Stronger Security and Mobile Payments - Dramatically Faster and Cheaper to Implement

Here is a simple, cost effective way to achieve transaction security for mobile payments that allows easy and secure provisioning of cards. Most importantly, it is compatible with existing retail POS systems and does not require retailers to make software or hardware changes.

A LoopPay White Paper by George Wallner

Fraud protection has always been a compromise: how much protection and at what cost? Many good solutions are never adopted because they either require too many changes or cost too much. Mobile Tokenization described in this paper adds substantial security at minimum cost because it does not require new equipment or software at the point of sale.

Magnetic stripe cards carry static data that can be easily copied and used time and again until their limit is reached or fraud is detected and the card cancelled.

Smart cards (such as EMV) contain a microchip that can "sign" transactions with cryptographically generated dynamic data based on a secret key stored in the card. Because the signature is cryptographically generated and is dynamic, smart cards are very effective against copy or replay fraud. The smart card concept has been adapted to contactless cards and mobile phones using NFC. The phones or UICC (SIM cards) are equipped with a Secure Element (SE), which is essentially a chip that can sign transactions in a similar fashion to a smart card.

This document describes a practical tokenization scheme that adds security to mobile transactions while remaining fully compatible with existing POS terminals and retailer systems. **Mobile Tokenization** is intended for card issuers who are looking for a flexible and easy method to add security to magnetic stripe cards as they move from the physical cards onto Loop's mobile LoopWallet and other virtual environments.

Security is always a compromise between protection and cost. A practical security system that gets adopted is better than a perfect one that stays on paper. Accordingly, **Mobile Tokenization** maintains compatibility with the existing retailer and acquirer infrastructure while providing good security at low cost.

While it is relatively easy to make and securely provision smart cards, mobile phones are much harder to securely provision and manage. That's because the card issuer cannot control them at any point in their lifecycle and also because the phones must support multiple cards belonging to different networks. Furthermore, the system requires a complex chain of "trusted" entities, hardware in phones, and a slow multi-step card provisioning process — all of

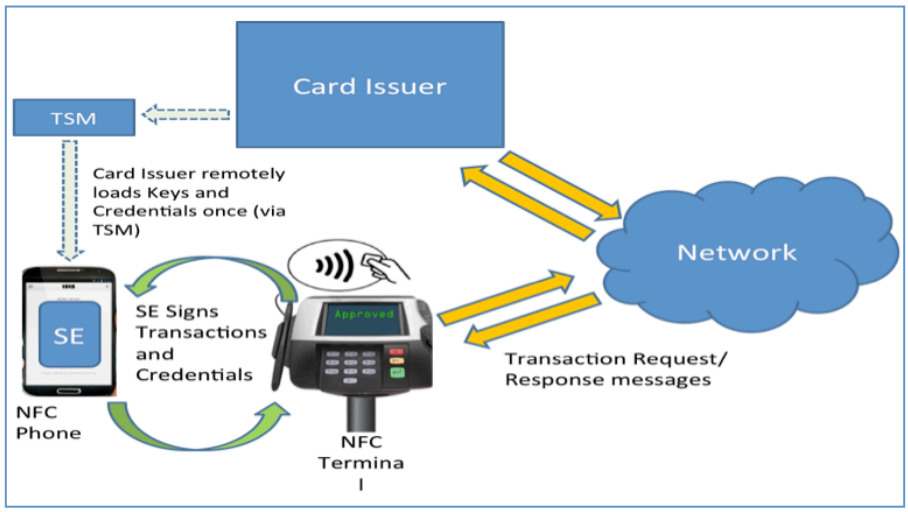

Figure 1: NFC Mobile Payments. The credentials and keys are provisioned into the SE of the smartphone. Once provisioned, the SE can sign any number of transactions (within some risk profile). The card issuer trusts the SE and accepts transactions and credentials signed by the SE.

which make widespread mobile payment adoption costly, complex and painful. If a card issuers wants to add another factor of authentication for more security, today the entire system would have to change from: NFC chip, to NFC certified POS terminal, to Acquirer back to the issuer.

Tokenization's Advantages and Constraints

Rather than empower the hardware (chip or phone) to sign transactions, tokenization is an alternative security technology that converts the traditional card data, including the Primary Account Number (PAN), into a token. The token is just a number, whose only function is to point to the original card data, which is stored in a secure host called the "Token Vault."

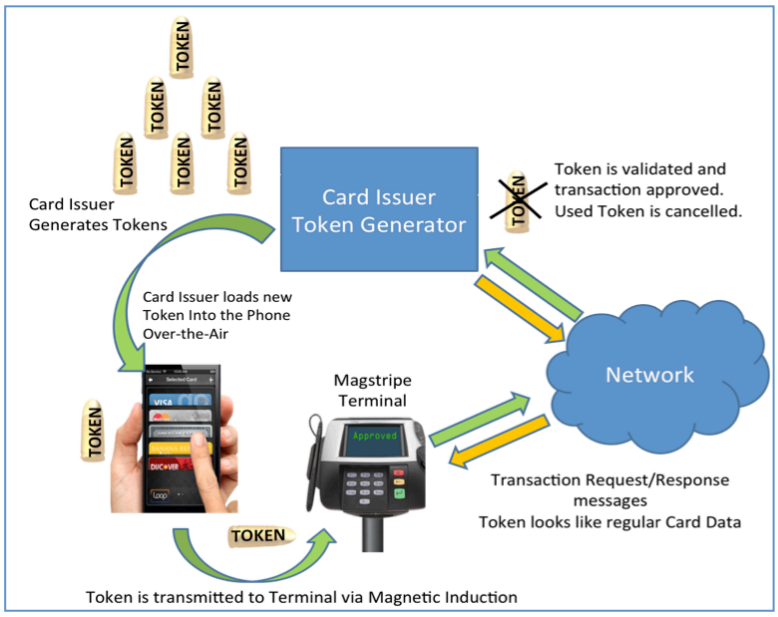

Figure 2: The Token Cycle

Protecting the PAN is one goal of tokenization. But unfortunately the PAN has become more than just an account identifier. Retailers, acquirers and cardholders all use the PAN for a variety of functions. The first six digits, (IIN or BIN) are used for routing. Some acquirers also use the first nine digits for routing. And the PAN is often used for refunds and dispute resolution. In addition, some retailers use the PAN to recognize frequent shoppers. Consumers use the PAN, or at least the part printed on receipts, to reconcile accounts (especially expense accounts).

In its classical form, tokenization obscures the entire PAN. Recent variations only tokenize part of the PAN, leaving the first six digits readable. They also rely on issuing new unique-BIN (IIN) PAN-s, so there is no chance that the randomized PAN coincides with an existing PAN. To be able to support all of this requires that retailers modify their systems to use the token instead of the card number (PAN) for various functions, including loyalty. But tokens change, which raises a number of issues. How, for example, would retailers match tokens with customers? Would the retailer have to refer to an outside organization that maintains the Token Vault to match a token with an account? Each time they see a token? What about consumers trying to reconcile receipts with statements?

The alternative is to leave the PAN un-obscured and only tokenize the rest of card data. Although this leaves some exposure, it ensures compatibility with existing retailer systems, acquirers and consumer behavior, while still adding substantial security. By not forcing retailers to change, a key barrier to adoption is eliminated.

Loop's Mobile Tokenization

Rather than empowering the phone (or its built-in Secure Element chip) to sign transactions, Mobile Tokenization relies on a central host to tokenize and distribute tokenized card data. This is possible because, unlike a smart card, a mobile phone is almost always connected to a communications network, which is the crucial game-changer that allows practical tokenization for these devices.

Compatibility with existing retail systems, meanwhile, is achieved by leaving the PAN (either fully or partially) readable. The Expiry and Service Code fields also remain readable. The rest of the card data, the Other Data and Discretionary Data fields, are replaced with a one-time token.

One-time mobile tokens can also be created by a secure microprocessor on various Loop enabled devices, like a dynamic CVV. The keys to create these one-time tokens can be sent to Loop devices via a central host provisioning and authentication server, hosted by the card issuer, or card processor/network. Just prior to transmission, the one-time token is created using the key plus sequence number, and even time stamped. Other authentication factors, from PIN to biometric, to location verification, can be added by the issuer without requiring merchant change. When the one-time token bundled with the track data is transmitted by the POS terminal via Loop's Magnetic Transmission, the package is delivered back to the issuer based on the PAN data, the issuer can then checks the PAN to see that it is a mobile tokenized card, if so, the issuer performs an authentication check on the one-time token, along with the other checks the issuer performs before it ultimately authorizes or declines the transaction.

Loop's Magnetic Transmission

The adoption of Mobile Tokenization is made practical by Loop's magnetic induction technology, which enables contactless POS transactions via existing POS terminals without requiring hardware or software changes. It can do this because it uses the ordinary magnetic stripe reader as the contactless data receiver. MST (magnetic secure transmission) formats the card data into simulated magnetic stripe tracks and transmits them via magnetic pulses, which can be read by existing terminals' magstripe reader. The contactless transfer distance is one to three inches (30 to 60 mm) and is extremely reliable.

MST essentially repurposes the ordinary magstripe readers for mobile payments so that mobile phones can make contactless card payments via the existing retail infrastructure — where the mobile phones use an internal MST transmitter or an external accessory.

***A simple analogy**: A smart card is like a gun that can make its own bullets. It can sign transactions on demand through its entire lifecycle (or until cancelled). This is awesome power that requires serious security. Hard to achieve in a mobile phone. In a tokenized environment bullets are made in a secure central host (this is called Host Card Emulation). Bullets (tokenized cards) are distributed to mobile phones on an as-needed basis. As the mobile phones do not know how to make bullets, the security burden on them is greatly reduced and the system-wide exposure of the card issuers becomes much smaller.*

And because the track data is simulated it doesn't have to be the original magstripe data; it can be dynamic tokenized card data. This offers an opportunity to replace magnetic stripe transactions with secure mobile transactions — all without the disruptive delays and the significant costs of retail system upgrades.

How Mobile Tokenization of Card Data Works

As stated earlier, retailers and acquirers need the Primary Account Number (PAN). Therefore Mobile Tokenization tokenizes only part of the card data, leaving the PAN, Expiry Date and the Service Code (SVC) readable. These are data fields that retailers and acquirers use. The rest of the card data, the Other Data and the Discretionary data, are tokenized.

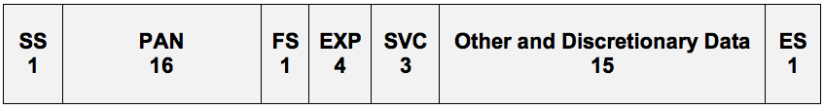

Figure 3: Typical Track 2 Data

The tokenized part of the card data that replaces the Other Data and Discretionary Data fields is called the Token Part. It consists of two data elements: the Token Part Value (TPV) and the Token Mode Indicator (TMI).

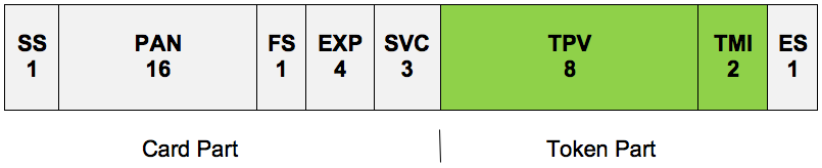

Figure 4: Tokenized Track 2 Card Data. The token replaces the data following the Service Code (SVC). The token consists of two parts: the Token Part Value and the Token Mode Indicator.

Because the Token Part Value is created through a cryptographic process whose key is secret, and because it includes dynamic data that changes with every new token, an attacker cannot predict what the next valid token should be. And because a token is valid for only one transaction, used tokens cannot be reused for fraud. Tokens are generated in a secure host environment and are encrypted and distributed to the mobile phones over the air. The Token Mode Indicator allows card issuers to identify tokenized cards, validate them and manage the tokens' lifecycles.

Creating the TPV

The Token Part Value is a cryptographically generated one-time token that is derived from the following data elements:

1. Card data elements: PAN, Expiry, SVC
2. Token Sequence Number
3. HASH, obtained from the Discretionary data and the Loop Account ID

PAN	EXP	SVC	TSN	HASH
16	4	3	4	9

Figure 5: The Token Part Value

The HASH includes the card's original discretionary data (which includes the CVV) to link the CVV to the token. It also includes the LoopWallet Account ID, which links the token to the users account. By linking the account and CVV together, tokens become specific to a card and an account.

The key used to generate the TPV is generated at the time the card is first provisioned and it is changed regularly afterwards. The HASH is also generated at the time of provisioning the card. Both are held in the database and later used for token verification.

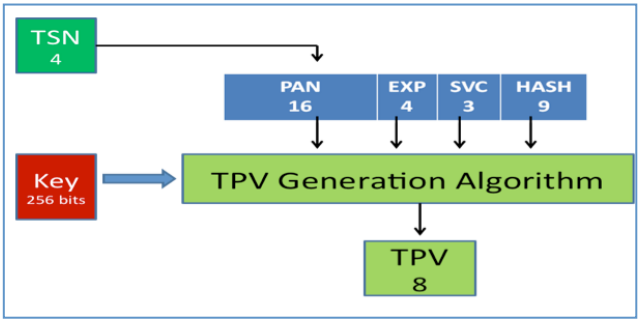

Figure 6: Generating the Token Part Value

The Token Sequence Number (TSN), which is one of the inputs to the token generation algorithm, is incremented each time a new token (TPV) is generated. Because of the new TSN value, and the encryption process that "randomizes" the output data, each new token will be very different than the previous one. The TSN therefore makes it impossible to predict the next valid token (TPV). Also, because a token is cancelled after it is used, a replay attack will also not work. It is expected that the issuer's system will change the key used to generate the TPV at least once before the TSN wraps around (i.e. reaches 9999). This means that tokens never repeat in a predictable fashion.

TPV Generation Algorithm

The algorithm is based on the public OATH One Time Password algorithm. The main difference versus OATH is that the inputs, which are derived from the card data and the account ID, comprise 128 bits while the extracted TPV is 8 digits.

By including the HASH, the TPV algorithm incorporates into the token value the card's original discretionary data and the LoopWallet user's Account number. This process adds an additional layer of security, which ensures that a token is both invalid for a different card, but also invalid when someone attempts to use the same card from a different account using the same issuer key. An attacker would not only have to know the

Is the magnetic stripe obsolete?

Yes, it is obsolete for financial transactions that don't require a PIN. The problem is the card: it is static and its data can be copied. Cards with a PIN, or retailer cards with low financial value — mostly cards where the cost of adding a chip is prohibitive — will continue using the magnetic stripe for a long time. In any case, the problem is with the card, not the reader. The card is static. The reader can read dynamic information and therefore it is possible to have good security via the magstripe reader. It is just an interface. The card is obsolete; the reader is not.

issuer key but also the LoopWallet user's Account Number, which is never visible outside the card issuer's authentication server due to the HASH generation process.

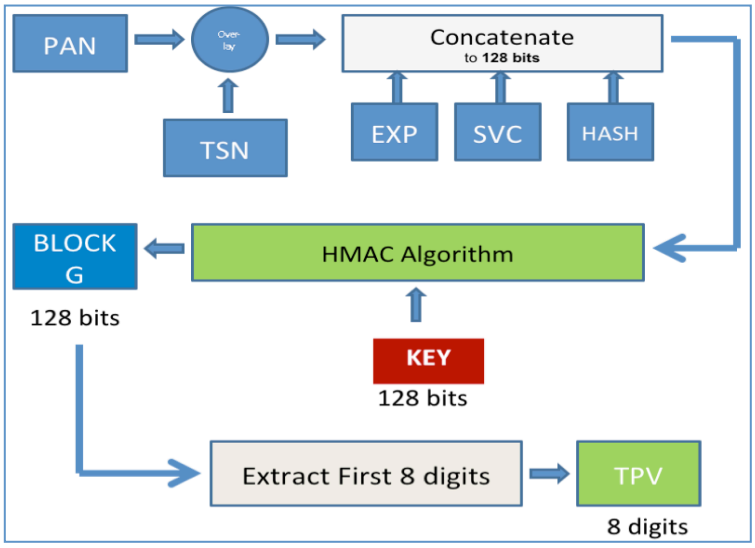

Figure 7: The TPV Algorithm

In Conclusion

Mobile Tokenization is a simple technology that offers an easy and cost effective way to improve card payment security without the need for the retailer to change his system. The technology provides greater end-user convenience when enabling mobile devices for payments, liberating consumers from plastic cards while also giving merchants the data they need to orchestrate effective customer engagement. Loop's Mobile Tokenization works with today's retail payment infrastructure and will work tomorrow with future infrastructures that comply with the EMVCO Tokenization Framework standard.

As this trend toward mobile payments gains momentum, retailers want two things: greater security plus a way to minimize large-scale infrastructure investment. Mobile Tokenization addresses both needs simultaneously.

About George Wallner | Inventor of the Modern POS Terminal

George Wallner's plan to transform payments as we know it was hatched in his kitchen. The year was 1978 and he and his brother Paul, both engineers, had been tinkering with a few ideas focused on developing large telephone systems and data collection networks. The Wallner brothers recognized that merchants needed a way to expedite consumer payments at the point of sale using the magstripe cards. And the company that they formed, Hypercom, was the first ever to enable the electronic payments that are the bedrock of the modern payments industry.

Hypercom grew into a global provider of POS terminals and support networks. George served in various roles there, including CEO, Chairman and Chief Technologist, taking the company public in 1997.

In 2006, Wallner went on to invest in ROAM Data, a leading vendor of mobile card acceptance equipment and software that was later acquired by Ingenico in early 2013. His latest venture, LoopPay, really comes full circle. It has developed a practical mobile payment solution that enables smartphones to be used for card present payments at the point of sale without requiring merchants to install any new hardware or software – leveraging the technology standard that powered the point of sale terminals he invented some two decades before.

About Loop

Loop invented the world's first mobile wallet app that allows consumers to securely store all their cards and pay with their Loop-enabled devices (accessories, smartphones, smart watches) virtually everywhere. The LoopWallet app reduces the clutter of plastic cards (payment, gift, loyalty, ID, membership cards) allowing consumers to leave their plastic behind with confidence. Based in Boston, MA, Loop's patented Magnetic Secure Transmission (MST) technology turns existing mag stripe readers into mobile contactless readers without any change or cost by the merchants or their payment processors. Loop provides not only breakthrough convenience for consumers to organize and pay with mobile devices, but also with the highest level of payment security to protect consumer card data. Loop is a Level One PCI Certified Payment Provider. To learn more and order Loop products, visit www.looppay.com

.

For further information:

Email: info@looppay.com
Web: www.looppay.com/contact-us