Date : May 11, 2023

Device based Tokenisation – Card Transactions

(Updated as on May 11, 2023)

1. What is tokenisation?

Ans. Tokenisation refers to replacement of actual card details with an alternate code called the "token", which shall be unique for a combination of card, token requestor (i.e. the entity which accepts request from the customer for tokenisation of a card and passes it on to the card network to issue a corresponding token) and device (referred hereafter as "identified device").

2. What is de-tokenisation?

Ans. Conversion of the token back to actual card details is known as de-tokenisation.

3. What is the benefit of tokenisation?

Ans. A tokenised card transaction is considered safer as the actual card details are not shared with the merchant during transaction processing.

4. How can the tokenisation be carried?

Ans. The card holder can get the card tokenised by initiating a request on the app provided by the token requestor. The token requestor will forward the request to the card network which, with the consent of the card issuer, will issue a token corresponding to the combination of the card, the token requestor, and the device.

5. What are the charges that the customer need to pay for availing this service?

Ans. The customer need not pay any charges for availing this service.

6. What are the use cases (instances / scenarios) for which tokenisation has been allowed?

Ans. Tokenisation has been allowed on consumer devices like mobile phones, tablets, laptops, desktops, wearables (wrist watches, bands, etc.), Internet of Things (IoT) devices, etc, for all use cases / channels (e.g., contactless card transactions, payments through QR codes, apps etc.)

7. Can tokenisation be enabled through a smart watch or such other devices?

Ans. The feature of tokenisation is available on consumer devices like mobile phones, tablets, laptops, desktops, wearables (wrist watches, bands, etc.), Internet of Things (IoT) devices, etc.

8. Who can perform tokenisation and de-tokenisation?

Ans. Tokenisation and de-tokenisation can be performed by the authorised card network or by the card issuer. The list of card networks authorised by RBI to operate in India is available on the RBI website at the link https://www.rbi.org.in/Scripts/PublicationsView.aspx?id=12043.

9. Who are the parties / stakeholders in a tokenisation transaction?

Ans. Normally, in a tokenised card transaction, parties / stakeholders involved are merchant, the merchant's acquirer, token service provider (card payment network or card issuer), token requestor, issuer and customer. However, an entity, other than those indicated, may also participate in the transaction.

10. Are the customer card details safe after tokenisation?

Ans. Actual card data, token and other relevant details are stored in a secure mode by the token service provider (card payment network or card issuer). Token requestor cannot store Primary Account Number (PAN), i.e., card number, or any other card detail. Card networks are also mandated to get the token requestor certified for safety and security that conform to international best practices / globally accepted standards.

11. Is tokenisation of card mandatory for a customer?

Ans. No, a customer can choose whether or not to let his / her card tokenised.

12. Does the customers have the option to select tokenisation for a particular use case?

Ans. Customers have the option to register / de-register their card for a particular use case, i.e., contactless, QR code based, in-app payments, etc.

13. How does the process of registration for a tokenisation request work?

Ans. The registration for a tokenisation request is done only with explicit customer consent through Additional Factor of Authentication (AFA),

and not by way of a forced / default / automatic selection of check box, radio button, etc. Customer will also be given choice of selecting the use case and setting-up of limits.

14. Can the customer set / select own limits for tokenised card transactions?

Ans. Customers have the option to set and modify per transaction and daily transaction limits for tokenised card transactions.

15. Is there any limit on the number of cards that a customer can request for tokenisation?

Ans. A customer can request for tokenisation of any number of cards. For performing a transaction, the customer shall be free to use any of the cards registered with the token requestor app.

16. Can the customer select which card to be used in case he / she has more than one card tokenised?

Ans. For performing any transaction, the customer shall be free to use any of the cards registered with the token requestor app.

17. Is there any limit on the number of devices on which a card can be tokenised?

Ans. A customer can request for tokenisation of his / her card on any number of devices.

18. Whom shall the customer contact in case of any issues with his / her tokenised card? Where and how can he / she report loss of device?

Ans. All complaints should be made to the card issuers. Card issuers shall ensure easy access to customers for reporting loss of "identified device" or any other such event which may expose tokens to unauthorised usage.

19. Can a card issuer refuse tokenisation of a particular card?

Ans. Based on risk perception, etc., card issuers may decide whether to allow cards issued by them to be registered by a token requestor.

20. Where can more information on RBI instructions on tokenisation be found?

Ans. More information can be found in the following circulars issued by RBI - DPSS.CO.PD No.1463/02.14.003/2018-19 dated January 8, 2019, CO.DPSS.POLC.No.S-469/02-14-003/2021-22 dated August 25, 2021 and CO.DPSS.POLC.No.S-516/02-14-003/2021-22 dated September 07, 2021.

These FAQs are issued by the Reserve Bank of India (hereinafter referred to as "Bank") for information and general guidance purposes only. The Bank will not be held responsible for actions taken and / or decisions made on the basis of the same. For clarifications or interpretations, if any, one may be guided by the relevant circulars, guidelines and notifications issued from time to time by the Bank.