White Paper

How Wincor Nixdorf Helps Customers Prepare for the Transition to EMV

WINCOR NIXDORF

EXPERIENCE MEETS VISION.

What is EMV and Why is it Important?

Introduced in 1994, EMV or Europay MasterCard Visa is a technical specification that facilitates interoperability between chip-based credit/debit cards and point-of-sale devices or ATMs. The EMV specification ensures that all EMV branded cards operate with all certified chip-reading devices, regardless of vendor, financial institution or place where the card is used. Today, more than 1.6 billion EMV cards are currently distributed around the globe by issuers such as American Express, MasterCard, Visa and others.

Credit and debit cards in the United States still store data in a static fashion, via mag-stripe technology which dates back to 1960. But the chip on the front of an EMV card stores data in a dynamically encrypted fashion that protects against unauthorized modification and fraudulent transactions. EMV cards support a wider array of cardholder verification methods. They support contactless “tap-and-go” purchases, and they provide issuers with more options for loyalty programs.

The key objectives of EMV are to reduce counterfeiting and fraudulent transactions and to standardize all payment solutions on a singular specification recognized around the globe.

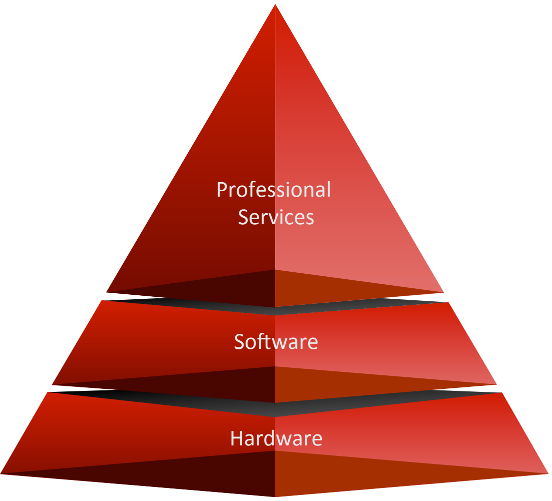
According to the Aite Group, an estimated $8.6 billion is lost to card fraud in the United States each year. The U.S. Secret Service estimates that more than $1 billion of this amount is lost directly at ATMs.

In each region where EMV has been adopted, ATM fraud has dropped dramatically — in some cases as much as 80 percent. The data is indisputable: EMV is more secure than mag stripe. As countries continue to migrate to EMV, fraud and counterfeiting activities shift to less secure places, such as the United States.

So why then does the United States remain the last non-EMV market: the final safe haven for stolen or counterfeited cards?

As we ponder this question, consider the most recent ATM theft in which organized thieves drained more than $45 million dollars from ATMs worldwide in mere hours. By accessing bank databases, cyber-thieves were able to eliminate limits on individual accounts, load customer data onto any plastic card with a mag stripe (even an old hotel room key would suffice) and use makeshift cards to withdraw millions of dollars in cities around the world. Such a scheme isn’t that difficult to accomplish with mag stripe technology.

The good news is that EMV is coming soon to an ATM near you. But “soon” is a subjective term. Most industry experts agree the primary driver for EMV migration in the U.S. will come from issuers, as they’re the ones tasked with replacing more than a billion mag-stripe credit and debit cards. This won’t be a singular event – but rather an ongoing process, where expired cards will be gradually replaced with EMV cards. The shift will be subtle, and the card holder may not even be aware of the change.



Before issuers can start providing customers with EMV cards, they need a plan for accepting them at the ATM. The first step towards accepting EMV cards at the ATM is typically an assignment of liability:

- MasterCard is the first in the U.S. to publicly declare that if fraud occurs on a transaction initiated through an EMV card on a MasterCard, Cirrus or Maestro network, then **the ATM owner will be liable for that fraud** if the ATM was not properly equipped to support EMV technology. Visa has also announced dates for liability shifts, and other issuers in the U.S. will soon follow suit.
- In Canada, Visa was first to shift the liability to ATM owners (in October of 2010). Within two years, all cards from Interac members (Royal Bank of Canada, CIBC, Scotiabank, Toronto-Dominion Bank, and the Desjardins Group of Credit Unions) featured EMV chips.

While the deadlines for compliance in the U.S. continue to shift, the message is clear: It's time to get ready for EMV at the ATM. This shift, which can take up to a year to complete, involves **hardware**, **software** and **professional services** to ensure compatibility on the back end. Wincor Nixdorf provides leading solutions for all three layers.

EMV Level 1 – Hardware: Wincor's EMV-compliant Card Reader

All Wincor Nixdorf ATM card readers are EMV Level 1 certified and have been for several years. Customers deploying Wincor hardware today already have the capability to accept EMV-based cards. As MasterCard and other issuers implement policies to shift fraud liability to ATM operators, customers can rest assured that Wincor hardware will protect them from liability shifts.

Wincor card readers are available in both motorized and hybrid-dip variations. When deployed in conjunction with Wincor's Anti-Skimming Module and the Optical Security Guard, they deliver the highest level of security currently available within the industry. Wincor's contactless card reader also delivers full EMV compliance and provides the means by which contactless and mobile phone-based payments can be performed.

The shelf life of a Wincor card reader typically exceeds that of the ATM, so customers deploying Wincor card readers today will not have to upgrade their hardware in the years ahead as the full migration to EMV runs its course.

EMV Level 2 – Software:

All of the activities at an ATM are driven by software. Wincor's EMV Level 2 Kernel interacts with compliant card readers from all major manufacturers to perform a number of tasks at the ATM, such as authorizing the user; determining what type of transaction they want (withdrawal, deposit, etc.); communicating the request to the issuing bank; confirming the request; and completing the transaction. In addition to customer-specific functions, Wincor's software also plays a role in monitoring a number of bank-specific items, such as:

- Terminal availability and connectivity to the network;
- Cash inventories;
- And a set of accounting features tracking the number of transactions and the different types of transactions at each ATM.

Wincor's certified EMV Level 2 Kernel is the world's most widely-deployed multi-vendor EMV Kernel. Each of Wincor's EMV Kernels (for Java, Java Enterprise Edition, C++, or traditional fat clients) ensures 100-percent multi-vendor compliance and can be deployed in any ATM.

Through downloadable upgrades, Wincor's software is easy to maintain, extending the life of a self-service terminal fleet while also helping to lessen the impact and costs of EMV implementation. It plays a key role in reducing terminal downtime while adding a security layer to prevent unauthorized use.

Bolstering Security at the ATM:

Malware attacks and anti-skimming jammers via direct USB connections at ATMs are on the rise. But a variety of terminal security solutions, including anti-skimming modules and optical security guards can protect against malware threats such as viruses, Trojans, spyware and denial of service attacks. These solutions prohibit the use of unauthorized USB sticks, hard-disks or memory cards, and they also encrypt the hard disc of the ATM to prevent unauthorized access and misuse.

Wincor's software-based security solutions are specifically built for the ATM and not the desktop/PC environment. They can be added in a standalone fashion for a single ATM or remotely deployed as a network-based solution for an entire fleet.

EMV Level 3 – Back End Integration:

Wincor's EMV hardware is standardized. Its EMV software Kernel is easy to certify and implement in a multi-vendor environment. But it is the professional services organization that differentiates Wincor when it comes to helping banks and ATM fleet owners manage the transition to EMV.

To become EMV-certified, a variety of tests and type approvals must be passed, and an EMVCo letter of certification must be obtained. All hardware, software and back-end connections between the acquirer and the issuer must be certified through rigorous testing.

- Level 1 type approvals certify electromechanical characteristics, the logical interface of the hardware, and transmission protocols;
- Level-2 type approvals test a variety of debit/credit application requirements that are defined in the EMV specification;
- And Level 3 approvals require the entire ATM network and switch environment to be certified for each card type that the ATM operator wants to authorize. Bank-A may issue Visa cards: Bank-B may provide MasterCards; and Bank-C may issue both. Each issuer has their own card scheme and their own tests that need to be passed, and validated by third-party auditors.

Changes made to the hardware or software at an ATM produce ripple effects that need to be certified by switch providers (FIS®, Vantiv®, VISA®, FDR®, etc.) to ensure that the back-end compatibility to the financial network has not been compromised.

Depending on the age of the ATM, the processor and the memory in the ATM's PC may need to be upgraded in order to run an EMV software Kernel. The operating system at each ATM is another concern: Microsoft recently announced that it will no longer support Windows XP, prompting ATM fleet owners to upgrade to Windows 7, which features different BIOS and security features. Changes made to the ATM's PC – no matter how big or small – need to be re-certified by the switch provider.

In order to minimize the ripple effects that all of these upgrades produce, Wincor's professional services organization has developed **a proven set of best practices** that helps banks and ATM fleet owners obtain certification at all three levels. Since 2006, Wincor has continuously refined its best practices by helping the biggest banks in Europe, Canada and in the Asia-Pacific region migrate their ATMs to EMV. Wincor's Best Practices include:

- **Strategy:** Experience gained from large-scale migrations helps new clients understand holistically what, why and when things need to get done. Identifying the pitfalls early in the process, and understanding how to avoid them can dramatically speed up the certification process.
- **Requirements:** Whether the EMV migration involves hundreds, or thousands of ATMs, a full inventory assessment should be carried out. Identifying how many different card readers are in place; listing which PCs need processor, memory or operating system upgrades; and also identifying which ATMs should not be upgraded – but replaced - streamlines the testing and certification process. Wincor goes beyond just basic hardware and software requirements. Our experienced consultants will look at the entire process flow and identify other areas in need of change, e.g. host based requirements including implementation support.
- **Testing:** Compatibility testing involves a number of parties, as each bank has its own test suites that must be carried out for each type of card it offers. Independent, third-party auditors must also be involved before an EMVCo letter of certification can be obtained. Coordination amongst these parties is a must, and Wincor has a dedicated consulting team that is familiar with the testing requirements.
- **Card Management:** With EMV, customer information (such as daily limits, PIN retries, etc.) is stored on the card's EMV chip. If a customer seeks to change their PIN or daily limit, those changes need to be communicated to the chip while the card is clamped into the ATM. Wincor's expertise with EMV Scripting helps banks address a wide variety of card management issues.
- **Maintaining EMV Status** is not a one-time event, but rather an ongoing process that must be validated when significant hardware or software changes are made. Wincor's Kernel can be updated remotely from a central point, which helps to ensure that a bank is always running a version of Wincor software that is compatible with whatever hardware or Operating System upgrades they make in their ATMs.
- **Deploying new functionality:** Beyond supporting conventional transactions, Wincor's consultants help clients leverage EMV to deliver new value-added services, such as stamps, tickets and mobile phone top-ups. Once the EMV software is installed, it opens up a variety of new business possibilities – which are sure to expand as mobile banking technologies continue to evolve.

Since 2006, Wincor has worked extensively with global payment brands, financial institutions, merchants, processors, acquirers, regional debit networks and industry suppliers to help them transition to EMV. Numerous customer engagements with banks in Europe, Canada and in the Asia-Pacific region have provided the expertise needed to swiftly manage an EMV migration.

When it comes to managing the transition to EMV, speed and efficiency are important factors. And the combination of a complete portfolio and a world-class professional services organization sets Wincor Nixdorf apart.

To learn more about how Wincor Nixdorf helps ease the transition to EMV, please contact your sales representative or Anissa Vaast at anissa.vaast@wincor-nixdorf.com.

Published by
Wincor Nixdorf International GmbH Banking Division
Corporate Headquarters:
Heinz-Nixdorf-Ring 1, D-33106 Paderborn, Germany
U.S. Headquarters:
8505 Cross Park Drive, Suite 300, Austin, Texas 78754
Phone: (512) 252 5622
Fax: (512) 252 5699
info.banking@wincor-nixdorf.com
www.wincor-nixdorf.com

Printed in Germany, July 2013

WINCOR NIXDORF

EXPERIENCE MEETS VISION.