, debit cards, gift cards, ATM cards and ID cards at the point of swipe, before fraud occurs. MSA's multi-layer security provides unmatched protection and flexibility for safer online transactions.

Encryption Support Organization

MagTek is an official ESO (Encryption Support Organization). For more details on MagTek and Magensa's PCI-DSS or ESO status, visit VISA's Global Registry of Service Providers.

- Go to www.visa.com/splisting/.
- Press Begin Search.
- Type in "Magensa" under Company Name. (To confirm PCI-DSS and ESO).
- Type in "MagTek" under Company Name.   (To confirm TPA and ESO).
- Press GO.
- Magensa PCI and ESO certifications will appear.



Search for specific service providers using a variety of filters. Simply use the select boxes below to narrow your search. You can search by Company Name, Validation Type, Location Country and State, Region of Operation, Services, Assessor or Validation date range.

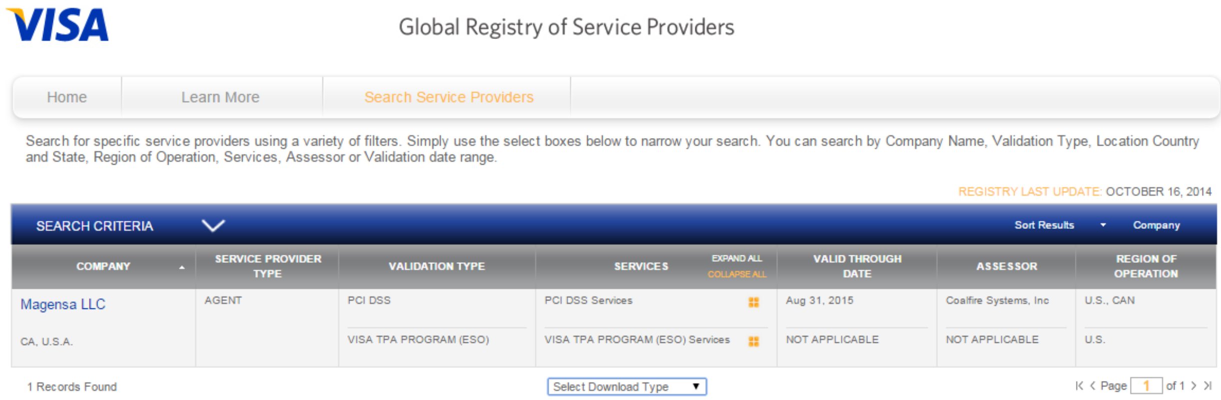
REGISTRY LAST UPDATE: OCTOBER 16, 2014

COMPANY	SERVICE PROVIDER TYPE	VALIDATION TYPE	SERVICES (EXPAND ALL / COLLAPSE ALL)	VALID THROUGH DATE	ASSESSOR	REGION OF OPERATION
MagTek Inc CA, U.S.A.	AGENT	VISA TPA PROGRAM (ESO)	VISA TPA PROGRAM (ESO) Services	NOT APPLICABLE	NOT APPLICABLE	U.S.

VISA TPA PROGRAM (ESO) Services
- Deploys ATM, POS or kiosk PIN acceptance devices and/or manage encryption keys

1 Records Found

Page 1 of 1



Search for specific service providers using a variety of filters. Simply use the select boxes below to narrow your search. You can search by Company Name, Validation Type, Location Country and State, Region of Operation, Services, Assessor or Validation date range.

REGISTRY LAST UPDATE: OCTOBER 16, 2014

COMPANY	SERVICE PROVIDER TYPE	VALIDATION TYPE	SERVICES (EXPAND ALL / COLLAPSE ALL)	VALID THROUGH DATE	ASSESSOR	REGION OF OPERATION
Magensa LLC CA, U.S.A.	AGENT	PCI DSS	PCI DSS Services	Aug 31, 2015	Coalfire Systems, Inc	U.S., CAN
		VISA TPA PROGRAM (ESO)	VISA TPA PROGRAM (ESO) Services	NOT APPLICABLE	NOT APPLICABLE	U.S.

1 Records Found

Page 1 of 1

3DES

Some of the following information was found at Wikipedia.   (Wikipedia, 3 DES, 2014)

- In cryptography, Triple DES (3DES) is the common name for the Triple Data Encryption Algorithm (TDEA or Triple DEA) symmetric-key block cipher, which applies the Data Encryption Standard (DES) cipher algorithm three times to each data block.
- The original DES cipher's key size of 56 bits was generally sufficient when that algorithm was designed, but the availability of increasing computational power made brute-force attacks feasible. Triple DES provides a relatively simple method of increasing the key size of DES to protect against such attacks, without the need to design a completely new block cipher algorithm.
- The encryption process employed by the MagneSafe Security Architecture is based on ANSI X9.24 Part 1.

Hardware Security Module

Some of the following information was found at Wikipedia. (Wikipedia, Hardware Security Module, 2014)

- A Hardware Security Module (HSM) is a physical computing device that safeguards and manages digital keys for strong authentication and provides crypto processing. These modules traditionally come in the form of a plug-in card or an external device that attaches directly to a computer or network server.

DUKPT

Some of the following information was found at Wikipedia. (Wikipedia, DUKPT, 2014)

- In cryptography, Derived Unique Key Per Transaction (DUKPT) is a key management scheme whereby every transaction uses a unique key which is derived from a fixed key. Therefore, if a derived key is compromised, future and past transaction data are still protected since the next or prior keys cannot be determined easily. DUKPT is specified in ANSI X9.24 part 1.
- DUKPT allows the processing of the encryption to be moved away from the devices that hold the shared secret (the HSMs). The encryption is done with a derived key, which is not re-used after the transaction. Within the MSA, DUKPT is used when encrypting magstripe card data. While it can be used to protect information between two companies or banks, it is typically used to encrypt PIN or other sensitive information acquired by SCRA devices.
- DUKPT is not itself an encryption standard; rather it is a key management technique. The features of the DUKPT scheme are:
    - enable both originating and receiving parties to be in agreement as to the key being used for a given transaction,
    - each transaction will have a distinct key from all other transactions, except by coincidence,
    - if a present derived key is compromised, past and future keys (and thus the transactional data encrypted under them) remain uncompromised,
    - each device generates a different key sequence,
    - originators and receivers of encrypted messages do not have to perform an interactive key-agreement protocol beforehand.

Encryption/Decryption Overview

Some of the following information was found at Wikipedia. (Wikipedia, DUKPT, 2014)

DUKPT was first invented in the late 1980s at Visa, but it didn't receive much acceptance until the 1990s. It was during this later period that the industry practices shifted towards recommending (and later requiring) that each device have a distinct encryption key. The scheme that was state-of-the-art at the time—known as "Master/Session"—would require that every PIN encrypting device be initialized with a unique master key. In consequence, processors would require a table of encryption keys as large as the number of devices deployed, when handling transactions originating from devices using Master/Session key management, given the need for unique keys per device. This table could become quite large for a major merchant acquirer. DUKPT solves this problem because—although each device is still initialized with a distinct key—this device initialization key is derived from a different key which an entire family of devices may share. Hence, the recipient of encrypted messages needs only to store one key to support a large number of devices in the field, while simultaneously meeting the unique-key-per-device requirement. It was this reason that MagTek chose to use DUKPT as a key management scheme for the MagneSafe™ Security Architecture (MSA).

This single key was called the "super-secret key" in the original description of the algorithm, but was later renamed to the more official-sounding "Base Derivation Key" (or BDK). The original name perhaps conveys better the true nature of this key, because if it is compromised then all devices and all transactions are similarly compromised. This is mitigated by the fact that there are only two parties that know the BDK: the recipient of the encrypted messages (typically a merchant acquirer), and in this case, MagTek, the party which injects the MagneSafe Secure Card Reader Authenticators (SCRAs). Further, there are pains taken to ensure that this key does not exist in plaintext outside of any tamper-resistant security module (TRSM, or HSM), and in fact is not the key that is used to initialize the encryption device that will participate in DUKPT operations. Rather, a different key is irreversibly derived from the BDK (and within a TRSM), known as the "Initial PIN Encryption Key" (IPEK). This is the key that is actually injected into the SCRAs, and a compromise of that key will not compromise the BDK (though the SCRA itself would be considered compromised, and will need to have a new key injected). Even then, the IPEK is used internally by the SCRA to create yet another set of keys irreversibly derived from it (called the “Future Keys”), and the IPEK is then immediately discarded.

On the originating (encrypting) end (the SCRA), the system works as follows:

1. A transaction is initiated with the swipe or insert of a card which involves magstripe data to be encrypted. The typical case is a customer's Bank or Gift card with a magnetic stripe.
2. A key is retrieved from the set of “Future Keys” that is used to encrypt the message, creating a cryptogram.
3. The pair of the cryptogram and an identifier known as the “Key Serial Number” (KSN) is returned from the SCRA. The KSN is formed from the SCRA’s unique identifier, and an internal transaction counter.
4. The (cryptogram, KSN) pair is forwarded on to the intended recipient, in this case, Magensa, LLC, where it is decrypted and processed further.
5. Internally, the SCRA increments the transaction counter, invalidates the key just used, and possibly generates more future keys if needed.

On the receiving (decrypting) end (Magensa, LLC), the system works as follows:

1. The (cryptogram, KSN) pair are received.
2. The appropriate BDK is located in one of Magensa’s Hardware Security Modules (HSMs).
3. The receiving system (Magensa) first regenerates the IPEK, and then goes through a process similar to that used on the originating system (MagTek) to arrive at the same encrypting key that was used (the session key). The Key Serial Number (KSN) provides the information needed to do this.
4. The cryptogram is decrypted with session key.
5. Any further processing is done. For merchant acquirers, gateways and processors, this usually means encrypting under another key to forward on to a switch (doing a “translate”), but for certain closed-loop operations may involve directly processing the data, such as verifying the PIN.

The method for arriving at session keys is somewhat different on the originating side (MagTek) as it is on the receiving side (Magensa). On the originating side, there is considerable state information retained between transactions, including a transaction counter, a serial number, and an array of up to 21 “Future Keys”. On the receiving side (Magensa) there is no state information retained; only the BDK is persistent across processing operations. This arrangement provides convenience to the receiver (Magensa) (a large number of devices may be serviced while only storing one key). It also provides some additional security with respect to the originator (MagTek) (secure magstripe readers and PIN capture devices are often deployed in security-averse environments; the security parameters in the SCRAs are ‘distant’ from the sensitive BDK, and if the SCRA is compromised, other SCRA devices are not implicitly compromised).