On-device tokenization in India

Payment law in India required a few years ago that server based card-on-file systems are not allowed. Instead, there is a necessity to store user data on-device to perform transactions.

This is an interesting topic that impacted a lot of local players like big merchants, Cred, Phonepe or Amazon so let me describe it in some details because maybe it will be implemented in a few years in other countries as well.

Requirement for storing tokens in a secure way on customer devices forces us to implement and certify secure SDK in which payment token data will be saved. It is a similar concept to standard HCE (Host Card Emulation) implementation for mobile NFC payments. While registering to a merchant or wallet system, the user adds a payment card, performs tokenization with approval (One-Time-Passwords) of the issuing bank and the token connected with his card is stored in this wallet / SDK.

Once we have a secure place of storing the user's token on his mobile phone we can use this token for multiple purposes:

1. NFC / contactless payments - the user uses his phone to perform transactions on a contactless acceptance network. Token and payment keys are transferred through the contactless interface to the payment terminal and acquirer for authorization.
2. inApp - the user chooses products and adds them to the basket in the merchant app, clicks that he wants to pay with a particular wallet or payment brand and confirms the transaction in a wallet app. The token is taken from an SDK, transferred to the cooperating acquirer in the form of a DSRP message (Dynamic Secured Remote Payment) and processed in standard way
3. web purchase - the user chooses products and adds them to the basket on the merchant website, clicks that he/she wants to pay with a particular wallet or payment brand and receives a push notification in his/her mobile app to finalize the transaction. As above, the token is taken from an SDK, transferred to the cooperating acquirer in the form of a DSRP message (Dynamic Secured Remote Payment) and processed in standard way. There could be a possibility to store the token inside the browser of the user on his laptop / PC but this requires more discussion with Mastercard and VISA.

To enable these use cases, several implementation points needs to be considered:

- types of devices - an inApp and web purchase can work on all devices (iOS and Android) but NFC is enabled on Android only. Apple is blocking the NFC access outside of the

European Union today.
- VISA vs Mastercard - do you need a solution working for both schemes? Are there any local certification requirements?
- Issuers - are banks ready to connect to your new X-Pay wallet? Which banks are enabled on local markets?
- local on-soil requirements - is there a need to store data in the country? What are the legal impacts?

This is an interesting development and area of work. We are live with a few partners and are happy to work with new ones. Please contact us if you are interested.

Thanks for reading.

Revision #4
Created 19 April 2024 05:10:09 by Krzysztof Drzyzga
Updated 22 April 2024 11:16:20