Secure Payments Framework Workgroup

EMV for the US Hospitality Industry

Version 1.0

About HTNG

Hotel Technology Next Generation (HTNG) is a non-profit association with a mission to foster, through collaboration and partnership, the development of next-generation systems and solutions that will enable hoteliers and their technology vendors to do business globally in the 21st century. HTNG is recognized as the leading voice of the global hotel community, articulating the technology requirements of hotel companies of all sizes to the vendor community. HTNG facilitate the development of technology models for hospitality that will foster innovation, improve the guest experience, increase the effectiveness and efficiency of hotels, and create a healthy ecosystem of technology suppliers.

THE INFORMATION IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES, OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF, OR IN CONNECTION WITH THE INFORMATION HEREIN.

Permission is granted for readers to use the names, labels, etc. contained within the document. The intent of publication of the document is to add clarity around a subject and to provide hoteliers with the information needed to make appropriate decisions for their needs.

This document has not been verified for avoidance of possible third-party proprietary rights. In implementing this specification, usual procedures to ensure the respect of possible third-party intellectual property rights should be followed. Visit http://htng.org/ip-claims to view third-party claims that have been disclosed to HTNG. HTNG offers no opinion as to whether claims listed on this site may apply to portions of this specification.

The names Hotel Technology Next Generation and HTNG, and logos depicting these names, are trademarks of Hotel Technology Next Generation. Permission is granted for implementers to use the aforementioned names in technical documentation for the purpose of acknowledging the copyright and including the notice required above. All other use of the aforementioned names and logos requires the permission of Hotel Technology Next Generation, either in written form or as explicitly permitted for the organization’s members through the current terms and conditions of membership.

Introduction

New rules issued by the major card brands in the United States related to EMV technology go into effect on October 1, 2015, which has generated a lot of questions from hoteliers looking to understand what EMV is, what they need to do to support it and what happens if they aren't ready by October. There has been a lot of hype in the news media about EMV, with varying levels of accuracy, unfortunately making it difficult to separate fact from fiction. This paper is intended to clarify the subject of EMV and to equip hoteliers with the information needed to make the right decisions for their business.

EMV Overview

The name EMV stands for Europay, MasterCard and Visa – the card associations who partnered together to publish the first specifications. The partnership currently consists of six card associations: Visa, MasterCard, Discover, American Express, JCB and UnionPay.

EMV refers to a set of technical specifications for processing payment transactions via smart cards (alternatively called chip cards or EMV cards). A smart card contains a chip on the card that stores the credit card information needed to process payment transactions. This data is encrypted and virtually impossible to counterfeit, making it a much more secure alternative to the traditional magnetic stripe for storing sensitive credit card information.

An EMV transaction for a smart card begins by inserting, or "dipping," the card in an EMV-capable payment terminal. The payment terminal will interact with an application on the chip and with a hotel's payment gateway to achieve three things:

1. To confirm that the card is authentic and has not been counterfeited.
2. To optionally request a personal identification number (PIN) or signature from the card holder in order to confirm that the person using the card is the legitimate card holder. Smart cards that support a PIN for verifying the card holder are referred to as chip-and-PIN cards. Smart cards that rely on a signature to verify the card holder are referred to as chip-and-signature cards.
3. To authorize the card for the requested funds.

EMV also supports contactless smart cards, which allow the payment terminal to interact with an application on the card's chip wirelessly. To initiate a contactless transaction, the card holder simply needs to hold the card within close proximity to the payment terminal. Payment applications for smartphones, such as Apple Pay or Android Pay, utilize contactless EMV.

Because of its reliance on payment terminals to interact with a smart card's chip, EMV is only suitable for card-present transactions. Card-not-present activity does not benefit from EMV protections.

PROCESS	RECOMMENDATIONS
Gratuity Tips ¶ 6.12.1 & 6.12.12	After authorization, add any gratuity or tip of up to 20 percent of the base transaction amount to the authorized amount submitted in the clearing record, just as you do today. In this instance, the authorized amount should always be equal to the amount of the bill prior to any added tip.
Hotel Reservations 🛏 ¶6.1	Reservations are handled as normal. The reservation process does not usually require the card being present or the chip being read.
Hotel Check-In 🛏 ¶ 6.3, 6.2.10, 6.2.11	• Complete Authorization at Check-In. • Determine the estimated amount to be authorized. • Process the authorization as you do today.
Extended Stay or Higher Estimated Spending 🛏 ¶ 6.4	If the guest accumulates more charges than authorized for his/her folio, perform an incremental authorization. The card does not need to be present, and the authorization should not include chip data.
Hotel Check-Out 🛏 ¶ 6.5	If the card has been authorized during check-in, a full EMV chip transaction is not required once the final transaction amount is known. If the final amount is significantly larger than authorized, it may require an incremental authorization prior to marking the transaction as ready for settlement. Settle or generate a sale completion for the final billing amount and, if chip data is required for clearing, then include the chip data from the original authorization. Provide receipts as you do today.

🛏 =Hotel   Tips = Restaurant   ¶ = Indicates specific paragraph of the HTNG Payment Systems & Data Security 2010B Specification

Supporting EMV

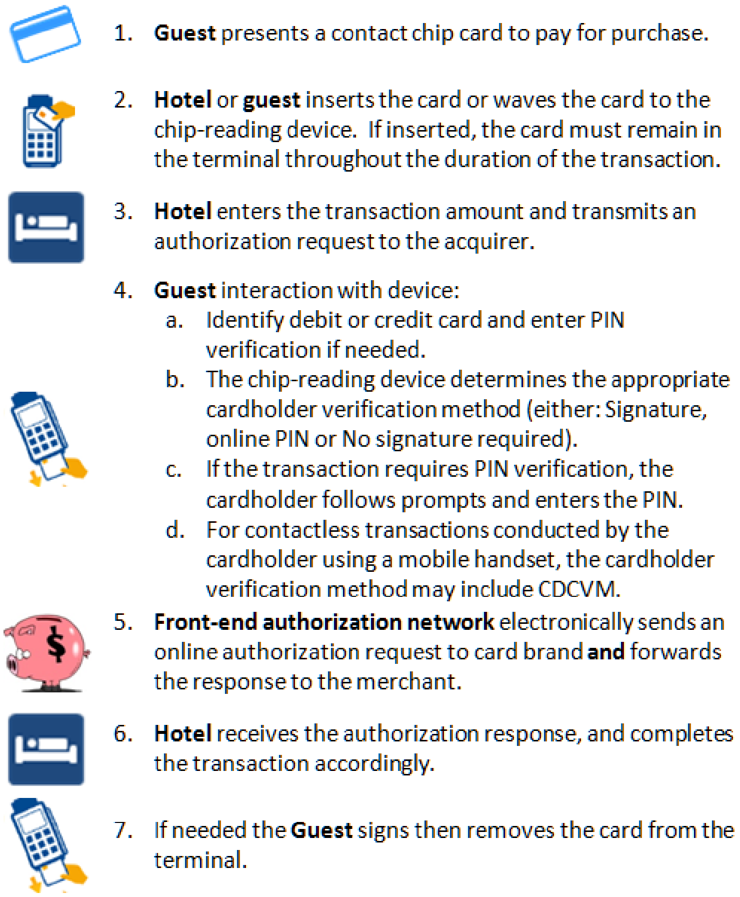
There is more to supporting EMV than simply deploying EMV-capable payment terminals. Although hardware is an important component, there are also software upgrades and workflow changes that need to be carefully considered and planned. Let’s briefly step through each of these.

Hardware Upgrades – Swiping cards in a magnetic strip reader has long been the standard for starting a payment card transaction. These readers cannot support EMV, which means hoteliers must install new devices at front desks, retail stores, restaurants, bars or any other location where card-present payment activity occurs. Hotels should consult with their hardware solution provider for recommendations and best practices related to hardware selection. There is not a one-size-fits-all solution, and the appropriate device for a particular merchant will depend on both their business model and the profile of the guests they serve.

Software Upgrades – Property Management and POS systems also need to support the proper EMV message formats and data flows. These technology providers need to go through new, stringent EMV certification programs with the card associations. Hoteliers need to consult with their vendors when planning and budgeting for an EMV solution to determine costs and timelines for deploying the needed software changes.

Workflow Changes and Employee Training – Unlike magnetic stripe transactions, EMV transactions require that the card be left inserted in the card reader throughout the length of the transaction. Furthermore, chip-and-PIN transactions necessitate that a payment device be presented to the guest. For merchants with a business need to accept chip-and-PIN (and not just chip-and-signature) transactions, the well-established processes of taking a credit card away from the guest at the front desk or after a meal in a restaurant must change. Staff (and guests for that matter) will need to be trained on not just the new hardware, but also on the new workflows. For example, in restaurant scenarios, payment devices will need to be brought to the table for payment. Will enough devices be on-hand so that they can be left with the guest without slowing service? Or will staff choose to “hover” and wait for the guest to enter a tip and complete the transaction? These and other questions will impact the number of devices required to support operations and the guest experience.

The following steps outline the chip card acceptance process:



1. **Guest** presents a contact chip card to pay for purchase.
2. **Hotel** or **guest** inserts the card or waves the card to the chip-reading device. If inserted, the card must remain in the terminal throughout the duration of the transaction.
3. **Hotel** enters the transaction amount and transmits an authorization request to the acquirer.
4. **Guest** interaction with device:
    a. Identify debit or credit card and enter PIN verification if needed.
    b. The chip-reading device determines the appropriate cardholder verification method (either: Signature, online PIN or No signature required).
    c. If the transaction requires PIN verification, the cardholder follows prompts and enters the PIN.
    d. For contactless transactions conducted by the cardholder using a mobile handset, the cardholder verification method may include CDCVM.
5. **Front-end authorization network** electronically sends an online authorization request to card brand **and** forwards the response to the merchant.
6. **Hotel** receives the authorization response, and completes the transaction accordingly.
7. If needed the **Guest** signs then removes the card from the terminal.

A significant majority of EMV cards issued in the United States will be chip-and-signature cards, so the incremental fraud protection that chip-and-PIN transactions can provide will generally have little tangible impact on a hotel’s bottom line. Given this, hotels will need to decide if the added costs and hassles associated with supporting chip-and-PIN transactions are warranted.

Liability Shift

Considering the impact of supporting EMV transactions, it is no wonder that its adoption has been slow. To encourage adoption, card brands have introduced liability shifts so that merchants who do not support EMV will be liable for fraudulent activity that could have been prevented with EMV. The first liability shift began in Europe in 2005, and most major markets other than the United States have all implemented the liability shift.

The liability shift for the United States will go into effect October 1, 2015. Although many of us may have heard this referred to as the "EMV mandate," *nothing* is being mandated or required with this liability shift. Hoteliers can choose to pursue, or *not* pursue EMV. Their decision will in no way impact credit card processing rates, and no fines will be levied if merchants do not accept EMV cards.

The liable party for fraudulent activity depends on the combination of the card and type of terminal being used for the transaction, as summarized in this chart.

Card Type	Terminal Type	Liable Party
Magnetic stripe	Magnetic stripe	Issuer
Magnetic stripe	Chip	Issuer
Chip	Magnetic stripe	Merchant
Chip	Chip	Issuer
Chip-and-PIN	Chip-and-signature (PIN not supported)	Merchant (except for Visa) Issuer (Visa)

The merchant will be liable for most fraudulent activity that occurs with a counterfeit chip card if the merchant does not have payment terminals that can interact with a card's chip. Card brands other than Visa will also hold the merchant liable for most fraudulent activity that occurs with a lost or stolen chip-and-PIN card if the merchant does not have payment terminals that support PIN entry. Visa will continue to hold the issuer liable for any fraud that occurs with a lost or stolen card.

Security Benefits

EMV is intended to make it more difficult to use a counterfeit, lost or stolen card in a fraudulent manner. To make it more difficult to steal the credit card data to begin with, hoteliers should deploy technology to support point-to-point encryption (P2PE) and tokenization. With P2PE, sensitive card data is immediately encrypted by the payment terminal when the information is collected, making it difficult to steal while being transmitted over the network. With tokenization, systems that would otherwise store the sensitive credit card data would rely on a highly-secure credit card vault to store this information on their behalf. The vault can provide a system with a token to reference the card data, but the system would not have direct access to the card data itself.

Tokenization makes it difficult to steal sensitive payment card data from databases or file systems. P2PE makes it difficult to steal sensitive payment card data while it is being transmitted between systems over a network. EMV makes it difficult to use stolen payment data in card-present transactions. Deploying all three technologies maximizes the security of payment processing for a hotel.

Of the three technologies, P2PE is generally considered to be the most crucial to implement. Computers at the front desk are easily compromised by viruses, putting all credit card data entered via front desk workstations at risk of being stolen. P2PE protects card data from computer viruses since there is no way for the information to be decrypted without having the decryption keys.

While EMV is an important part of the secure processing of payment transactions, it is the least crucial of the three technologies since it does not prevent payment data from being stolen, and only provides value with card-present transactions.

Since most of the software and hardware changes needed to support P2PE also apply to EMV, it generally makes sense to implement them together.

Considerations for Deploying EMV

The primary incentive for supporting EMV is to avoid additional costs for fraudulent charges after the liability shift goes into effect in October 2015. For many hotels, however, the card-present fraud and chargeback rate for credit card payments is less than 0.03%, which means that the costs to implement EMV may exceed the risks of the increased exposure to fraudulent charges.

The payment terminals needed for EMV provide additional benefits that should be considered beyond just avoiding the fraud liability:

- EMV-capable payment terminals that also support P2PE can protect hotels from serious data breaches. The costs of a data breach that exposes credit card data can be enormous, easily justifying an investment in P2PE capability.
- Payment terminals that support contactless EMV will also enable a hotel to accept alternative payment options from guests, such as Apple Pay or Android Pay. Providing guests with additional payment options can improve the overall guest experience.
- As EMV transactions become more prevalent, guests will start to associate “dipping” their cards in a payment terminal as a more secure process than the traditional credit card “swipe.” Hotels without EMV capability will be perceived as not being able to adequately protect card data, which could result in more guest service issues.

Impact of EMV on HTNG standards

The primary HTNG standard addressing EMV transactions is the HTNG Payments Processing Specification version 2.0 (2010B). Paragraphs 6.12.9 through 6.12.13 of this specification identify business processes related to check-in and restaurant authorization that are handled differently for EMV transactions (either chip-and-PIN or chip-and-signature). Other business processes are not affected by EMV.

Other payment related specifications – Data Proxy, Hosted Payment Capture and Point-of-Sale – are not affected by EMV and do not directly address EMV.

The recommendations offered in the Secure Payments Framework are not affected by EMV.

Conclusion

EMV is an important part of the secure processing of payment data, and has proven to dramatically reduce card-present counterfeit fraud in regions of the world where it has been broadly adopted. New liability rules going into effect in October are incentivizing merchants in the United States to make the investments needed to support EMV for payment transactions. While there is no requirement for hoteliers to support EMV, those who choose not to do so will be liable for fraudulent activity that could have been prevented by EMV.

Hoteliers who choose to implement EMV should also talk with their software and hardware vendors about implementing tokenization and point-to-point encryption as well. Together, these three technologies provide the best security for protecting guests' sensitive payment data from theft and fraud.

Contributing Members

Juli	Barter	*POST Integrations, Inc.*
John	Bell	*AjonTech LLC*
Eduard	Biete	*Mangalis Management Group*
Larry	Gorman	*SkyTouch Technology*
Diane	Li	*JC Resorts*
Rob	Martin	*Ingenico*
Christian	McMahon	*Merchant Link, LLC*
Jeff	Simko	*Agilysys*
Steve	Sommers	*Shift4 Corporation*
Christopher	Spalding	*Travelport International*
Jack	Jack Waller	*Transaction Resources, Inc.*
Jim	Weiler	*Starwood Hotels & Resorts Worldwide*