Euronet Software Solutions
A Division of Euronet Worldwide
Powerful Payment Solutions that Bring Currency to Life

A Euronet Software Solutions White Paper

Apple Pay and Tokenization

Background and Overview

By Stephen Butcher
Euronet Software Solutions
Product Manager
Cards and Networks

November 2014

Euronet Software Solutions
17300 Chenal Parkway, Suite 200
Little Rock, AR, 72223

Tel: 1-501-218-7300
Fax: 1-501-218-7302

E-mail us at: euronetsoftwaresolutions@eeft.com
Visit our Web site at www.euronetsoftware.com

Euronet Worldwide Inc.
Corporate Headquarters
4601 College Boulevard, Suite 300
Leawood, Kansas 6621

Executive Summary

No doubt if you are in the payment space you have been inundated with all of the news about Apple Pay and tokenization as well as how the payment landscape is changing. This paper will provide some clarity and background behind this topic as well as a general timeline and a high level overview.

Timeline of Events

The international payment networks – Visa, MasterCard, etc., were probably working with or aware of Apple Pay all of this time but were sworn to secrecy until Apple's launch. In hindsight, this secrecy might have been the reason a clear business case or explanation of the problem payment tokenization was solving could never really be given.

Payment tokenization leverages many of the EMV data elements. Because of this, both Visa and MasterCard introduced a lightweight option much like the 'on behalf of' EMV service where the network handled the EMV data for issuers who were not ready to make the EMV software changes.

At the same time payment tokenization was being announced, Host Card Emulation (HCE) was also being revealed. HCE is intended to remove the dependence on the mobile operator for mobile payments. This can be accomplished because the Secure Element in the phone is no longer needed and the card credentials can be stored in the cloud and downloaded to phone via a phone app from the issuer bank.

Android phones (Kit Kat O/s) followed the HCE process with Visa and MasterCard offering services to manage the HCE vaults in the cloud. At this point, Apple had not yet announced Apple Pay or the NFC iPhone6.

On September 9, 2014, Apple announced the iPhone6, iPhone6 plus and Apple Pay. Visa announced their payment token service on the same day. Unlike the Android and HCE approach, the NFC iPhone6 uses the secure element and touts the Passbook functionality of the phone to enable payments using the Apple Pay phone application. Another important point here is that Apple, and not the mobile operator, owns the secure element.

OCTOBER 1, 2013

Visa, MasterCard, American Express and Discover announce an initiative to establish a tokenization standard.

OCTOBER 22, 2013

A working group is established by EMVCo to define the following:

- New form factors at POS
- End to end payment integrity
- Secure payment credentials
- Interoperable standard based on 3rd party enablement

FEBRUARY 2014

Information about Visa and MasterCard payment tokenization appears in industry publications.

MARCH 2014

EMVCo standards are published.

- It is thought that the Target breach was a catalyst
- Payment tokenization is not a replacement for PCI

APRIL 2014

Visa and MasterCard mandates acceptance of payment token information in the United States. Existing data elements were reused so the changes were not seen as onerous to software vendors.

SEPTEMBER 9, 2014

Apple announces iPhone 6, iPhone6 plus and Apple Pay. Visa announces its payment token service.

OCTOBER 20, 2014

Apple launches Apple Pay.

Apple Pay went live on October 20th 2014. As of mid-November, the latest statistics report that more than 500 banks and over 220,000 merchants have signed up for Apple Pay. Additionally, in the first 72 hours, over one million cards were registered. These numbers represent roll-out in the United States only. Apple decides the roll-out strategy with regard to Apple Pay and it seems to be directly related to where the iPhone6 sales are occurring. The international payment networks are no doubt preparing their global payment tokenization roll-out, now synonymous to Apple Pay for all intents and purposes.

One probably less emphasized consequence of the phenomenal roll-out of Apple Pay and payment tokenization is that once the card token/credentials have been downloaded to the phone from the cloud, payments performed are really just contactless payments. In reality, Apple Pay can be used anywhere globally to perform payments without additional action from merchants that support contactless payments other than to send the mandated indicators that the payment was contactless.

As the way payments are made continues to evolve, payment tokenization, EMV and PCI standards are intended to be leveraged for NFC, QR, BLE (Bluetooth Low Energy) and Geofencing payment solutions.

Payment Tokenization

- Tokenization is the replacement of the card PAN with an alternative card number in this case in the mobile device.
- Digitization or provisioning is the loading and personalization of card details into mobile devices and onto servers.
- The token, not the card number, is used for online payments. The token:
  - Is 13 – 19 characters long
  - Has an expiration date
  - Starts with a BIN (for routing purposes)
  - Has its own POS entry mode
  - Is bound, mapped and affiliated with PAN
- The token is distinct and identifiable in payment systems. Separate BINS or BIN ranges may be used for provisioning tokens. There will be a one-to-one relationship between the card BIN/product and the card's payment token.
- The token is compatible with existing payment standards for web, NFC, POS, etc.
- The token can be static or dynamic but mainly static due to the use of actual BINs.
- The token supports USA regulatory routing (Durbin).
- One PAN can have multiple tokens; a recent use case mentions as many as 100 tokens.
- The token can be restricted to certain channels or domains.
- The token is requested by and specific to individual merchants. For example, Netflix, Walmart and Target might each have individual tokens for the same PAN.

- If a merchant is compromised, the token – not the card number – is compromised. Therefore, depending on the type of compromise, there may not be a need to issue a new card but instead just provision a new token.

Additional Token information

- Data elements being added to the payment message:
  - Token requestor id
  - Token cryptogram similar to EMV and contactless cryptograms
  - Assurance level
  - Assurance data
  - Requestor indicator
  - ID&V – Identification and verification – how to know the right person is requesting the token
  - Network or issuer risk analysis
  - Token domain restriction – who can use the token – token per merchant

Targeted Payment Types

Payment tokenization targets certain types of payments and reduces, but does not replace, the need for a plastic card. Some of the payments suitable for payment tokenization are as follows:

- NFC
- Card not present (CNP)
- Recurring or card on file
- Mobile and online payments

Token Service Provider and Token Requestor

Payment tokenization has introduced two new roles in the payment space – Token Service Provider and Token Requestor. While the role of Token Service Provider is open to any party that can be assigned a BIN, the international payment networks dictate the specifications and own the payment landscape. As a result, the international payment networks are naturally emerging as the dominant Token Service Providers.

- The Token Service Provider
  - Any institution that can get a BIN
  - Must be certified by the international payment networks (Visa or MasterCard)
  - Has the token to PAN vault
  - Provides the token to the token requestor
- The Token Requestor
  - Can be a merchant or cardholder
  - Has card number(s) that need to be replaced by a token

  - Replaces card number storage with storage of the token
  - The token requestor must be registered with the Token Service Provider as a token can only be used by its requestor

- APIs available between service provider and requestor
- The token vault can be maintained at Network or issuer

Token Provisioning

Token provisioning is the process by which the token is provided to the Token Requestor by the Token Service Provider and stored into the Token Requestor's system or device.

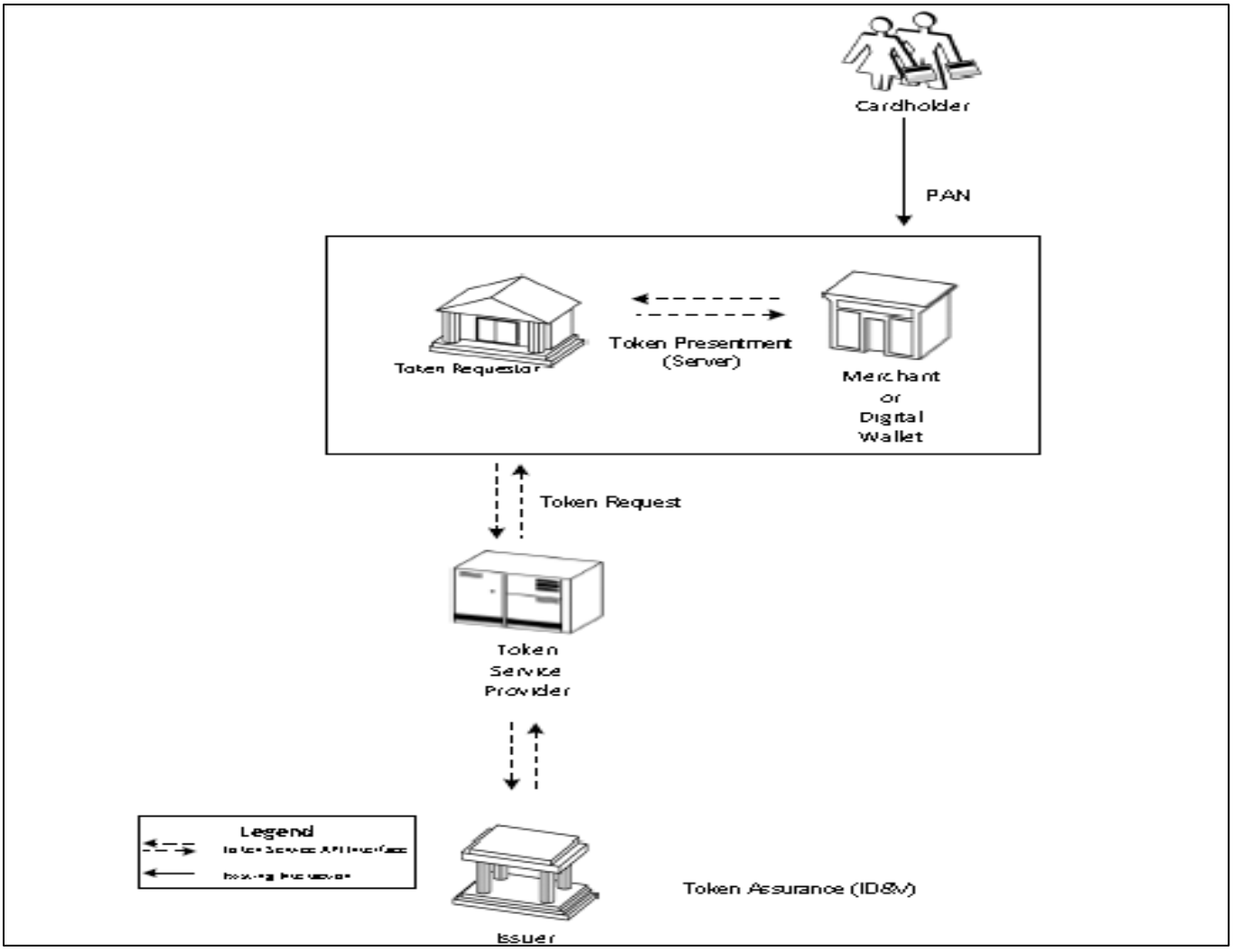

**Image courtesy EMVCo tokenization standards documentation.*

Transaction Using Payment Token

The diagram below illustrates a tokenized transaction showing the role of the Token Service Provider in the message flow. The Token Service Provider can also be the Payment Network.

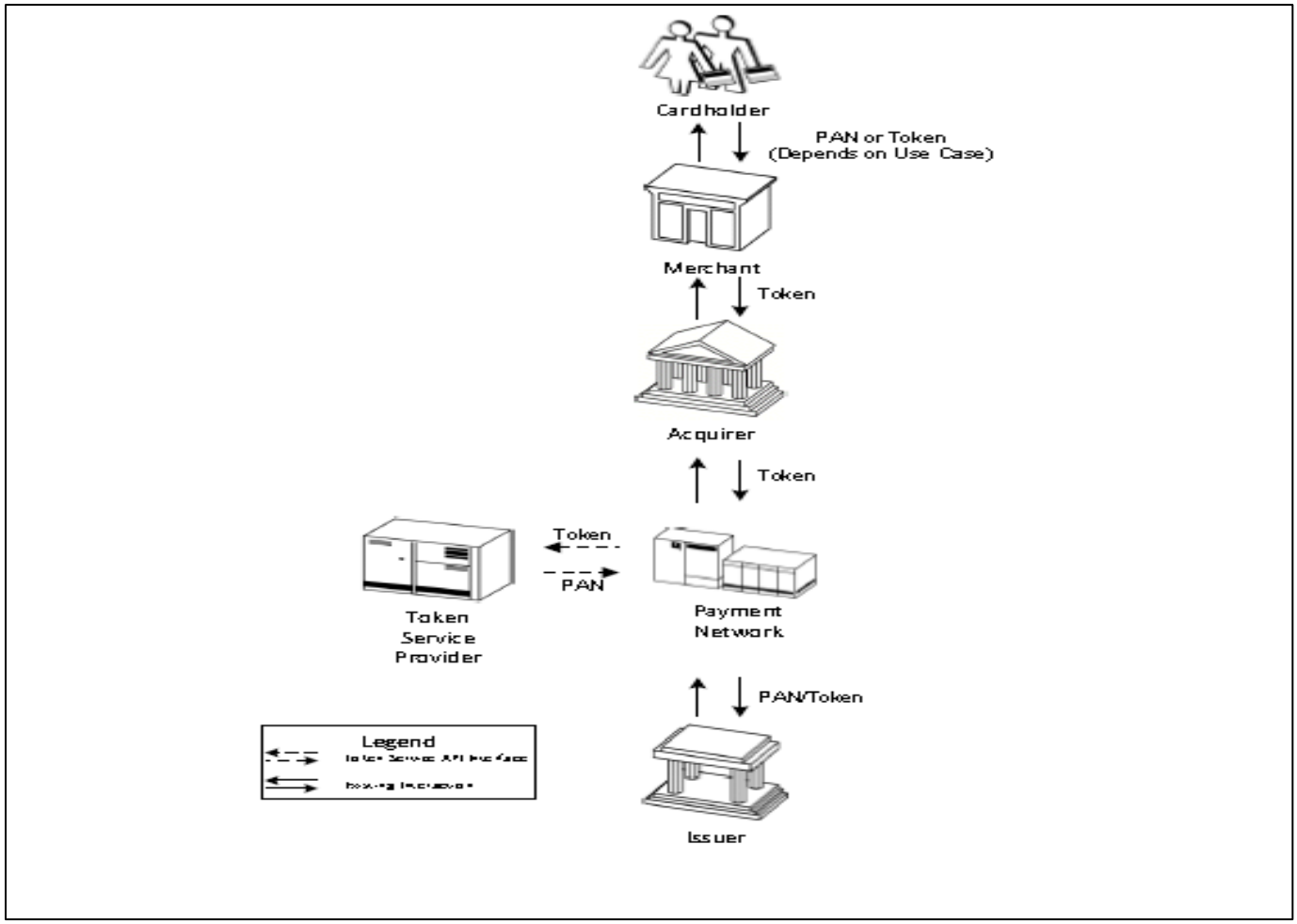

**Image courtesy EMVCo tokenization standards documentation.*

Conclusion

Not often has there been an introduction in payments that is both secure and trendy. This hopefully will be the story of tokenization and Apple Pay. The tremendous brand recognition of Apple is no doubt helping the adoption of token processing, and Apple Pay is making financial transactions more secure by removing the card number. Rivalled only by Apple product sales, the adoption of Apple Pay and by extension the use of payment tokens are truly proving to be a welcomed disruption. Stay tuned for the next chapter… wearable technology. Did someone say Apple Watch?

About Euronet

Euronet Software Solutions, a division of Euronet Worldwide, is recognized as a leading provider of software that powers electronic payment and transaction delivery systems around the world. Our solutions have reliably served the worldwide cards, payments and financial services markets since 1975.

Ensuring quick time-to-market and delivering a quality experience, we enable our clients to provide secure electronic payment convenience to millions of people around the world. Whether your organization is a bank or a provider of processing services to financial services organizations, our proven solutions will support your critical business needs now and in the future.

We provide a fully integrated suite of solutions for issuing, acquiring, self-service, e-banking and card scheme connections. Utilizing our services-oriented payments hub architecture, our software offerings are designed to increase your revenue, reduce your expenses, improve your security and increase the value of your customer relationships.

For more information:

- **Visit us online at www.euronetsoftware.com**
- **Contact your Euronet sales representative**
- **Email us at euronetsoftwaresolutions@eeft.com**