tieto

Tokenization: Safety and Power Capabilities

Mobile payment solutions and their security, tokens and tokenization are among the hottest trends in the payments industry. The FUETE magazine asked Raivis Joksts, the senior offering manager at Tieto Retail Payments and Cards, to participate in a discussion on the topic of tokenization

– Nowadays, a lot is said and written about tokenization. Why is it a trending topic?

– The bottom line is that in the payment card industry tokenization helps to hide a card number from the fraudulent attacks and keep it hidden, thus contributing to the developement of secure card-based electronic payments in such areas of e-commerce and mobile payments where the vulnerability is higher.

– How does tokenization work?

– Tokenization is the process of substituting a value which is considered secret and confidential, in this case, a payment card number, with another value, referred to as a token, which is used instead of the original data, in our case – instead of the real card number. Such a replaced data element has no value without a context.

Tokenization has gained wide popularity after the scandalous data breaches on major e-commerce sites in the United States, when hackers broke into the database and stole card numbers of regular customers of these online stores. Now, if those e-stores did not store the payment card numbers but rather some values linked to those cards, then such a breach would not have caused such a disaster, because a token value by itself cannot be used by a third party to initialize a transaction.

Whereas, an online store can easily initiate a transaction using a token through its TSP (Token Service Provider – a financial institution that provides the token issuing service). Such a transaction is more secure because the card number undergoes fewer processing steps. The payment card number is only visible to TSP and the card issuer. The online store and the acquirer do not see the actual card number, but only a token.

– And what is a token?

– It is a set of numbers generated according to certain rules. The token repeats the format of the card number. For outsiders it is impossible to distinguish a token from the real card number. This is done on purpose, because the token must exist and operate in the current infrastructure of card payments. In fact, the entire infrastructure of acquiring, switching, and processing must treat it as a real card number. Therefore, the token format is regulated by EMVCo – an organization that defines how a token should look like and keeps record of all token issuers.

– So, there is no external difference between a token and a card – they both have 16 digits…

– That's right.

– One of the key benefits of tokenization is better security. What other advantages are there for banks, merchants?

– Merchants do not have to store real card numbers, so their PCI DSS scope is reduced, meaning that fewer systems are subject to audit, accordingly, there is a decrease in costs of achieving PCI DSS compliance.

Acquiring banks that work with e-merchants can offer tokenization as a service. This is an additional business for an acquirer.

– For what period of time can a token be set or can it be used only once?

– There are many options. Restrictions on the use of a token are determined by an issuer. Issuers can set calendar limitations on a token's lifecycle or impose restrictions on the scope of application of a token (e.g. for e-commerce or mobile payments only). By establishing these rules, issuers can further control risks and protect their cardholders from attacks.

– And how does the substitution with a token affect the transaction speed?

– Technically, it is an extra step in the authorization processing, but it is executed so fast that the end user does not notice it. In other words, the user will not notice the difference when paying, for example, with a contactless card at a POS terminal or making a payment from the mobile wallet at the same POS terminal. These are fractions of seconds, not more.

– As you mentioned, EMVCo defines the requirements for the token format. Does it mean that EMVCo sets standards for all tokens that are used in the banking and payment card sectors, or are there separate standards for each international card organization?

– International card organizations operate through EMVCo. EMVCo acts as a token standardizer. And international card organizations operate in accordance with specifications issued by EMVCo.

– So, there are common rules for everyone.

– Yes, absolutely.

– Are there any examples of successful implementation of tokenization technology on the mobile payments market?

– MasterCard and Visa provide tokenization services through their digitalization services – MDES (MasterCard Card Digital Enablement Service) and VTS (Visa Token Service). Currently, these are one of the best known examples of mobile payment support services.

– Are banks interested in the tokenization technology?

– In our experience, yes, they are. And not only banks, but also processing centres. This is particularly noticeable in countries and regions where the so-called branded mobile wallets are actively promoted, such as Apple Pay and Samsung Pay, which use tokenization in their solutions, and therefore banks must also follow these rules.

Recently, Sberbank and Apple Pay have issued a press release announcing their commencement of operation in Russia. Apple Pay uses tokenization, and Sberbank has also connected to MasterCard tokenization services.

Our customers who are already working or planning to work with branded mobile wallets also use tokenization. Thus, Tieto delivered an IT solution to the Russian Standard Bank to enable provision of the Samsung Pay payment service, where a token is used instead of a payment card.

Tokenization is also used in HCE-based (the Host Card Emulation technology) mobile wallets. Such solutions are mainly implemented by banks that want to build their own mobile wallets. Similar HCE-based solutions are available in countries where Apple Pay or Samsung Pay are not operating yet, and the banks take the initiative and launch their own solutions.

– What features and functionalities does the Tieto's solution provide for tokenization?

– We have implemented tokenization as part of the functionality of our HCE solution which is included in the Tieto Card Suite product line. The Tieto Host Card Emulation solution can be used by our existing customers (i.e. as part of an existing system, Card Suite) or as a stand-alone solution with systems delivered by other suppliers. Tieto Host Card Emulation solution provides such functions as user registration, tokenization of cards, processing of tokenized transactions (detokenization), cryptogram validation, and generation of payment attributes that can later be downloaded to a mobile phone. In addition, Tieto provides different APIs for integration with a mobile app, API for integration with an issuing system, as well as an online interface to transaction processing host systems. We also plan to use tokenization for e-merchants in future applications of this technology.

– Does the Tieto's solution support a number of business models of mobile wallets?

– Yes, we implement and support various models. If a financial institution wants to work with such branded wallets as Apple Pay or Samsung Pay, our solutions will ensure the relevant support. We can also provide a solution for those financial institutions that want to launch their own wallets.

– Does Tieto offer its own (off-the-shelf) wallet solution?

– Tieto has a large unit that develops mobile banking applications for financial institutions. If a customer is interested, we will certainly provide a full-featured mobile banking solution with an integrated functionality of personal payments, contactless payments, etc. However, according to our current projects, customers who adopt mobile payments tend either to choose or work with brands like Apple Pay and Samsung Pay (and they already provide their applications), or embed the payment functionality into their existing mobile banking platform and existing smartphone applications. Banks have not yet shown any interest to such individual (or I would say "naked") applications that would provide the only ability to pay.

– Does it mean that Tieto Card Suite includes support of Cloud Based Payments?

– The term "Cloud Based Payments" was first used by MasterCard to denote the entire complex of solutions and processes that allow integrating a card into a phone and carrying out mobile payments. Nowadays, Cloud Based Payments is a marketing slogan, and we support the technology, business models and requirements that it provides for, including the digitalization programs MDES and VTS, HCE technology, tokenization etc.

– Is the Ukrainian market ready for the implementation of mobile payments and tokenization?

– Yes, we have identified Ukraine as a potential market for contactless and mobile payments. According to the statistical data available to us, users in Ukraine hold about 20 million smartphones, 60% of which are of the Android platform (the platform that supports the HCE technology of tokenization). According to statistics, about 40% of POS terminals in Ukraine support the contactless technology. The acquiring infrastructure already exists. We believe that this direction will develop quite rapidly.

– In your opinion, what is the main advantage of the solution provided by Tieto as regards tokenization?

– Tieto's solution can be operated not only by our existing customers, but also by customers of other suppliers. We can integrate our solution with any other issuing host system. Like other Tieto products, our tokenization and mobile payments solutions are delivered with public interfaces. Thus, banks and processing centres, using our interfaces, can build any solutions for their end users – we do not limit the use of the functionality.