THE HOLY TRINITY OF PAYMENT SECURITY

May 2015

creditcall
The Heart of Payments

THE QUEEN'S AWARDS
FOR ENTERPRISE:
2014

creditcall.com

Contents

"There remains a lot of confusion and uncertainty among those who are tasked with actually ensuring and implementing the security — namely, software developers."

The Holy Trinity of Payment Security

Payment security remains a topic of great consequence in North America due to the recent number of card holder data breaches as well as the imminent EMV liability shift in October 2015.

Despite absolute agreement on the need for heightened security, and the involvement of many large players from the industry, there remains a lot of confusion and uncertainty among those who are tasked with actually ensuring and implementing the security — namely, software developers.

Today, security technologies such as tokenization, EMV, and P2PE (point-to-point encryption) are considered the solutions to today's threats. However, each has its strengths and weaknesses. In this report, we'll take a closer look at each security method and illustrate how, separately, the technologies fall short, but together, can be leveraged by ISVs to form the best and most secure payment security solution possible.

"A P2PE solution is a combination of secure devices, applications, and processes that encrypt data using cryptographic keys only known to the payment company or gateway..."

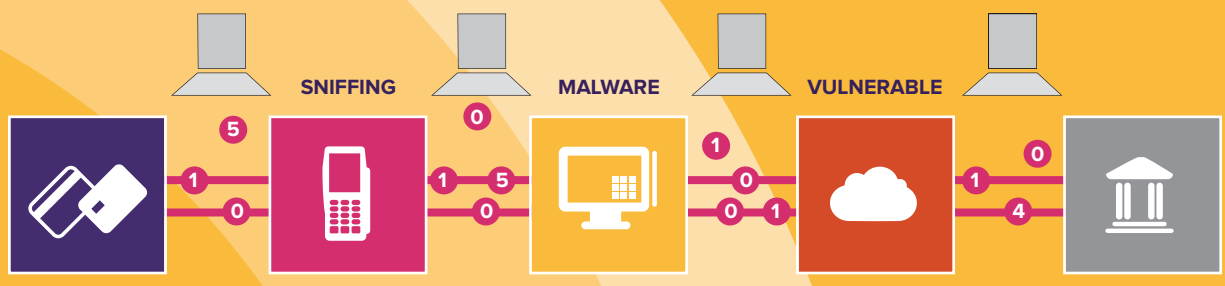
P2PE

Going back 10 years, criminals were less technically sophisticated than they are today. Criminals now are very technically savvy and comfortable with intercepting card readers, skimming, and scraping memory from Windows machines.

In the past, we would have thought such actions were too difficult or required too much effort. Now, such methods are commonplace and common knowledge. As a result, it's become necessary to change the methods being used to combat criminals who sought to intercept valuable card holder data. P2PE is the answer.

A P2PE solution is a combination of secure devices, applications, and processes that encrypt data using cryptographic keys only known to the payment company or gateway from the earliest point of the transaction (i.e., at the point of swipe, dip, or tap in the case of contactless payments) until the data reaches the payment company. With this security method, any data intercepted would be worthless to a criminal.

Without P2PE



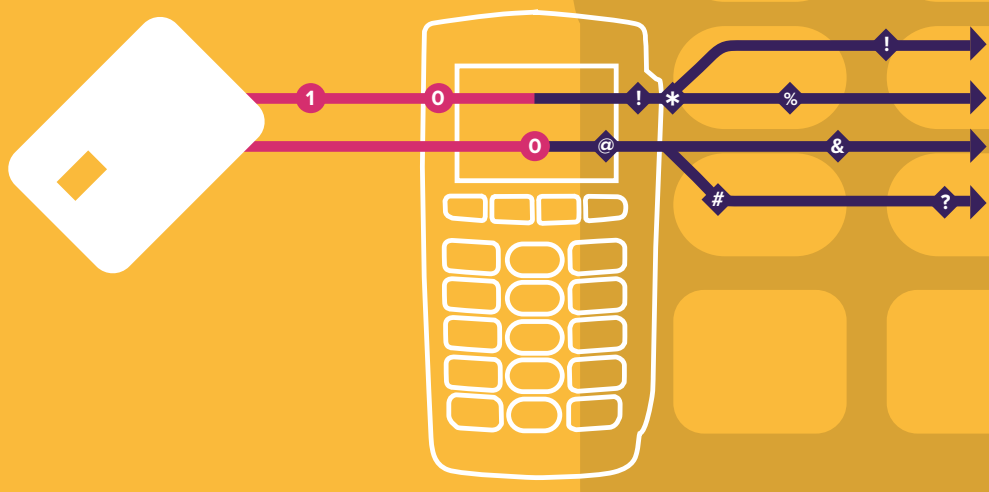
WHY P2PE WORKS

One of the challenges with P2PE due to the cryptography is the management and sharing of keys. Simply, how does a cryptographic key get into the card reader? The solution is an algorithm known as derived unique key per transaction (DUKPT), or "duck putt." With DUKPT, a base key is generated, and shared with the device manufacturers in a secure manner. Each card reader or PINpad manufactured gets its own unique key derived from this.

As a result, if a criminal goes through the effort of somehow compromising a single card reader, they won't be able to leverage that information to gain access to other card readers. More importantly, the key changes for each transaction. This makes for very secure transactions and creates a constantly moving target for would-be criminals.

For the sake of comparison, assume the key on a cryptographic reader is fixed, and a criminal gets their hands on the device. One could run multiple cards through that reader and analyze the resulting output data. By knowing the input data, and studying the output data, it's possible to reverse engineer the cryptographic key. With DUKPT, running the same card through a reader a million times will result in output data that will be different every time, making it impossible to reverse engineer cardholder data.

With P2PE



PROS & CONS OF P2PE

Apart from the benefits of encryption for card holders, P2PE technology creates a huge benefit for ISVs and merchants as well. PA-DSS certification was designed to address the problems created when card holder data is not encrypted.

When an application uses P2PE, it no longer has to be PA-DSS (Payment Application Data Security Standard) certified. This can be a significant time and cost benefit for ISVs that have historically gone down the PA-DSS route, and help to remove customers from scope. That said, while introducing P2PE takes care of PA-DSS, it does open the door for a new certification, PCI P2PE, which today is the best way to address the scope defined in PCI DSS.

"The biggest potential downside of P2PE is that it isn't cheap if you want to do it in-house."

The biggest potential downside of P2PE is that it isn't cheap if you want to do it in-house. The generation and management of DUKPT-based keys is done within a secure cryptographic device known as a Hardware Security Module (HSM), which is a highly-specialized tamper-resistant computing device used to securely manage, create, and store cryptographic keys. These devices can run $30,000 to $40,000 each and when you build out everything you need, the cost can reach $100,000. Beyond the costs of HSMs themselves, you're looking at months, if not years, of work in creating the proper environment for a P2PE solution.

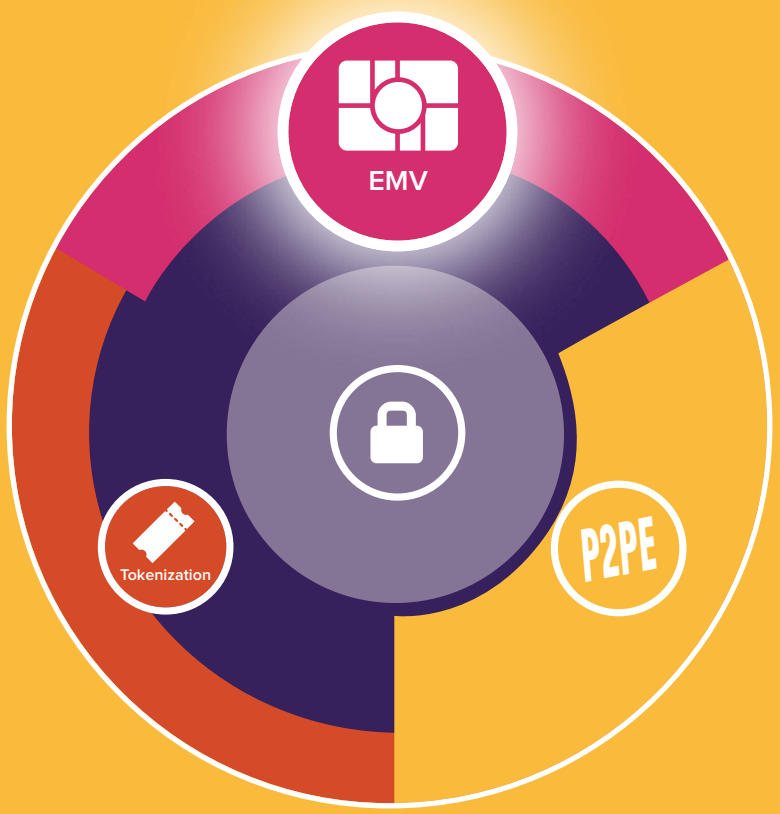
"You're looking at months, if not years, of work in creating the proper environment for a P2PE solution."

P2PE

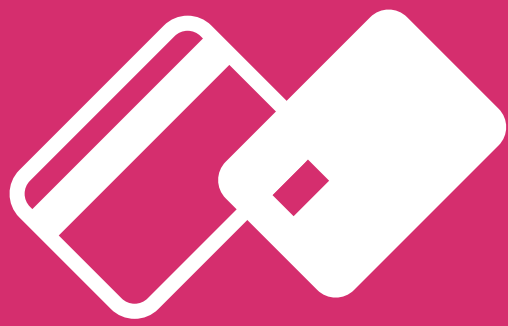
Alternatively, ISVs can partner with a company that hosts this expensive infrastructure and shoulders the burden of maintaining it. Additionally, such a partner could already have the PCI P2PE certification mentioned earlier, saving an ISV the additional burden of seeking that certification themselves.

Apart from these factors associated with P2PE, there's an issue that ISVs could run into if they have functionality that relies on using the PAN (primary account number). Applications that rely on using the PAN will need to be altered to function without this data since it isn't available on the back end of a P2P-encrypted device. While this might be a nuisance to ISVs, the benefits vastly outweigh the need to change some code. Indeed, P2PE boils down to a decision for ISVs — albeit a simple one. Would you like to not have to deal with PA-DSS? Would you like your merchants to have a reduced PCI scope and give your software a distinct marketable quality? The cost might be as simple as some coding changes.

Despite all of its benefits, P2PE doesn't solve the problem of counterfeit cards. A counterfeit mag-stripe card run through a P2PE device will be encrypted and the transaction will proceed without fail. To protect the cards themselves, we need EMV.



EMV



PROS & CONS OF EMV

Fundamentally, EMV relies on the use of an integrated chip embedded into the payment card to ensure the card being presented at the point of transaction is authentic and belonging to the person using it. Whereas mag-stripes are easy to counterfeit, EMV chips are not. Additionally, EMV uses cryptography to create dynamic data for every transaction. The combination makes for a powerful guard against credit card skimming.

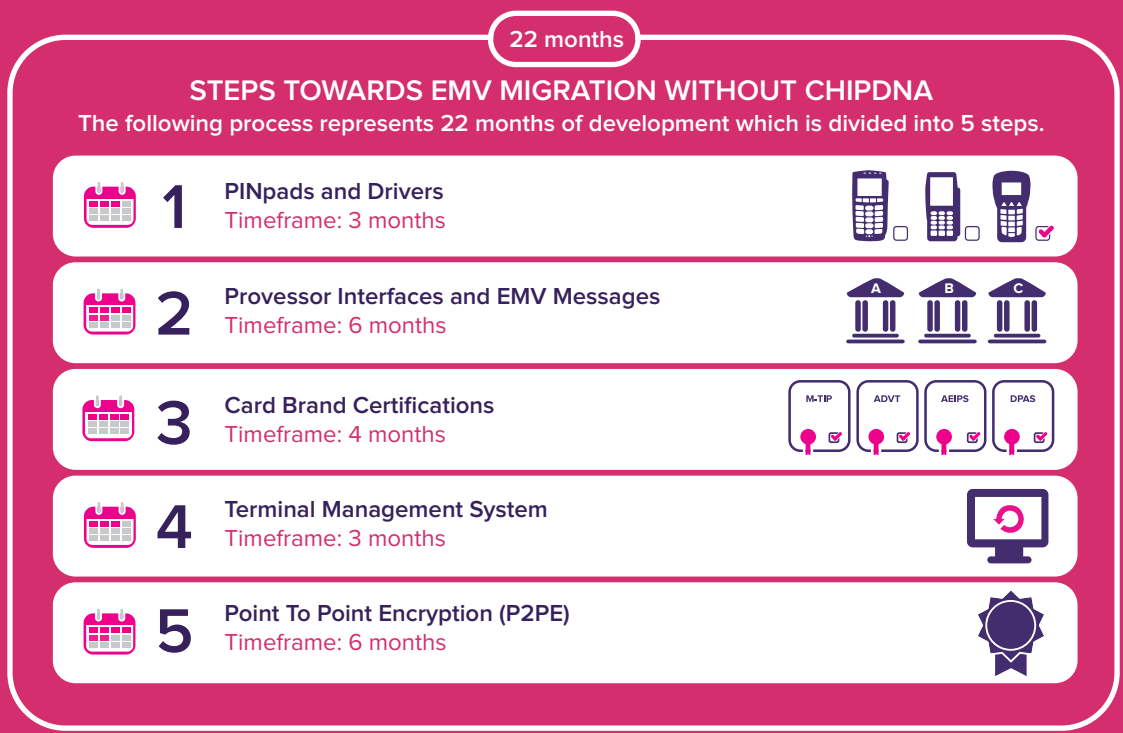
However, to leverage the power of EMV, new payment terminals are required to read the chip-enabled cards. These terminals have been one of the factors slowing down the adoption rate in North America. Traditional mag-stripe readers, which have been around for decades, are relatively affordable, while EMV devices can cost ten times as much.

The biggest downside to EMV for ISVs in North America is the complexity of creating an EMV solution. While the security benefits are clear, there's a lot of confusion and stress as various processors each want things done differently and the process for certifications is often complex and nebulous. It's not impossible for an ISV to build EMV solutions in-house, but it's difficult and unnecessary when there are plug-and-play EMV solutions available

"It's not impossible for an ISV to build EMV solutions in-house, but it's difficult and unnecessary when there are plug-and-play EMV solutions available. "

EMV CERTIFICATION CHALLENGES ABOUND

A typical ISV interested in certifying a few PINpads with a few processors faces up to 22 months of work and some considerable financial expenses. Additionally, certifications need to be revisited every couple years.



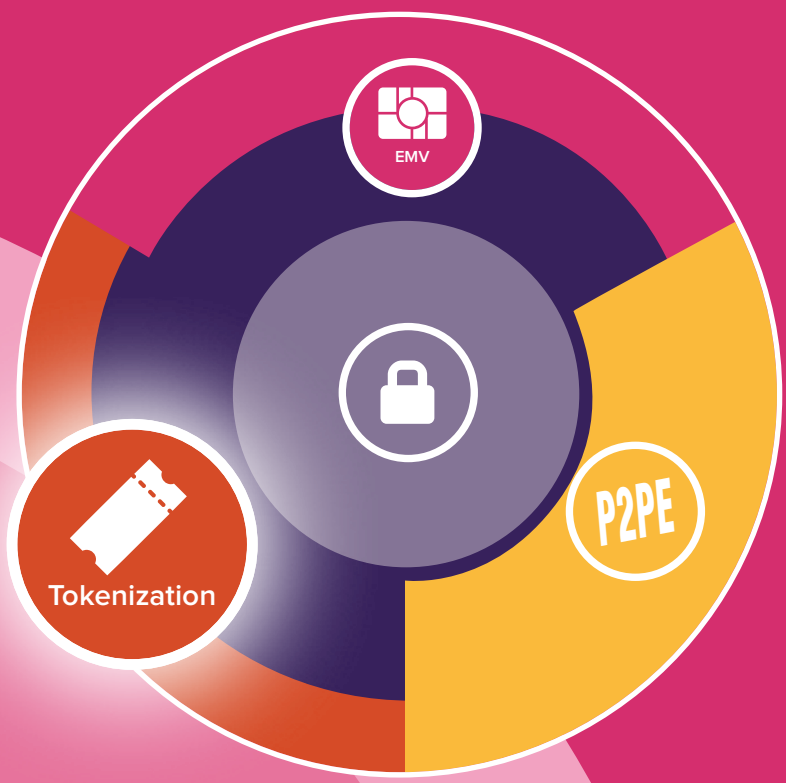
Finally, due to a large number of pending certifications, processors are going to be fairly backed up over the next few years. Unless an ISV has large merchants using its software, it will most likely find itself toward the bottom of the certification waiting list. In short, ISVs looking to deal with EMV alone are in for a frustratingly long and costly process.

"ISVs looking to deal with EMV alone are in for a frustratingly long and costly process."

EMV

Therefore, just as most ISVs would be advised to rely on a partner for P2PE, EMV migration is similar due to the significant cost and time benefits of plug-and-play EMV solutions such as Creditcall's ChipDNA. Indeed, leveraging prepackaged and pre-certified APIs removes most, if not all, of the need for research, certifications, and complexity while the payment partner shoulders the burden of uncertainty, risk, time, and cost.

Surely, P2PE and EMV make for very effective security measures to protect card holders. And yet, there's one additional security measure ISVs shouldn't overlook.



Tokenization

The PCI DSS standard dictates that card holder data must be protected when it's stored. The best way to do this is via Tokenization.

The PCI Security Standards Council describes tokenization as a process by which the primary account number (PAN) is replaced with a surrogate value called a token. De-tokenization is the reverse process of redeeming a token for its associated PAN value. Essentially, this process replaces sensitive card data with valueless data.

Tokenization is particularly appealing when merchants have a need to reuse card holder information such as with recurring billing, future payments, loyalty programs, or operations such as refunds (often seen with hotels, bars and rental services). Storing tokens instead of PANs means merchants can store transaction data without running into PCI scope issues. ISVs interested in tokenization either have to build out their own system (practically becoming a payment gateway), or work with a trusted provider.

While tokenization is essential, on its own it does not prevent one method used in many recent retail card breaches. That is, if malware is remotely installed on POS devices, it's possible for customer card data to be stolen before it is tokenized. Therefore, it's essential to pair tokenization with P2PE and EMV to protect cardholder data at all transaction points and offer optimal security.

Conclusion

THE STRONGEST PAYMENT SECURITY RELIES ON ALL THREE

ISVs face an uphill battle learning, understanding, and incorporating these three technologies into their software. The job becomes even more complex when you consider how they all need to interoperate.

A common theme to each of these technologies is that they require significant investments of time and money to properly implement. The fastest, easiest, and most affordable answer is to partner with a payment company that has the experience and infrastructure in place to offer plug-and-play functionality to ISVs such as Creditcall.

Taken independently, neither P2PE, EMV, nor tokenization are the strongest, most complete security measures. However, when combined, they form today's most powerful and effective shield against payment crime.

creditcall

The Heart of Payments

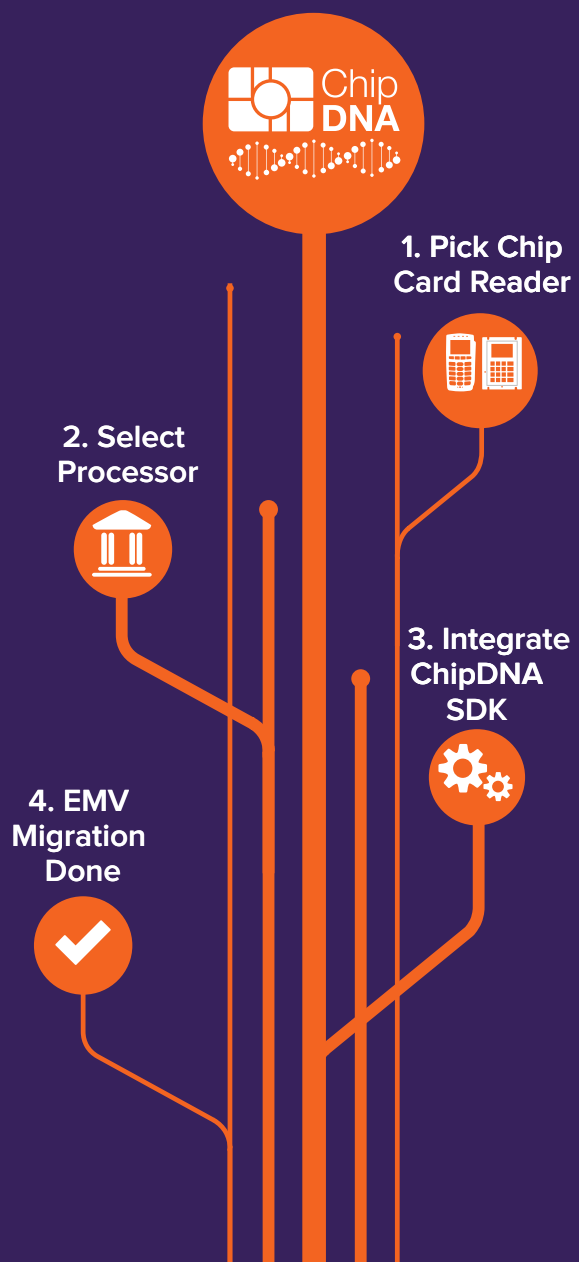
Creditcall makes card acceptance simple from any device, anywhere. No matter if in retail, hospitality, parking or transportation, our award-winning EMV-ready Payment Gateway and EMV Kernels are at the very heart of our clients' business. No matter if in-store, online or mobile, we ensure payments flow securely, all day, every day.

Founded in 1996 and with over 14 years of proven track record in EMV Migration, Creditcall's plug-and-play ChipDNA SDK provides the most secure, simplest and fastest route for developers, ISVs and VARs to enable EMV payments in Windows, Windows CE or Linux based Point of Sale (POS) applications. ChipDNA removes the complexities of EMV Migration and dramatically reduces the lengthy certification processes.

With ChipDNA you will have access to:

- **Security** - Point to Point Encryption (P2PE)
- **Simple Integration** - SDK
- **Speed to Market** - Accelerated route to EMV from months to a few days
- **Flexibility** - Pre-certified with major processors
- **Choice** - Multiple attended and unattended PINpads supported
- **Updates** - Ongoing compliance and certification updates
- **Remote PINpad Management** - Terminal Management System (TMS)
- **Reliability** - Data synced in four data centers
- **Cross Industry Expertise** - Retail, hospitality, parking, vending and transportation

Creditcall – The Heart of Payments.



Regional Offices

Creditcall North America
1133 Broadway, Suite 706, New York, NY 10010, USA
T: +1 (800) 868 1832
E: *hello@creditcall.com*
W: *www.creditcall.com*

Creditcall Europe
Merchants House North, Wapping Road, Bristol, BS1 4RW, United Kingdom
T: +44 (0)117 930 4455
E: *hello@creditcall.com*
W: *www.creditcall.com*

Registered No: 3295353.
VAT Registered No: 713 0076 80.

For more white papers from Creditcall, visit *www.creditcall.com/white-papers*

creditcall
The Heart of Payments

THE QUEEN'S AWARDS
FOR ENTERPRISE:
2014