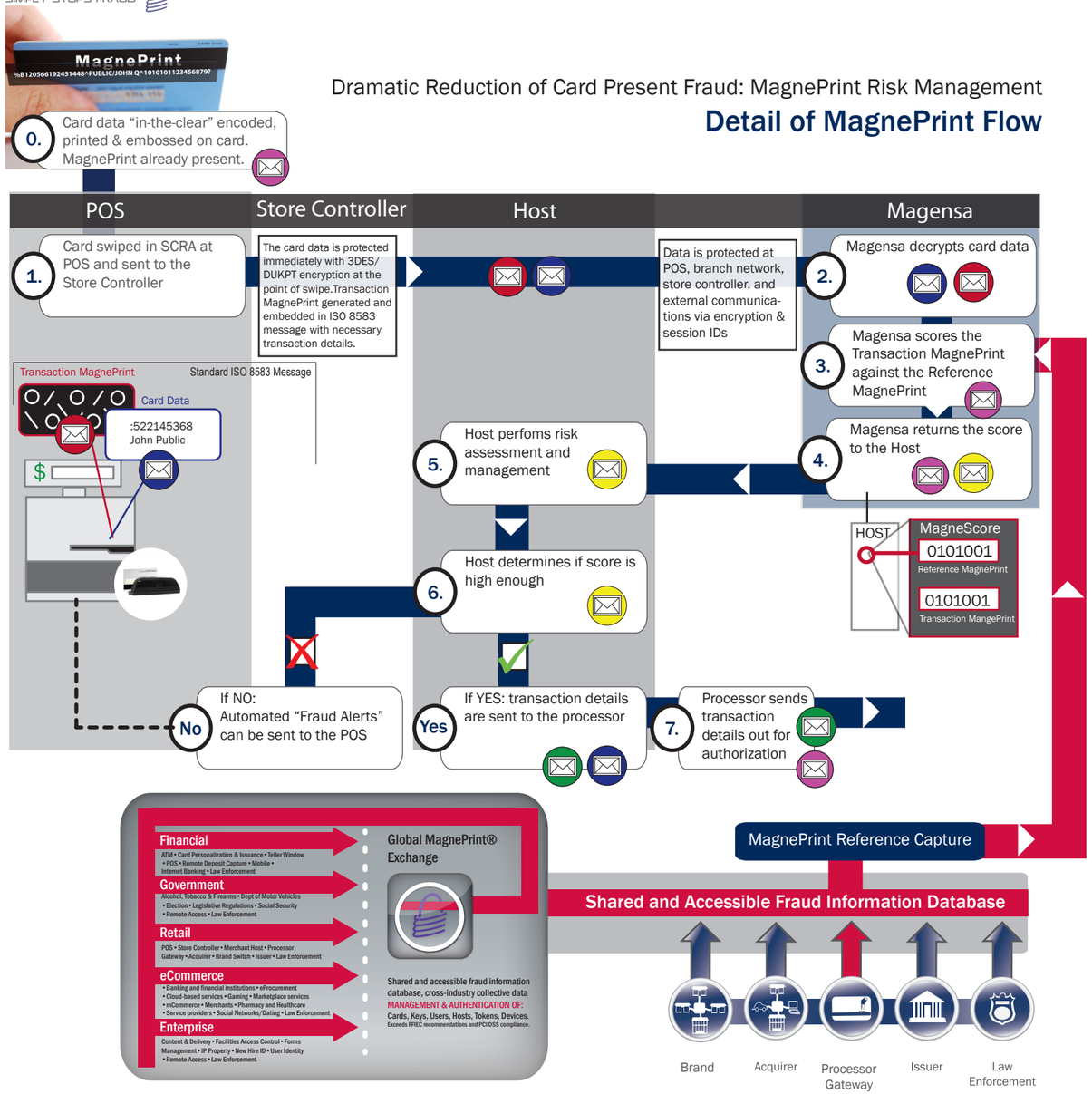
MAGENSA
SIMPLY STOPS FRAUD

Dramatic Reduction of Card Present Fraud: MagnePrint Risk Management

Detail of MagnePrint Flow



Topology Key

- Clear text card data (unencrypted)
- Transactional MagnePrint
- 3DES/DUKPT Encrypted Card Data
- MagnePrint Score

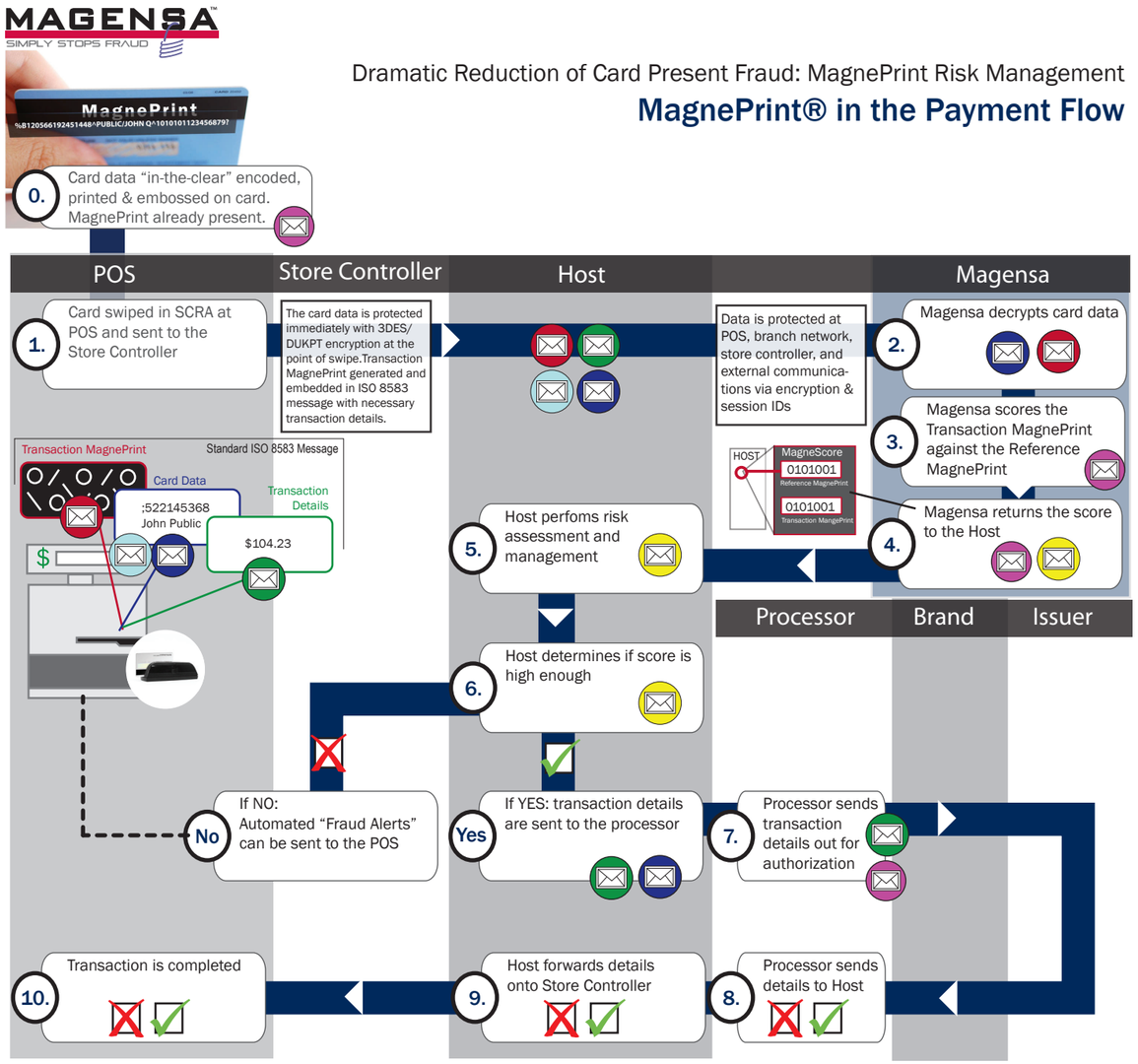
When strong encryption and secure tokenization are used in conjunction with dynamic card authentication, it provides a solution that can protect cardholder data while at rest or in transit and exceeds PCI DSS requirements. It further secures payment systems with real-time information to prevent, detect and alert to the presence of fraudulent transactions and rogue devices.

(SCRA) Secure Card Reader Authenticator reads ISO/AAMVA encoded surface layer data, reads the magnetic particulate layer below, encrypts the data within the tamper resistant authentication sensor and transmits the encrypted cardholder data along with the stripe's dynamic digital identifiers (DI) for card and cardholder data authentication during the transaction authorization process. ONLY MagneSafe secured devices fit this description.

MAGENSA
SIMPLY STOPS FRAUD

Dramatic Reduction of Card Present Fraud: MagnePrint Risk Management

MagnePrint® in the Payment Flow



Topology Key

- Clear text card data (unencrypted)
- Transactional MagnePrint
- Tokenized and/or Masked Data
- 3DES/DUKPT Encrypted Card Data
- Transaction details
- MagnePrint Score

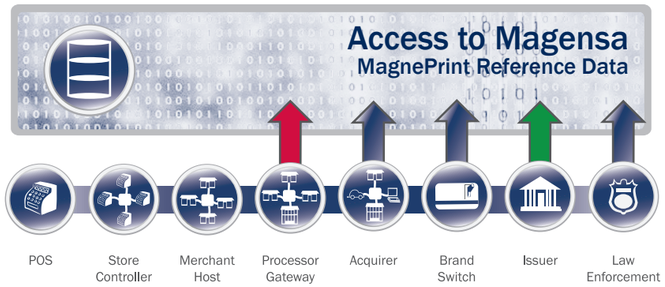
When strong encryption and secure tokenization are used in conjunction with dynamic card authentication, it provides a solution that can protect cardholder data while at rest or in transit and exceeds PCI DSS requirements. It further secures payment systems with real-time information to prevent, detect and alert to the presence of fraudulent transactions and rogue devices.

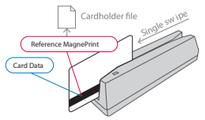
(SCRA) Secure Card Reader Authenticator reads ISO/AAMVA encoded surface layer data, reads the magnetic particulate layer below, encrypts the data within the tamper resistant authentication sensor and transmits the encrypted cardholder data along with the stripe's dynamic digital identifiers (DI) for card and cardholder data authentication during the transaction authorization process. ONLY MagneSafe secured devices fit this description.

Dramatic Reduction of Card Present Fraud
MagnePrint Risk Management

How Do Magensa and MagnePrint Work?

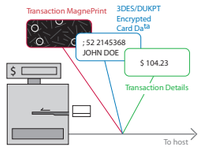
When a card-present transaction is submitted, the MagnePrint of the card read at the transaction point is transmitted along with the encrypted card data. At Magensa, the MagnePrint risk management tool compares the 'transaction MagnePrint value' to a 'reference MagnePrint value' already present in the authorization database. These reference values are currently submitted by Processors, but ideally they will also come from Issuers or any other party above that has access to Magensa.





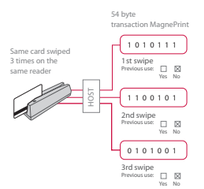
Capture the Reference MagnePrint

MagTek makes readers that recover the encoded track data and the MagnePrint simultaneously. The MagnePrint is converted to a 54 byte digital string. When the card is first issued or first used, the Processor or Card Issuer stores the digitized original MagnePrint at Magensa. This is information is designated as the Reference MagnePrint.



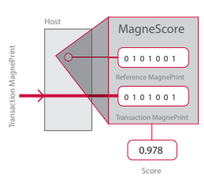
Encrypt the Card Data and Capture the Transaction MagnePrint

MagTek makes a variety of readers suitable for use in ATMs, gas pumps, PDAs, kiosks, PCs, vending machines, MACs, cell phones, ECRs and POS terminals. When a card is read, the encoded card data, the MagnePrint and the usual transaction details are 3DES/DUKPT encrypted and sent to the Card Issuer for verification. The MagnePrint obtained at this time is designated the Transaction MagnePrint.



Verify the Transaction MagnePrint

Transaction MagnePrints have a remarkable and valuable feature. They change stochastically – that is they change dynamically, but in ways that can't be predicted with any certainty. The change is a matter of probability, built in by the imperfection of nature. The odds of obtaining two identical 54 byte Transaction MagnePrints from a single card are about 1 in 100 million. A Transaction MagnePrint identical to one previously used will be rejected. This inherent variability of Transaction MagnePrints provides an algorithmically verifiable, unique transaction number for every card swipe.



Score the Transaction MagnePrint against the Reference MagnePrint

Magensa receives a Transaction MagnePrint, compares it to the Reference MagnePrint and calculates a score based on the correlation between the two. A high score indicates a legitimate card. A low score points to a counterfeit card. The Card Issuer sets the minimum passing score and uses the MagnePrint Score as part of the transaction accept/decline criteria. MagnePrint scoring is a fast "real-time" process. Typical scoring times are 10 milliseconds or less.

Dramatic Reduction of Card Present Fraud
MagnePrint® Risk Management

Magensa™ is a fraud prevention, detection and advisory service. It maintains a globally accessible registry of authentication information so that consumers, financial institutions, retailers, businesses and governments can assess the validity and trustworthiness of the credentials and products they rely upon in the course of online identification, payment, and other important transactions.

Additionally, Magensa provides token management and cryptographic services, vital to the protection of cardholder data, the payment system, and personal or sensitive information. Magensa is a subsidiary of MagTek, Inc.

Magensa I 1710 Apollo Court, Seal Beach, CA 90740 I 562-546-6500 I info@magensa.net