MAGTEK®
SECURITY FROM THE INSIDE

MagnePrint:
A Real Time Risk Management Tool

By Kiran Gandhi
Vice President, MagTek, Inc.
09/09

Overview

MagneSafe™ is a digital identification and authentication architecture that safeguards consumers and their personal data. Designed to exceed PCI regulations, MagneSafe 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 MagneSafe 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. MagneSafe's multi-layer security provides unmatched protection and flexibility for safer online transactions.

Introduction

The MagnePrint risk management tool provides issuers, brands, technology vendors, processors, acquirers, and merchants with an additional layer of protection against fraud, in card-present credit and debit card transactions. The necessary technology to implement this tool is now available, tested, and ready for use. The purpose of this paper is to explain to a technically informed audience the tool, the technology and processes behind it, and the benefits that will accrue from it to card issuers, acquirers, and merchants.

MagnePrint is a card security technology that will, when properly implemented, detect skimmed or magnetically altered counterfeit cards. The MagnePrint risk management tool, developed by MagTek, Inc., imposes no significant time cost and only a minimal dollar cost on the merchant at the point of transaction, and the necessary infrastructure investment is negligible in the context of the ongoing costs of fraud to issuers and acquirers. Additionally, its success does not depend on the mass re-issuance of cards or the deployment of updated card accepting terminals. Since the cards currently in circulation can be brought into participation automatically over time during the course of their normal use, MagnePrint users can be tactical in their approach to fighting fraud. Starting with high fraud locations,

users can update the terminal base and register cards. As the fraud migrates, more terminals can be deployed to better manage the overall risk.

MagnePrint technology is complementary to chip technology. For the foreseeable future the magnetic stripe will remain as either the primary or fallback (if and when chip fails) machine-readable technology on financial transaction cards. The chip will protect the chip and will not protect the magnetic stripe. However, MagnePrint will protect the magnetic stripe.

Worldwide, reported credit card skimming fraud is a US$4.7 billion dollar problem, with an unknown but likely significant additional fraud cost related to debit cards that go unreported. Credit and debit card fraud is everyone's problem. The costs of fraud are carried initially by issuers and acquirers, who pass them on to merchants in the form of authorization fees and discounts, who pass them on to consumers in the form of higher prices for goods and services.

Over time, the adoption of MagnePrint technology is expected to lead directly to an annual savings in the range of US$1 billion dollars of card-present credit card fraud that is currently borne by card issuers. In addition, there will be annual savings directly related to the elimination of currently unreported debit card fraud.

More Data Yields Better Decisions

It's empirically clear that the current authorization system is generally successful in keeping credit card fraud within a predictable, actuarially useful range. But the system is not perfect. As we noted above, in the range of US$4 billion dollars worth of fraudulent transactions are cleared per year, the vast majority of which presumably represent "false positives" that were erroneously passed through by the authorization system.

No matter how much information is available, the decision to authorize a given transaction (to indemnify the merchant for that transaction, provided that certain conditions are met) is always a statistical judgment call – a risk-management decision. The issuer adjusts his authorization algorithm to take into account all available information that is relevant and the algorithm produces an authorization decision.

The accuracy of that decision, and its effectiveness in filtering out fraud, is directly related to the amount of information available to the algorithm. More data yields better decisions. For example, if the payer's identity and the card he presents were authenticated at the time of transaction, it would without question reduce the incidence of fraud. It is in the spirit of "more data yields better decisions" that MagTek developed the MagnePrint risk management tool. MagnePrint is a way of providing another useful, reliable piece of data about the likely authenticity of a given credit or debit card. This data point can be used as an input to the card authorization process.

The Genius of MagnePrint

MagnePrint uses the inherent properties of magnetic materials to provide the authorization algorithm with a reliable measure of how likely it is that the card presented is the original card issued by the issuer – not a clone, not a copy, or not one that has altered data on the magnetic stripe, but the unique original. There currently exists no other cost effective technology capable of providing such statistically reliable, real time authentication of the payment instrument in a credit or debit card transaction. As a result, issuers that take MagnePrint into account in their authorization process should see an immediate and material decline in their fraud losses resulting from skimming.

MagnePrint Fundamentals

What is MagnePrint

MagnePrint is a dynamic card authentication technology based on the unique physical properties of the magnetic stripe, also referred to as the stripe's digital identifier or (DI). It provides validation that the card itself is genuine and that its encoded data has not been altered.

How the MagnePrint value is determined

MagnePrint technology, based on research conducted by Washington University's Department of Security Technologies, measures the background magnetic particulate distribution on a standard magnetic-stripe card, and converts that distribution into a 54-byte value that is a simplified representation of that particulate distribution.

What needs to change on the current magnetic stripe card

There are no changes required to the manufacturing process of the magnetic stripe, the plastic card manufacturing process, or the data encoded on the magnetic stripe. Also, there is no need to re-issue cards.

Why MagnePrint is useful

Because the particulate distribution is persistent over the useful life of the card, multiple MagnePrint values read at different times from the same physical card (assuming the encoded card data has not been changed) will always be equivalent within statistical limits. In contrast, the MagnePrint values read from different physical cards, even if encoded with identical card data, will always be different. This means that the MagnePrint serves as a reliable indicator of the identity of a physical card, and can be used to prevent the authorization of fraudulent card-present transactions initiated from "cloned", "skimmed", or "altered" cards.

How the MagnePrint is used to screen for fraudulent transactions

When a card-present transaction is submitted from a MagnePrint-enabled reader for authorization to a MagnePrint-enabled host system of an issuer, the MagnePrint of the card read at the transaction point is transmitted along with the card data and other data. MagTek's MagnePrint risk management tool compares the transaction MagnePrint

value to a reference MagnePrint value already present in the authorization database, calculates the degree of correspondence (the match value) between the two MagnePrint values, and makes a judgment about the authenticity of the card based on all available transaction information, including the match value.

What technology is required

MagTek's MagnePrint risk management tool requires a MagnePrint-enabled card reader at the point of transaction, an acquirer host that is enabled to transport the MagnePrint value to the issuer, as well as a MagnePrint-enabled system at the issuer's host site. The MagnePrint-enabled components, which can be retrofitted into most existing card authorization systems at a nominal cost, will be available from MagTek and its partners.

Four Layers of Security

MagnePrint technology offers four layers of security. These are increasingly impregnable layers that act as barriers to prevent the compromise of MagnePrint technology.

The first layer of security is inherent in the complexity of the particulate distribution on a standard magnetic stripe. The MagnePrint algorithm leverages the fact that the 3.375 inches of stripe space along each card's encoding area is populated by a persistent random distribution of particles that are permanently fixed. (The changes in the magnetic stripe's physical structure that occur during the lifetime of the card, e.g., by abrasion during normal use, are statistically insignificant.) Furthermore, the likelihood that two different cards will yield identical particle distributions, given the randomness inherent in the process by which magnetic stripes are manufactured, is in the range of one in 900 million. And the hundreds of millions of particles make it statistically and practically impossible for an existing magnetic stripe to be cloned (from the perspective of particle distribution) in a way that yields an equivalent MagnePrint value.

As a second layer of security, MagnePrint technology determines the 54-byte MagnePrint value in reference to the positions of the flux reversals of the encoded card data. The data pattern is larger (by order of magnitude) than the particle pattern. Therefore, if a valid card with a known particle pattern were to be re-encoded with identical data, it would show non-trivial variances in the way the written data pattern microscopically aligns with the physically permanent particle structures of the magnetic stripe on the card. As a result, cards with "altered data" can be detected MagnePrint technology.

The third layer of security is the random variations inherent in each incidence of reading a card. Each read of a card (whether the card is swiped by hand, inserted into a reader, or read by some other method) is a microscopically different experience, due to the impossibility of precisely duplicating the reading process, variations in the read head among card readers, and so forth. Paradoxically, this means that a transaction MagnePrint value that is identical to a previous MagnePrint value on file is almost certainly fraudulent. Multiple MagnePrint values taken from the same card on

successive reads are expected to vary, within a statistical range. The probability of an exact match on all 54 bytes in separate card reads is in the range of one in 100 million. This inherent variability provides a statistically probable, unique transaction number for every card read, assuring that MagnePrint is very difficult to compromise.

Finally, as a fourth and ultimately impregnable security level, the MagnePrint authorization process is protected against fraud by the simple fact that it depends on information that is in plain view. There is nothing hidden about the particulate structure of the card, or the encoded alphanumeric data. This means that there is no "secret" to the fundamental MagnePrint technology that, if cracked, would compromise the system.

Determining Acceptance Criteria

It is important to understand that MagnePrint does not guarantee the authenticity of the transaction. It provides the card issuer a data point representing the probability that a given card used for a transaction is authentic. By using this data point, card issuer can establish their acceptance criteria for a level of risk that is financially acceptable. During the Beta Test in 2002, a run of a million transactions with an acceptance threshold set at 0.5 resulted in a "false accept" rate of zero (that is, all attempts to process fraudulent cards were thwarted) and the resulting "false reject" rate was only 0.027 percent.
In comparing a given transaction MagnePrint to its reference MagnePrint, MagTek's algorithm assigns a match value between zero (no match) and one (perfect match). MagTek has found in practice, as expected in theory that match values tend to follow a normal (Gaussian) distribution, with two bell curves anchored near opposite ends of the value scale. The MagnePrint authorization methodology allows each financial institution to select an acceptance threshold between zero and one for its transactions; or even to specify a threshold that varies according to the characteristics of the transaction (e.g., be more stringent for higher-dollar transactions originating from a fraud prone merchant).

As important as it is to reject fraudulent transactions, for many merchants it is just as important not to reject legitimate transactions (i.e., not to generate "false rejects"). In order to preserve customer goodwill, some issuers might wish to be more forgiving, e.g., set the acceptance threshold at 0.35, which would result in authorizing a very small number of fraudulent transactions, while statistically eliminating the incidence of "false rejects" while still maintaining the robustness of MagnePrint as a risk management tool. These risk management decisions have been deliberately left in the hands of the issuer, so that each can establish acceptance thresholds that are prudent in the context of its own business and its own customers.

Growing the MagnePrint-Enabled Card Base

The MagnePrint risk management tool depends upon the presence of reference MagnePrint data in the authorization database. This allows comparison of transaction MagnePrint data and reference MagnePrint data to authenticate the card.

Reference MagnePrint data should of course be collected as a matter of course whenever a card's identity is known with certainty, e.g., at the time of issuance. To avoid re-issuance costs, how can reference MagnePrint data be gathered reliably on cards already in circulation, without imposing an unacceptable convenience on cardholders?

Fortunately, MagTek's MagnePrint authorization tool provides a built-in channel for collecting reference MagnePrint data "on the fly" during the course of normal card use. When a transaction MagnePrint is submitted as part of the authorization data set, and if no reference MagnePrint exists for that card, this first transaction MagnePrint is presumed to be legitimate and recorded in the authorization database with "provisional" status. Henceforth, the provisional MagnePrint collected at the time of this earlier transaction will be available for use as the reference MagnePrint in authorizing future transactions. The authenticity of this provisional MagnePrint is not guaranteed, because it was collected in circumstances in which the authenticity of the card from which it was provided was not known with 100% certainty. However, there is a strong statistical probability (inherent in the overwhelming margin by which legitimate transactions outnumber fraud attempts in the transaction pool as a whole) that any such "provisional" MagnePrint will in fact be legitimate, so treating all such provisional MagnePrints as authoritative, in the absence of evidence to the contrary, is a statistically rational business decision. Furthermore, if there are no disputes from the cardholder regarding the transaction that was used to collect the "provisional" reference then the "provisional" status can be changed to permanent status. The MagnePrint risk management tool requires the adoption of both new technology and minor process changes in order to operate successfully. The changes should be adopted as widely as possible in order for the tool to have maximum value to its users. Fortunately neither the technology changes nor the process changes are particularly onerous.

Technology, Process, and Motivation

The successful spread of MagnePrint risk management requires simultaneous changes by issuers, acquirers, and merchants. It is in the interest of all these constituencies that the necessary changes take hold as broadly and as quickly as possible, because the benefits of MagnePrint risk management to all these constituencies will increase geometrically as MagnePrint is adopted more and more widely.

For the merchant: MagnePrint-enabled equipment

At the "front end" of the transaction process, merchants are a propelling force in ensuring that the MagnePrint risk management tool is adopted. They have a motivation to reduce their "charge back" costs. This is an important leverage merchants have over acquirers in encouraging them to retrofit their authorization systems, to accommodate the transmission of MagnePrint data, and over equipment manufacturers in ensuring that MagnePrint-enabled point-of-sale equipment becomes the standard. At the transaction point, the card must be read in a MagnePrint-enabled card reader attached to a MagnePrint-enabled terminal or MagnePrint-enabled Electronic Cash Register

(ECR). The reader will capture a transaction MagnePrint from the card's magnetic stripe (along with the alphanumeric data normally captured) and transfer it to the terminal, which will upload the transaction MagnePrint along with the typical data to the host for authorization.

For the acquirer: MagnePrint-enabled infrastructure
Active participation of acquirers in the MagnePrint program is also crucial, because acquirers typically have leverage over authorization procedures that are followed by merchants at the point of transaction. Their motivation is to reduce "charge back" processing costs. Acquirer participation will ensure that equipment manufacturers universally MagnePrint-enable their card readers and terminals. It will also ensure that the infrastructure message flow will support the transmission of a MagnePrint value from the point of transaction to the issuer's host.

For the issuer: MagnePrint-enabled host
They have the strongest business case to adopt MagnePrint technology. Fundamentally, the MagnePrint risk management tool reduces fraud loss suffered by the issuer. Their authorization host must be MagnePrint-enabled. It must be capable of accepting transaction MagnePrint values (from those transactions submitted for authorization that include them), of retrieving reference MagnePrint values (for those cards for which they are already on file), of passing the MagnePrint pair through MagTek's comparison algorithm to generate a match value, and of accepting or rejecting the transaction according to the issuer's threshold value and other acceptance criteria. Ideally, the issuer will also be equipped to record the transaction MagnePrint as a "provisional" reference MagnePrint for card accounts that do not already have a reference MagnePrint on file.

Risk Management Benefits from MagnePrint

The MagnePrint system as a whole has been exposed to rigorous beta test environments of statistically significant size, with quantifiable positive results. Following are some of the most prominent benefits associated with the adoption of the MagnePrint risk management tool.

Decline in Direct Skimming
As it begins to be adopted, MagnePrint will immediately begin to impact the success of skimming – a method for creating counterfeit cards in which a legitimate string of card data bytes is captured and copied to create another card. Counterfeit cards created by skimming are easily detected by MagnePrint technology. The decline in skimming will lead to a decline in credit and debit card fraud losses.

Other benefits will include MagnePrint technology increasing the confidence and goodwill among both cardholders and merchants. Although difficult to quantify, this benefit is significant. With the increased awareness in identity fraud, consumers are becoming

concerned with fraudulent uses of their credit and debit cards. Furthermore, both issuers and acquirers will benefit over time in the form of lower acquisition costs, lower churn levels, and increased card activity.

Conclusion

The MagnePrint risk management tool was developed as a result of thoughtful deliberation among MagTek's scientists and engineers, informed by the most current understanding of the intricate properties of magnetic materials, of the relevant ANSI standards, and of the inner workings of card reading and encoding devices.

All the necessary components of the system (including MagnePrint-enabled card readers, encoders, and authorization system components) are available from MagTek and its partners.

To learn more about MagnePrint visit
www.magneprint.com or
contact MagTek at 562-546-6400