CORE®

TOKENIZATION

Basic Technology of Digital Payments

Branko Milanovic
Fabian Meyer

15. March 2016
COREtechmonitor | Blogpost

Key Facts

- Technology providers predict strong growth of payments with mobile terminal devices at point of sale (POS)
- Tokenization is basic technology for increasing security and data protection when processing mobile payments at point of sale
- Tokenization replaces sensitive payment data (PAN, expiration date) with non-sensitive surrogates, i.e. tokens, coupled to specific transactions
- In cooperation with international schemes, global technology providers establish network tokenization based on EMVCo-defined technical standards
- European issuers will implement tokenization technology for maintaining future responsiveness

Report

Since October 2014, payment service Apple Pay can be used in combination with credit and debit cards of a partner bank in the USA. Additional markets, such as the UK, Canada and Australia successively followed. Following market entry in China during February 2016, the payment service has now been successfully established in five countries. The fact that during market launch in China, more than 40 million cards were activated within the first 48 hours is one indication of its increasing relevance. This quick adaptation rate indicates great potential. It is therefore safe to assume that the trend towards digital payment will continue.

The global transaction volume with mobile Wallets at the point of sale (POS) will total approx. 75 billion USD in 2016. Studies predict a growth to 745 billion until 2020. This would correspond to an annual growth rate (CAGR) of close to 78%. In addition to Apple, other global technology providers such as Samsung or Google, with their payment methods Samsung Pay and/or Android Pay play an important role with regard to this development. The basic technology of these three providers as well as other innovative payment solutions is called tokenization.

Tokenization describes the substitution of sensitive data with non-sensitive equivalents, the tokens. With regard to mobile payments, this means concretely replacing the debit or credit card numbers (primary account number) against a token. This token has the same format as the underlying card (i.e. 16 digits for credit cards and the respective analog card information for debit cards) but is linked to a specific device (smartphone, tablet, wearable). It has a separate expiration date. The token service provider ensures the mapping between PAN and token, as well as the integrity of the token.

Technical framework conditions for tokenization are defined by EMVCo, an organization whose members include the major credit card providers American Express, Discover, JCB, MasterCard, UnionPay and Visa.

When carefully observing market, it becomes evident that the major technology providers increasingly establish network tokenization as new standard, in close cooperation with international schemes. Network tokenization requires a new interface from issuer to tokenization service provider in order to enable initial issuer authorization of token while ve

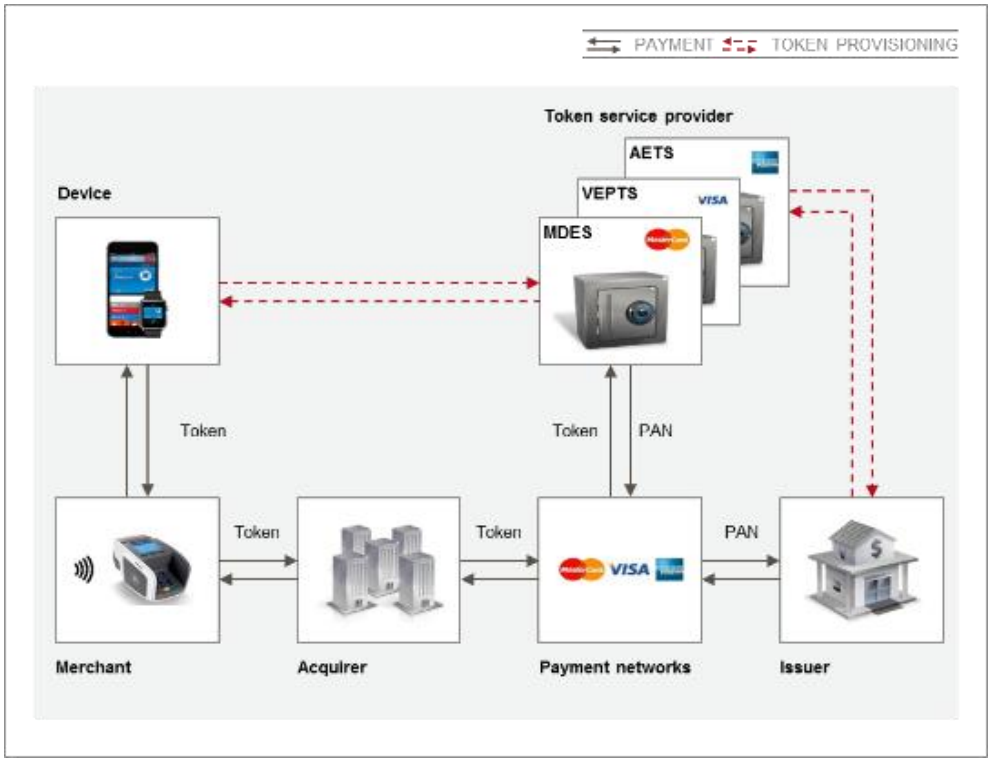

Fig 1: Tokenization provisioning required interface from issuer to tokenization service provider

rifying customers. As illustrated above, an active token is placed on the mobile terminal device and a customer can use the device to make a wireless payment at the point of sale. The successful registration and authorization of the user by the issuer serves as basic prerequisite. From customer perspective, the customer experience is at least analog to an NFC (near field communication) credit card payment but can be augmented with additional services.

The mapping between PAN and token is placed in a secured token vault to which only the tokenization service provider has access. During the payment process and prior to the authorization request with the issuer, the token service provider re-substitutes the token with the PAN in the payment network. For identifying a digital payment, the issuer receives in the authorization request both, the token and the underlying card information. This process avoids providing the merchant or the acquirer with additional personal information about the customer's credit card.

The basic requirement for the issuer to participate in the ecosystem is the integration with a tokenization service provider, which forms a new entity in the overall system. Tokenization service providers can generally be the schemes themselves, such as e.g. MasterCard Digital Enablement Services (MDES) or Visa Europe Payment Token Service (VEPTS), third parties such as First Data or even the issuers themselves. The decision whether to use an existing service or establish a separate solution depends on individual factors and should be decided based on situational factors. Throughout, a distinction between Secure Element (e.g. Apple Pay) or cloud-based (e.g. Samsung Pay, Android Pay) transactions continues to be relevant. If the latter case applies, an additional party, the so-called HCE (Host Card Emulation) provider is necessary.

A significant advantage of network tokenization consists in the fact that the payment infrastructure doesn't require merchant and/or acquirer adjustments and all existing interfaces continue to be active. The payments occur via the same communication channels as before, the sole difference being that instead of credit card data, only token details are transmitted.

Furthermore, tokenization technology increases mobile payment security. This is so because of increased data transmission security and thanks to decreased merchant responsibility. Sensitive payment data no longer require storage with the merchant and will no longer be transferred during the transaction. Instead, the exchanged data are coupled to a device, a merchant or even a transaction before expiring completely in case a data contamination has taken place. The card owner's data are therefore significantly more secure.

This enables numerous new and secure application possibilities such as Apple Pay, Samsung Pay, Android Pay or various Wallet solutions.

One important benefit also consists in the integration capabilities of revenue-increasing measures into the digital business process. Sales promotions or cash-back campaigns can for example be communicated to the customer directly via the Wallet. Additional services and loyalty programs can also be added for digital cards in order to enable a comprehensive and comfortable shopping experience to customers.

Various European issuers have already started projects for readying their systems for tokenization. They successively add new application cases. The timely integration of this technology forms the basis of the ability to act in the future. It is therefore considered an essential step toward digital payments. The noticed trend toward accepting mobile Wallet solutions justifies the necessity for swift action.

Sources

Dan Schatt: Virtual Banking: A Guide to Innovation and Partnering, Wiley, 2014, pages 27-29

EMVCo: Technical Framework. Payment Tokenisation Specification, 2014, pages 22-27

Slava Gomzin: Hacking Point of Sale. Payment Application Secrets, Threats, and Solutions, Wiley, 2014, pages 83-85

Statista: Digital Market Outlook found under

https://www.statista.com/outlook/331/100/mobile-wallet-pos-payments/worldwide

Heise: China_-_Start: Apple Pay Overrun by Users

http://www.heise.de/mac-and-i/meldung/China-Start-Apple-Pay-von-Nutzern-ueberrannt-3113246.html

Branko Milanovic is Transformation Associate at CORE. He studied industrial engineering at the priv. FH Nordakademie, Elmshorn. and completed his dual studies with a Bachelor of Science degree. With CORE Branko is mainly active in the innovative field of mobile payments. As an expert for the basic technology Tokenization he accompanies the implementation of the technical basis for mobile wallet use cases.

Mail: branko.milanovic@coretransform.com

Fabian Meyer is Transformation Director at CORE. He obtained a Master of Science in Business Administration at the School of Management and Technology and gained experience as a business consultant and entrepreneur. At CORE, Fabian supports clients in implementing complex IT projects. In addition, he attends to the optimization of our internal ERP processes.

Mail: fabian.meyer@coretransform.com