EMV IN HOSPITALITY
2 YEARS LATER

Version 1.0

15 January 2018

About HTNG

Hospitality 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 hospitality professionals and their technology vendors to do business globally in the 21st century. HTNG is recognized as the leading voice of the global hospitality community, articulating the technology requirements of hospitality companies of all sizes to the vendor community. HTNG facilitates the development of technology models for hospitality that will foster innovation, improve the guest experience, increase the effectiveness and efficiency of hospitality venues, and create a healthy ecosystem of technology suppliers.

Table of Contents

1 Contributors

Author	Company
John Bell, co-Chair of the HTNG Payments Workgroup	AjonTech, LLC
Rob Martin, co-Chair of the HTNG Payments Workgroup	Ingenico Group
Juli Barter	POST Integrations, Inc.
Christian McMahon	Merchant Link, LLC
Wendy Mertz	Hard Rock Hotels
Daniel Montellano	Shift4 Corporation
Douglas Rice	Hospitality Technology Network, LLC
Steve Sommers	Shift4 Corporation
Tina Stehle	Mandarin Oriental Hotel Group
Jim Weiler	Marriott International

2 EMV & Hospitality

Europay, Mastercard and Visa (EMV) is a global standard for credit and debit payment cards based on chip card technology. Originally written in 1994, it achieved significant implementation in the first decade of the 2000s outside of North America. Canada followed a bit later, while the U.S. started adopting it during 2014. Since then, the U.S. has achieved a fairly high level of adoption, driven in large part by a "liability shift" that makes merchants responsible for certain kinds of fraud if they have not upgraded to EMV.

In October 2015, when the liability shift was imminent, HTNG issued a white paper entitled "EMV for the US Hospitality Industry," providing information to help U.S. hotels prepare for the changeover. This white paper revisits the issues approximately two years after the original one.

Adoption of EMV by the hospitality industry, especially among lodging establishments, has been slow. There is not one single reason why, but rather a myriad of contributing factors.

This document is intended to assist hospitality executives who have not yet made a decision to implement EMV and to help assess whether the timing is right to do so. The document may also be useful to those who have made the decision, but are still in implementation, as it covers some of the issues that may need to be considered.

2.1 The Liability Shift: Why EMV is Important

EMV provides a degree of protection from fraudulent credit cards **physically** presented by guests. However, it is important to understand EMV alone does not protect a typical hotel from data breaches (the theft of payment card data from its systems).

Once a US merchant has implemented EMV, it generally will not be liable for fraudulent charges made in card-present transactions. After October 2015, however, merchants who have not implemented EMV will generally be liable in these situations. It was believed card-present fraud rates tend to be quite low at hotel front desks, but can be much higher in outlets such as restaurants, spas, or retail (where the guest can be gone before fraud is likely to be discovered). Individual hotels and brands should conduct a risk analysis for front desk and retail outlets.

2.2 EMV, Point-to-Point Encryption and Tokenization

While this document is not intended to address Point-to-Point Encryption (P2PE) or tokenization, it is important to recognize that EMV only ensures that presented cards are not fraudulent. Whenever a payment card is presented, the card data is still sent to the gateway or the acquirer and it must be protected. The best way to accomplish this is through P2PE, where the card data is encrypted at presentment and not decrypted until it reaches the gateway or processor. If the hotel systems have no access to the decryption keys, then P2PE prevents a malicious actor from using the hotel system to steal payment card data.

Additionally, many hotel systems need to store payment card data for future use, such as to guarantee future room reservations. Whether the card data was physically dipped, tapped, swiped, or manually keyed, tokenization is the technique that enables the hotel system to use the payment card for future transactions (without actually storing it and risking it being stolen).

Because EMV, P2PE and tokenization are most effective when used in conjunction with each other, hotels should always consider implementing all three together. The goal should be to reduce payment processing risk and lower the cost of PCI DSS compliance.[1] While some payment processing solutions incorporate built-in P2PE, EMV, and tokenization, many do not.

[1] PCI Scope in this document is referring to the merchant scope of compliance for PCI DSS, which can be found here: https://www.pcisecuritystandards.org/merchants/

In addition, it can be significantly more expensive to implement EMV and P2PE separately because you may need to replace the card terminals for each implementation. Implementing both together ensures compatibility across all systems and one-time replacement of payment terminals.

2.3 What EMV Implementation Requires

EMV is a highly technical system that is designed to authenticate the payment card in card present transactions, but in any such system, there are many challenges that must be addressed to achieve the desired outcome. Governing bodies, such as EMVco and the card brands, offer and require certification processes for products participating in EMV transactions.

The important thing to understand about EMV certification is that it applies to the combination of the payment device, the payment gateway, the acquirer, the merchant services provider and the country. EMV certification may also apply to hotel systems (such as the PMS and/or POS) if they are a part of any transaction including unencrypted EMV card data. The certification process is time-consuming and expensive; therefore, it is important to consider whether a particular combination has already been certified, and if so, to which versions of the various products. A hotel's desire to continue working with a particular acquirer may, for example, limit the choice of payment terminal and gateway. Over time, more and more payment services and terminal providers are being certified in various combinations, but it is the merchant's responsibility to ensure all pieces are certified to work together in each country where it needs to be deployed. For many hotel companies, different combinations will be necessary to meet the needs of hotels in each country.

The standard is also evolving, as some solutions include Quick Chip and other additions that make the process faster and increase the security level.

3 Challenges in EMV Implementation in Hospitality

This section addresses some of the principal reasons why EMV implementation has lagged in hospitality.

3.1 Need for Integrated Devices

When EMV arrived, most integrated merchants had the choice of waiting for new EMV devices to be integrated with their business systems, or implementing EMV without integration, reverting to a stand-alone bank terminal.

The business needs of most US hotels generally require payment devices that can integrate with their property management system and/or point-of-sale system (PMS/POS). However, when EMV was first introduced, this integration was not supported. Devices were standalone units connected through a network to the merchant processor or bank. Integration, while not essential, helps to address problems such as dropped and/or duplicated transactions, pre-settlement auditing, slow user experience, a more seamless operational workflow (no double entry) and other issues. Hotels that currently benefit from the ease of integrated payments will generally not want to give up this capability for the sake of EMV implementation.

3.2 Challenges with Integrated Devices

The version of each component of the payment process ecosystem (PMS, POS, PIN pad device, gateway) needs to support EMV processing; all components involved in the EMV flow need to be certified. **It is important** to note that EMV certification is required for any component that touches plain text EMV data.

Once all of these steps have happened, and the devices have been ordered, delivered, configured and are ready to go live, the hotel can proceed cautiously. There are many ways to misconfigure an EMV system, and the only way to know if the full system is configured correctly is to turn the system on in a live production environment. In a large installation, cutover is a significant risk; therefore, a pilot site should be tested before the bulk of the new devices are configured and distributed.

3.3 The Payment Industry was Late to Comply

The US payment industry got a late start for various reasons (including legislative changes, such as the Durbin Amendment) which delayed implementation through the payment industry. Due to the domino effect, complex integrated systems in hospitality and the certification process, device and software support for lodging transactions came well after the October 2015 deadline, delaying the adoption of EMV.

Today, nearly all of the payment technology providers in hospitality offer full support for EMV.

3.4 Gateways & PMS/POS Direct Connects

Many hotels connect to credit card networks electronically from their PMS or POS, either directly or via third-party gateways. To support EMV, these hotels needed their PMS and/or POS and/or gateway vendors to upgrade interfaces to support EMV. Assuming these companies had experience working with devices, and that they were architecturally set up for EMV, the integration projects could be started only after the acquirers or merchant processors had completed their own work and published specifications. Gateways, PMSs and POSs were required to certify for each device family (e.g., Ingenico and Verifone) and each processor (e.g., Chase Commerce and First Data Rapid Connect) with whom they chose to work with. Certification is a resource intensive, time-consuming and costly exercise. Gateway, PMS and POS providers had to prioritize scarce resources, based on their own product roadmap and customer needs, and choose which processors and devices to support and when to do so. Some gateway providers decided to sunset some of their legacy technologies during this time rather than incur the costs

of certification. Many PMS and POS vendors that had historically communicated directly with processors deprecated those connections and moved to work with gateway partners instead.

As of late 2017, gateways, PMS, and POS vendors have been completing their US EMV certifications (and many are finally making the new solutions available to clients). Functionality is starting to be expanded to support such functions as contactless EMV and "Pay-at-Table" workflows for restaurants.

3.5 Deployment & Implementation Experiences

As acquirers, gateways, terminal manufacturers and software vendors rushed to implement the complex new EMV requirements, the flow of information has often been confusing. Continual changes to unfinished integration projects led to frequent miscommunications and information gaps. Hotels need to work with all partners involved and pay careful attention to specific software versions that are supported and certified. All parties need to agree as to the level of certification required between the PMS or POS, the gateway, and the device, as this can vary depending on the architecture of the solution; the vendors should all be able to confirm that the solution conforms to the P2PE and tokenization requirements. Hotels should confirm the proposed solution in writing with all vendors, restating all software versions, compliance claims, and the reasons supporting any claims of compliance exemption. Hoteliers may also need to evaluate creative cable management techniques (so connections are invisible to the guest), as well as additional cabling for the PIN pad device.

3.6 Food & Beverage Pay-at-Table Scenario

Merchants operating restaurants should consider pay-at-table solutions, which are starting to become available from many vendors. Since pay-at-table solutions should ideally work with the chosen gateway or bank solution, vendor compatibility should be considered when implementing EMV (even if pay-at-table is not done at the same time). While some pay-at-table solutions may operate independently of current banking relationships (and thus may not require compatibility), the choice of such a provider could affect transaction volume with existing acquirers and result in unexpected fee increases, which need to be factored into the cost.

Hotel infrastructure is very complex; hotels cannot simply plug in a stand-alone terminal that will allow them to process pay-at-table transactions without compensating controls and well documented processes to properly track settlement. Technology updates include the integration between multiple systems and require the inclusion of multiple third parties. Questions to ask your vendor include, but are not limited to:

- Does the POS have the ability to support pay-at-table functionality?
- Is the gateway provider certified with applicable devices that support pay-at-table functionality?

EMV works just fine in restaurants for non-PIN credit card transactions, which cover the majority of US issued cards. However, if the POS system does not support pay-at-table, it may be necessary to turn off the capability to enter a PIN ("PIN bypass"). This requires asking a guest with a non-US issued Chip-and-PIN card, for which the PIN requirement cannot be overridden, to walk over to a server station to enter their PIN, which may be undesirable (especially in fine dining outlets). Additionally, by disabling the PIN, the hotel opens itself up to chargebacks from the use of cards that are PIN-preferring (US issued cards where the issuer prefers but does not require the use of a PIN).

Continued work by vendors is likely to result in new solutions in the future.

3.7 Card Present (Counterfeit) Fraud

Card present fraud occurs when criminals make copies of legitimate credit cards. This is done by copying data contained in the card's magnetic stripe and then programming that data onto phony or counterfeit cards. Prior to October 1, 2015, card present (swiped/signature) counterfeit fraud chargeback liability was absorbed by the issuing bank and not passed on to merchants. This changed, and after October 1, 2015, the liability for counterfeit fraudulent transactions will move to the "weakest link" in the transaction. For merchants who are not EMV enabled, they may have seen an increase in counterfeit fraud chargebacks, even though the merchant may have swiped the card to prove that the card was present. If the swiped

card has Chip technology, and the merchant does not have a Chip-accepting terminal, the merchant would be liable for the chargeback. In many cases, this is an increase in chargeback costs in areas that previously had little expense related to card present transactions.

4 Appendices

4.1 Glossary of Terms

An online glossary of terms may be found here: http://www.htng.org/paymentsglossary

4.2 Cryptographic Key Injection Notes

To support PIN-preferring cards issued in the US, the hotelier will need to have a cryptographic key injected that is tied to their specific acquirer. This acquirer PIN key must be injected at a secure key injection facility (KIF) that is certified under the PCI PIN program. Most P2PE programs also use symmetric cryptographic keys that must be injected in a secure, certified KIF.

Terminal distributors and terminal manufacturers generally offer cryptographic key injection as part of their service offering. These KIFs have a library of keys from acquirers and P2PE providers. Unfortunately, there is no KIF that has a full library of all acquirer PIN keys and P2PE provider keys as the transferring of keys from an acquirer or P2PE provider involves contractual, industry regulatory and operational security complexities.

This places a burden on the hotelier purchasing equipment to find a distributor with a KIF that can provide the terminal devices injected with the proper keys. This may require contacting multiple distributors to find the complete package.

On top of ordering devices with the appropriate acquirer PIN key, P2PE key and current device firmware, the hotelier may want to make sure the appropriate software is loaded on the device so that when a processor change is performed (if even possible), the hotel can do remote key injection (RKI) and update the PIN key on the device. Without the required software, performing remote updates will not be possible, and any processor change will be delayed. If not handled correctly at the onset, this could literally mean having to unplug, repackage and ship devices back to a KIF for re-injection.