Apple pay - What do we know?

UL's independent assessment

Apple Pay - What do we know?

On September 9, Apple announced Apple Pay as their mobile payment solution. In this paper, we will describe what we know about Apple Pay in both technical and organizational context, as well as what questions still remain to be answered. As independent experts, our goal is to provide insight and knowledge that UL has gathered, in order to best inform all stakeholders involved.

Technology

Apple Pay is based on NFC technology for proximity payments and an embedded Secure Element in the iPhone and Apple Watch. Apple Pay uses industry-standard EMV contactless protocols over NFC (and MSD – Magnetic Stripe Data - contactless for backward compatibility for the US market). This makes it compatible with a wide range of contactless payment terminals in deployment today.

Apple Pay is compliant to the EMVCo tokenization framework and works with a tokenized PAN (Device Account Number) and Cryptogram (transaction specific dynamic security code). Apple only uses the token services from payment schemes (currently only Visa Token Service, MasterCard Digital Enablement Services and American Express Tokenization Service).

Security

The iPhone 6 and Apple Watch use an embedded Secure Element to store information for payment. On the iPhone the Secure Element contains the fingerprint information for TouchID authentication. It is unclear if the Secure Enclave used in the iPhone 5S, is also available in the iPhone 6. We assume that the fingerprint data is stored in the Secure Element on the iPhone 6.

Apple does not store card holder information and account numbers (PAN) on the iPhone. Instead of actual debit and credit card information, a unique Device Account Number (tokenized PAN) for each card is assigned, encrypted and stored in the Secure Element. These Device Account Numbers are only stored in the Secure Element of the iPhone and the token service. Not on Apple servers.

When making a purchase, the Device Account Number alongside a transaction-specific dynamic security code is used to securely process the payment. So the actual credit or debit card numbers are never shared with merchants or transmitted with payment. The focus of Apple is on the security aspects of payment.

Privacy

Apple is putting the focus on privacy. Because the iPhone (and Apple Watch) does not contain actual debit and credit card information, the merchant only receives a tokenized PAN. As part of the transaction, the Secure Element receives payment confirmation. This information is used to store recent purchases in Passbook.

There are no indications that the Device Account Number (tokenized PAN) is used to generate a dynamic PAN for each transaction.

If the iPhone sends the Device Account Number with each transaction, the device could be recognized because the same tokenized PAN is used for each transaction and allows merchants to link a device to multiple transactions.

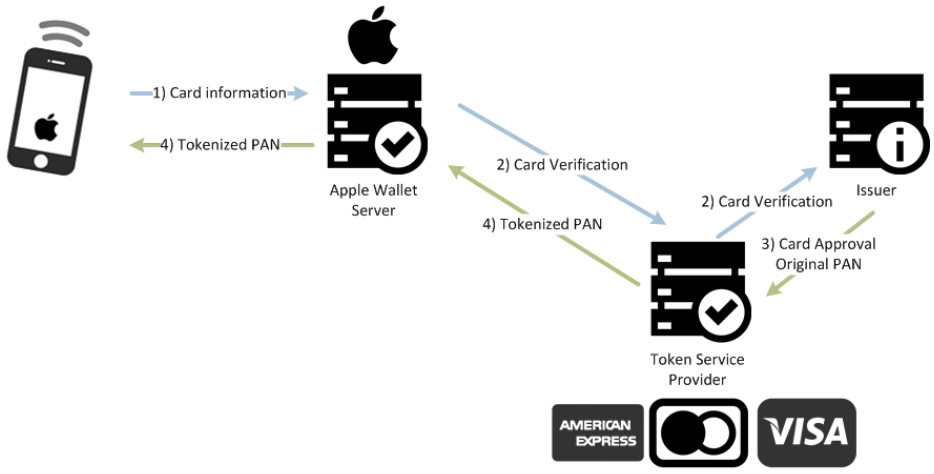
Apple Watch

The Apple Watch was also announced on 9 September and is expected to be available early 2015. Specifications of the watch are limited but Apple announced that Apple Pay can be used through the watch. The Apple Watch will have NFC and an embedded Secure Element to store payment information. Current information is that payment with the Apple Watch will be authorized with a PIN code and as long as you wear the watch (skin contact monitored by sensors), you can make payments. Once you take off the watch, the PIN code has to be entered again.

The Apple Watch makes Apple Pay for remote payments available on the iPhone 5 series (5, 5C and 5S). As the iPhone 5 series do not have a Secure Element, the Secure Element of the Apple Watch is used via a Bluetooth connection to make remote payments.

Enrollment

To add payment cards to Apple Pay (Passbook), the card holder can link the card information from the iTunes account or take a picture of the card with the camera of the iPhone. The information on the card is verified by Apple with the relevant scheme and the card issuer. After verification, the token service of the scheme will send the Device Account Number (tokenized PAN) to wallet server of Apple which will store the tokenized PAN on the Secure Element in the iPhone.



It is yet unknown what role the issuers will play in the enrollment of payment cards. Will an activation code be needed; or is a $0 transaction be sufficient; or is there a need for a CVC2 validation? Also indications are that in the future 3D SecureCode could be used by Apple to support enrollment.

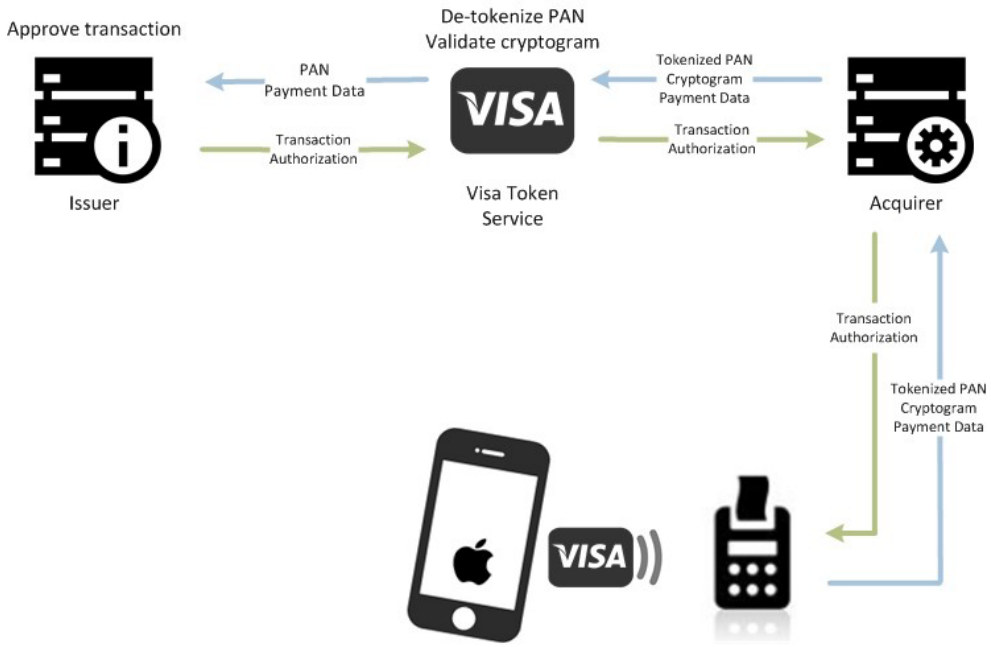
Proximity Payment iPhone

To make an NFC payment, the card holder taps the iPhone against the terminal and authorizes payment with a fingerprint (TouchID). The Secure Element contains the payment application and is triggered to send, among others, the Device Account Number (tokenized PAN) and a generated transaction specific dynamic security code (cryptogram) to the merchant (terminal).

The tokenized PAN and cryptogram are sent into the acquiring network for processing. The Token Service of the scheme will de-tokenize the PAN to convert to the original PAN. The scheme will validate the cryptogram and send the transaction with original PAN to the issuer (e.g. bank) for approval.

Other questions that are not (yet) answered are:

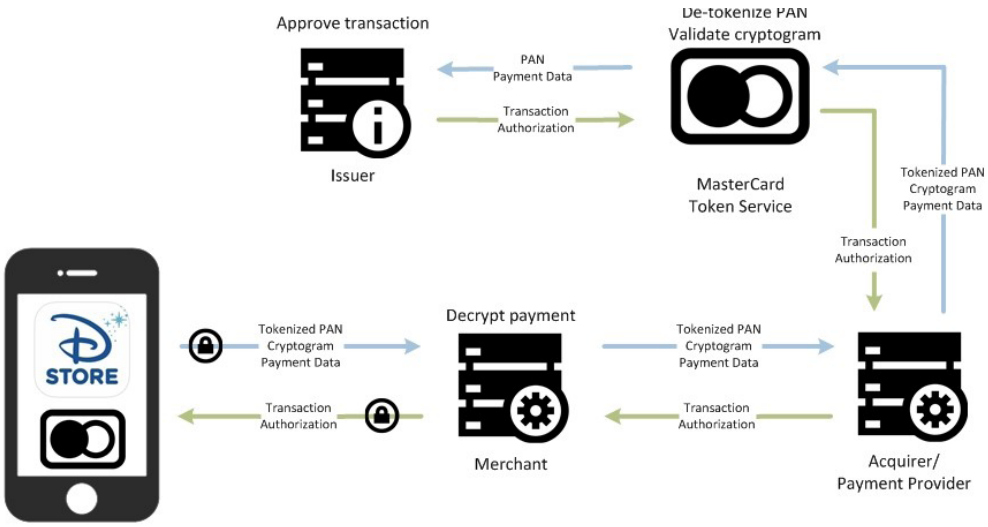
- Does Apple Pay allow offline transactions and how are offline counters implemented?
- Does Apple Pay make a difference between low value payments and high value payments?
- Are the payment applications from the scheme preloaded into the Secure Element?

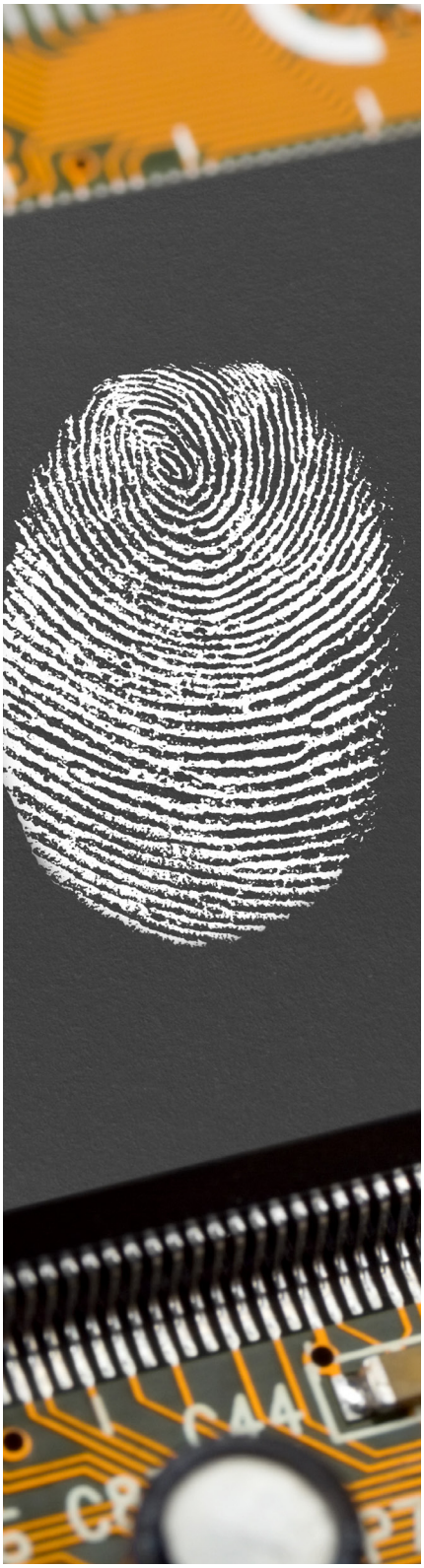


Remote Payments iPhone

Apple Pay also supports remote payments.
Merchants can develop apps that use Apple Pay to pay for online transactions. The app must use the Apple Pay API to allow the use of this payment method.

The card holder collects items in a shopping cart in the merchant app on the iPhone. When the customer is ready to pay, checkout will be with the Apple Pay option. The card holder authorizes the payment with TouchID and the Device Account Number and dynamic security code are sent to the acquirer/payment gateway. The acquirer/payment gateway forwards the tokens to the Token Service for de-tokenization and validating the cryptogram. The de-tokenized PAN and the cryptogram are sent to the issuer for payment approval. The issuer approves the transaction and payment is complete.





Based on current information, Apple Pay appears to make a remote payment into a Card Present payment instead of the Card Not Present payments that normally are used for remote payments. This reduces the risk for the merchant and could result in lower transaction fees for the merchant.

Ecosystem

The Apple Pay ecosystem is built upon the four corner model as known in the payment industry. The schemes MasterCard, Visa and American Express, have made agreements with Apple (iOS 8 source code analysis showed references to UnionPay as well). In the agreements with the payment schemes, Apple managed to negotiate a reduced rate for payments in the Apple Store and iTunes Store to 25 basis point (from 40 basis points), saving Apple around $ 27 million in payment costs.

On top of that Apple made agreements with large issuers such as Citi, Bank of America, Capitol One, Wells Fargo and Chase (for now only in the US) and more banks are lined up to join. In the agreements with issuers, Apple has negotiated a fee of 0,15% of the transaction value for every Apple Pay transaction. Only Passbook has access to the Secure Element, so banks will not be able to use their own wallet application. In the agreement between Apple and the banks, Apple requires banks to allow TouchID to be used.

With Apple Pay the use of TouchID is mandatory to perform a purchase. TouchID replaces the card PIN as Card Holder Verification Method (CVM) when using Apple Pay. The issuer receives a confirmation that an on-device CVM was performed. With Apple Pay the on-device CVM is the TouchID instead of mPIN used in other mobile payment solutions.

To accept in-store Apple Pay transactions, merchants must have NFC enabled payment terminals. A number of large merchants in the US have installed NFC enabled terminals to support Apple Pay proximity payments. What Apple can deliver is a consistent user experience for payment on iPhones – mobile operators and banks were not prepared to create this and wanted to compete with each other.

And what about the Mobile Network Operators? Apple Pay has no dependency on MNOs. The role for the MNO seems to be minimal in the Apple Pay ecosystem.

The business model of Apple is to sell hardware, more specific iOS devices. Apple Pay allows Apple to sell more iPhones and Apple Watches. However new revenue stream cannot be ignored. The expectation is that in October, Apple will announce new iPad devices with TouchID allowing the iPad to use Apple Pay for online payments. Selling more iOS devices, will also generate revenue through iTunes Store in music, movies and applications (Apple earns 30% from every purchase via iTunes).

Conclusion

Apple Pay looks promising for mobile payments. Apple is positioning itself as a trusted partner. The focus is on security and privacy. Apple facilitates mobile and remote payments but is not interested in the data gathering and processing that other companies see as a benefit from mobile payments. The choice of Apple for NFC makes it clear that NFC is the standard communication technology between handset and payment terminal.

Apple Pay still must prove itself and a lot of details about how Apple Pay works are still unknown. As an independent expert, UL's Transaction Security division will keep investigating new payment solutions such as Apple Pay to make sure that the payment solution fits the demands of our customers.

ABOUT US

For more than a century, UL has been one of the most recognized and trusted resources for advancing safety. Its Transaction Security division guides companies within the mobile, payments and transit domains through the complex world of electronic transactions.

UL is the global leader in safeguarding security, compliance and global interoperability. Offering advice, test and certification services, security evaluations and test tools, during the full life cycle of your product development process or the implementation of new technologies.

UL's people pro-actively collaborate with industry players to define robust standards and policies. Bringing global expertise to your local needs. UL has accreditations from industry bodies including Visa, MasterCard, Discover, JCB, American Express, EMVCo, PCI, GCF, ETSI, GSMA, GlobalPlatform, NFC Forum and many others.

CONTACT US: WWW.UL-TS.COM / INFO@UL-TS.COM

SAFEGUARDING
SECURITY,
COMPLIANCE
AND **GLOBAL**
INTEROPERABILITY