paybook

Presented by Verifone
Vol. VII • October 2017

Payments: Inside and Out

Imagine you're on a treasure hunt—actually, multiple treasure hunts. You have different maps for finding different buried chests, all starting from the same Point A. Each map has directions on how to get to Point B, Point C, and so on, with specific instructions such as, "Walk 10 paces north" or "Five paces west." Simply follow the directions and you'll find your buried treasures.

Now, imagine having the maps, but Point A is hidden. What good are all those coordinates if you don't know where to start? Sure, you can stumble upon a treasure, but the odds of this are greater than a billion to one.

In the treasure-rich landscape of electronic payment processing, an encryption algorithm is only as strong as its keys. The keys are what allow sensitive data to be encrypted and decrypted from one point to the next, with the most important key—the master or base derivation key—being the secret Point A. If not kept secret, eager pirates would have free rein to intercept any and all sensitive cardholder information available, right from the point of first contact with the payment device.

Verifone has long used DUKPT in its payment solutions, since at least the early 90s, but the standard has seen its own revolution over time. Today, AES (Advanced Encryption Standard) DUKPT offers an algorithm that can do everything previous incarnations of DUKPT could do, but at scale. Specifically, AES DUKPT takes advantage of advancements in cryptography to allow for greater processing speeds; a terminal can handle more transactions from its single, initial key than is expected for the life of the device.

"There is a real push to use the AES version of DUKPT," said Vance, who co-created the new standard and has been behind the push since 2009. "With the existing DUKPT, known as TDEA DUKPT, each device's unique initial key is limited to just over 1 million transactions. With AES DUKPT, each device can support nearly 2.5 billion transactions."

While the scale of AES DUKPT is vital, especially for high-traffic areas, the security of its encryption standard is still seen as the biggest advantage, according to its co-creator.

THE MASTER OF KEYS

The algorithm securing payments— at a scale like never before.

For every master key in the payment process, other important keys are derived along the way that handle encryption, decryption, authentication, and integrity of data. The modern industry standard for this key management scheme is known as Derived Unique Key Per Transaction, or DUKPT (pronounced "duck putt"). The algorithm was first introduced in the late 1980s by Visa, but didn't achieve industry relevance until the 1990s.

The strength of DUKPT as an algorithm is its ability to generate unique keys for every transaction (like our unique treasure maps from before), without requiring the device that originated the transactions to retain any sensitive information that could link to any previous keys. Using the master key (our Point A) and data elements contained in the transaction, the receiving device can derive the key used by the originating device.

"DUKPT simplified key management on every device; it made them safer," says Joachim Vance, Chief Security Architect at Verifone. "Before DUKPT, payment devices were not considered very secure. They were vulnerable as far as protecting the keys used in each transaction."

"The main advantage of AES DUKPT is AES itself," says Vance, noting that AES was approved as a federal government standard over 15 years ago. "AES DUKPT allows the future of financial transactions to finally move into the best security that cryptography has to offer. AES DUKPT supports up to 256-bit keys, which are immune from all known methods of attack, even quantum computing attacks."

In September 2017, AES DUKPT was approved by ASC X9, an accredited standards developing organization for the U.S. financial services industry. While it won't be commonly used until next year, Verifone has functioning implementations ready to go. We expect all of our new devices to support AES DUKPT in 2018.

Payment security—with the proliferation of EMV, end-to-end encryption, and tokenization—continues to be a top priority here at Verifone, as we strive for solutions that protect the billions of transactions passing through our systems on a monthly basis. As an early adopter of AES DUKPT, we aim to increase that protection to anywhere and everywhere fraudsters may lurk.

Check, please

Why the U.S. appears to be behind the times when it comes to paying at the table, and how this may soon change.

"We're in a different spot than Europe," says Drago Dzerve, Vice President of Product Management at Verifone. "But yes, it's definitely coming to the U.S."

If you've been to a restaurant in Europe, chances are your waiter has brought a payment device to you at the end of the meal. This simple change in how you pay in a restaurant offers an additional level of convenience, speed, and security to the dining experience. For instance, you don't need to wait for your card to be charged and then brought back to you; it happens all at once, right at the table. And if you're with a large group that needs to split the bill, it's incredibly simple. When all of the transactions happen at the table, instead of somewhere else in the restaurant, there's also less room for theft.

So why hasn't the U.S. adopted pay at the table (PATT)?

Some have suggested it's because of the tipping culture in the States. Tips are not a requirement in Europe, and as Russell Boone, senior partnership manager at Vantiv, has stated, "There's kind of a stigma around [pay-at-the-table] in that you're thinking the server is going to be like the bellhop and wait for a tip." The awkwardness of tipping in front of your waiter instead of discreetly in a closed billfold may contribute to the low adoption of PATT.

> "There's kind of a stigma around pay-at-the-table in that you're thinking the server is going to be like the bellhop and wait for a tip."

Others have suggested that Americans value the ceremony of the receipt signature. In other words, we prefer our tradition of "picking up the check", signing it, and then relaxing as we finish the rest of our drinks.

But Dzerve believes he can answer this question in three words: chip and PIN.

He explains that in the early 2000s, Visa and MasterCard mandated the use of chip-and-PIN cards for transactions in European countries. For the U.S., they only required a simple signature. The act of entering a PIN changed the restaurant industry dramatically. Because you can't simply tell your PIN to your waiter, restaurants needed a way to have their customers enter their PINs discreetly without disturbing the dining experience. This caused mass adoption of mPOS devices in European restaurants.

In the U.S. where there's no need to enter a PIN, waiters can simply bring a receipt slip and pen to your table. So, the implementation of PATT in Europe was really born of necessity, not a desire for convenience.

But the good news is that Dzerve believes we're fully ready and capable of doing more with PATT in the U.S. However, he isn't sure it'll be exactly like it is in Europe.

"It might be Ziosk, it might be TabbedOut, it might be something completely different. It's all about the why," says Dzerve. Ziosk is a device that sits at the table and facilitates ordering and payments, and TabbedOut is an app designed to help you pay the check with your phone. He goes on to explain that there are three main reasons why a restaurant should implement a PATT system:

1. **Faster turnover.** Ziosk boasts that it will save a restaurant eight minutes per table on average. Increased table turnover is a big deal for restaurants, and if you have, say, 20 tables, you're looking at an extra 160 minutes of time you can devote to additional customers.

2. **Security.** The less time a card spends out of the hands of its owner, the more secure it is. Plus, hackers have an easier time penetrating one POS in the back of the restaurant than 10 secure payment terminals wirelessly connected.

3. **Convenience.** Perhaps some customers really do appreciate the ceremony of the check, but Dzerve is willing to bet that, more often, a customer appreciates a good use of his or her time. The time-saving factor of PATT and the ease of splitting the check are great conveniences that anyone would appreciate.

Still, there are issues for Americans, one of which is scale. For large chain restaurants, implementing a PATT system can be very costly. There's also the matter of the learning curve involved in training the staff. A pessimistic restaurant owner might not buy the eight-minutes claim and instead figure it's more like two to three minutes saved, which makes the call to invest in PATT much more difficult.

Regardless, at Verifone, we're prepared. Devices like our e355 and VX 690 can perform PATT in any restaurant environment. They both connect to Bluetooth and WiFi for uninterrupted service. They accept all the latest payment methods (EMV, mobile wallets, etc.), and are extremely durable, cost-effective, and easy to operate.

So, if you're a restaurant owner in America looking to get a competitive edge, pay at the table is the answer. For the investment, you'll provide extra security, convenience, and speediness for your customers. But it'd be wise to act soon, as it's likely your competitors are already looking into a PATT solution as you read this.

For more information, contact Drago Dzerve at DragoD2@verifone.com. ∎
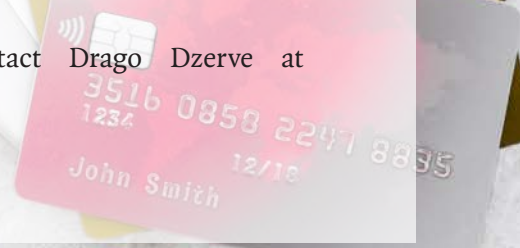
Pump up the value

The petro market is entering a new horizon of payment security and technology, one that better protects and engages its customers.

The current state of the U.S. petroleum retail industry, and the more than 150,000 gas stations and convenience stores across the country, is one of ongoing transition. Much like the broader spectrum of retail merchants, petro retail is reacting to recent changes in payment technology and security sweeping the landscape.

Among the current advancements in payments, the one most pressing from a regulatory standpoint is EMV. The migration from magstripe to chip cards is already underway in retail, due to the October 2015 liability shift pushed by Visa and Mastercard. Since the shift, merchants not equipped to accept EMV payments are on the hook for any fraud-related liability.

For payment terminals in gas pumps, the deadline for EMV migration was set for October 2017, but in December 2016, that deadline was pushed back to October 2020. The delay is due to the complex nature of fuel dispensers—merchants need to factor in not only the technology, but the regulatory obligation that comes with a combustible product like gasoline. The resulting three-year reprieve gives petro merchants more time to adopt EMV, which has emerged as the global standard in secure payment card transactions.

Verifone, aware of the vast undertaking EMV at the pump requires, partnered in 2014 with the top fuel dispenser provider in the business, Gilbarco, to address the matter head on. Under the partnership, Verifone provides the technology for EMV acceptance, which is then integrated into Gilbarco's dispenser product line.

"When Visa announced the extension for EMV compliance, from 2017 to 2020, it gave retail operators more time to convert locations," said Michael Tyler, Sr. Director of Global Petro Marketing for Verifone, about the EMV rollout. "It's an enormous task with limited resources; time is really of the essence. Fuel is the last area not safe from EMV protections."

In 2016, Verifone and Gilbarco launched FlexPay IV, the first PCI PTS 4.X-certified fuel dispenser payment terminal in the U.S. to support EMV. While FlexPay IV represents the best in payment security technology, that's not where its innovation ends. The terminals also support NFC, mobile wallets, encryption, and 2D barcode scanning for loyalty, making FlexPay IV a truly universal, commerce-enabled device.

As it happens, while dispensers across the country are either being retrofitted or replaced to support EMV, the simultaneous emergence of mobile payment at the pump has created an opportunity for merchants to kill two birds with one stone, by upgrading to a terminal that can accept both EMV and mobile. In today's app-driven society, it's no surprise that gas companies are looking at ways to engage customers via their smartphones, and even their smart cars. By partnering with innovators in payment technology, giants like Gulf and ExxonMobil can offer more than just payment apps—they can provide value-added services like location searching/routing, loyalty programs, and more.

Just as it did with EMV, Verifone took a proactive approach when it came to mobile pay. Aligned with top partners in mobile payment tech, POS manufacturing, and petro retail, Verifone engaged with Conexxus—the standards body of the convenience store and petroleum market—to establish a new mobile payment API standard.

By adopting and deploying the new Conexxus Mobile Payment Standard, dubbed Mobile 2.0, Verifone is embracing a cooperative industry solution that also benefits the consumer.

"We've been able to partner with so many great companies in this space, all with different ways to deploy innovative payment and value-added services at the pump," says James Hervey, Director, Product Management at Verifone. "It's the beauty of having an open interface, with different providers offering their strengths and benefits. We're essentially telling merchants to pick what best suits their needs—that we will support whatever payment scheme they bring to us."

The payments industry is constantly evolving to make way for new advancements, and petroleum retail is no stranger to the rising tide. In fact, it's becoming a haven for commerce innovation. ∎

PSD2:
Return of the Directive

In 2018, Europe is extending its Payment Services Directive to include better security and a lower barrier of entry for new payment facilitators.

In the early 2000s, changes in payments were happening everywhere in Europe, but banks were slow to adopt them.

"Some of the non-bank players were coming up with solutions that were good for consumers, but the banks were slower to bring these solutions to market," says Neil Burton, Chief Administrative Officer of Verifone Europe.

But this all changed in 2007 when the European Union issued the Payment Services Directive (PSD), which held third-party payment facilitators to the same standards as banks. After the directive, these third parties, such as PayPal and Western Union, became Authorized Payment Institutions (APIs), and the banks were more compelled to work with them now that everyone complied with the same rules and regulations.

Innovations like greater convenience and cheaper peer-to-peer payments had existed for a while, but after PSD, the banks had good reason to start bringing these innovations to their customers.

Now, it appears the EU is about to shake up the market once again. PSD2, set to be enforced in 2018, aims to extend the themes of PSD. With a customer's consent, PSD2 allows non-banks to access their account information and facilitate payments.

AISP: account information service provider
PISP: payment initiation service provider

These are the two new industries the directive is trying to foster. For AISPs, like Mint, PSD2 allows for secure access to a customer's account. And for PISPs, PSD2 shortens the value chain; PISPs will be able to make bank-account-to-bank-account payments—something previously reserved only for banks. To make this possible, however, banks need to alter their digital infrastructure to allow easier communication with third parties.

The directive will also require that all payments operators and banks comply with multi-factor authentication (MFA) to maintain high standards of security for anyone wanting to get into the payments game.

With these changes, it can be difficult to predict what kind of payment model will take market share, but there are already a few contenders. Instant payments, a model that allows for instant credit transfers, is already sweeping through much of Europe. There have also been a few commercially successful, bank-led initiatives such as MobilePay in Denmark and Vipps in Norway. Although some predictors are saying that alternative payment methods like instant payments may take some market share away from cash and card payments in the next five years, the 2017 World Payments Report stated that credit cards grew globally in 2015 by 10%, and debit cards accounted for the highest share (46.7%) that same year. In essence, the ramifications of PSD2 will more likely be a broadening of the payments industry, rather than one new solution usurping another. The whole purpose of PSD2 is to foster more competition and greater innovation in the payments space—not herd consumers into picking one option.

So, where is Verifone amidst all this opportunity? We've met our PSD2 requirements for the 2018 deadline and are currently assessing the options.

"History shows that if you want to get anywhere in payments, you need to get to scale, and in order to get to scale, you need the proper security, infrastructure, and resilience—all things Verifone has in abundance." says Burton. Verifone will continue to work on the foundation of coexistence for multiple payment models—allowing the customer the choice to pay however they'd like.

Verifone has always been an advocate for diversification and innovation in the payments space, and so, for us, PSD2 is more than welcomed. ∎

NON-CENTS

There Are No Canaries in the Digital Mine

The growing popularity of cryptocurrency has given birth to a new industry: digital mining. But not only is this costly and labor-intensive career doomed to eventually die, it's all one humongous gamble.

Mining cryptocurrency is a lot like mining gold. You need the right equipment. You need to dedicate weeks, months, even years of your life to it. Some ventures fail, and some make you richer than Scrooge McDuck.

But the biggest difference between mining for gold and mining for cryptocurrency is math. Take for example, Bitcoin—the industry leader in cryptocurrency. The process of "mining" for Bitcoin is really just solving a series of complex math problems that eventually produce a code—and that code is a new Bitcoin. However, the algorithm is constructed in such a way so that every time a Bitcoin is mined, the process of mining the next is more difficult.

Nevertheless, the value of Bitcoin is rising, and people everywhere are trying to get in on the digital gold rush. Miners set up garages, offices, and sometimes warehouses with an assortment of computers all programmed to solve the math that'll eventually produce a Bitcoin. One miner confessed that with the amount of equipment he needs, his electricity bills come to $80,000 a month, but he's able to produce 100 Bitcoins a day. At the time of writing, the value of 100 Bitcoins is over $390,000.

Still, Bitcoin, like most cryptocurrency, cannot be mined forever. Bitcoin is constructed in such a way that there can only ever be 21 million Bitcoins in existence. The mining industry will eventually collapse.

Ever since its creation in 2009 by the anonymous cryptographer known only as Satoshi Nakamoto, Bitcoin has rocked the payments industry to its foundation. But even with its high-priced value today, there are no indicators as to what will become of it after the mining industry collapses. It would make sense that the value would increase as we mine the last of the Bitcoins, but the wild fluctuations in cryptocurrency value, combined with the emergence of new currencies like Zcash and Ether, paint an unclear picture of Bitcoin's future.

Take for instance, Bitcoin Cash. This new cryptocurrency was a recent "fork" of Bitcoin and, overnight, it achieved a $12 billion valuation. One of the reasons for the new currency, ironically, was the popularity of Bitcoin. Bitcoin only allows a user to process one megabyte of transactions at a time and, with increasing upticks in active users, this process is becoming rather slow.

Iqbal Gandham, the U.K. Managing Director of the brokerage company eToro, said in a press statement, "For Bitcoin to continue to scale and have the potential to become a globally used currency, this slowdown in transactions has to be addressed."

Bitcoin Cash increased the transaction limit to eight megabytes. This has been a tremendous boon for the new currency, currently worth $450 per coin.

We do seem to be heading for a digital currency future. Cash is vulnerable to destruction, degradation, and theft in ways that cryptocurrencies simply never will be. When looking at global payment trends, nearly every country in the world is slowly moving away from cash-based economies. Cryptocurrency feels like the next logical step. But picking the one that will emerge as the global leader? That's much, much harder to predict. This makes miners look less like math geniuses and more like sophisticated gamblers.

And this gambling act involves all players. Creators of new cryptocurrencies need miners to produce more digital coins for circulation, and investors are banking on miners to help the currency appreciate in value. It may look promising now, but this system is inherently precarious.

Maybe one day, there will emerge a global standard cryptocurrency—one so strong, it's impervious to being overtaken by another. But until that day comes, it might be wise to hedge your bets.