भारतीय रिज़र्व बैंक
RESERVE BANK OF INDIA
www.rbi.org.in

RBI/2018-19/103
DPSS.CO.PD No.1463/02.14.003/2018-19 January 08, 2019

The Chief Executive Officer / President
All authorised card payment networks

Madam / Dear Sir,

Tokenisation – Card transactions

Continuing the efforts to improve safety and security of card transactions, Reserve Bank of India had permitted card networks for tokenisation in card transactions for a specific use case.

2. It has now been decided to permit authorised card payment networks to offer card tokenisation services to any token requestor (i.e., third party app provider), subject to the conditions listed in Annex 1. This permission extends to all use cases / channels [e.g., Near Field Communication (NFC) / Magnetic Secure Transmission (MST) based contactless transactions, in-app payments, QR code-based payments, etc.] or token storage mechanisms (cloud, secure element, trusted execution environment, etc.). For the present, this facility shall be offered through mobile phones / tablets only. Its extension to other devices will be examined later based on experience gained.

3. All extant instructions of Reserve Bank on safety and security of card transactions, including the mandate for Additional Factor of Authentication (AFA) / PIN entry shall be applicable for tokenised card transactions also.

4. All other instructions related to card transactions shall be applicable for tokenised card transactions as well. The ultimate responsibility for the card tokenisation services rendered rests with the authorised card networks.

भुगतान और निपटान प्रणाली विभाग, केंद्रीयकार्यालय, 14वींमंजिल, केंद्रीयकार्यालयभवन,शहीदभगतसिंहमार्ग, फोर्ट, मुम्बई - 400001
फोनTel: (91-22) 2264 4995; फैक्सFax: (91-22) 22691557; ई-मेलe-mail : cgmdpssco@rbi.org.in
Department of Payment and Settlement Systems, Central Office, 14th Floor, Central Office Building, ShahidBhagat Singh Road, Fort, Mumbai - 400001

5. No charges should be recovered from the customer for availing this service.

6. Before providing card tokenisation services, authorised card payment networks shall put in place a mechanism for periodic system (including security) audit at frequent intervals, at least annually, of all entities involved in providing card tokenisation services to customers. This system audit shall be undertaken by empanelled auditors of Indian Computer Emergency Response Team (CERT-In) and all related instructions of Reserve Bank in respect of system audits shall also be adhered to. A copy of this audit report shall be furnished to the Reserve Bank, with comments of auditors on deviations, if any, from the conditions listed in Annex 1, along with the compliance thereto. Further, a report on the details provided in Annex 2 shall be submitted at monthly intervals to the Chief General Manager, Reserve Bank of India, Department of Payment and Settlement Systems, Central Office, Mumbai and by email.

7. This directive is issued under Section 10 (2) read with Section 18 of Payment and Settlement Systems Act, 2007 (Act 51 of 2007).

Yours faithfully,

(P Vasudevan)
Chief General Manager

Encl.: As above

Annex 1

(DPSS.CO.PD.No.1463/02.14.003/2018-19 dated January 08, 2019)

Card tokenisation services

Tokenisation refers to replacement of actual card details with an unique alternate code called the "token", which shall be unique for a combination of card, token requestor and device (referred hereafter as "identified device").

Conditions

Tokenisation – de-tokenisation service

i. Tokenisation and de-tokenisation shall be performed only by the authorised card network and recovery of original Primary Account Number (PAN) should be feasible for the authorised card network only. Adequate safeguards shall be put in place to ensure that PAN cannot be found out from the token and vice versa, by anyone except the card network. Integrity of token generation process shall be ensured at all times.

ii. Tokenisation and de-tokenisation requests should be logged by the card network and available for retrieval, if required.

iii. Actual card data, token and other relevant details shall be stored in a secure mode. Token requestors shall not store PAN or any other card detail.

Certification of systems of card issuers / acquirers, token requestors and their app, etc.

iv. Card network shall get the token requestor certified for (a) token requestor's systems, including hardware deployed for this purpose, (b) security of token requestor's application, (c) features for ensuring authorised access to token requestor's app on the identified device, and, (d) other functions performed by the token requestor, including customer on-boarding, token provisioning and storage, data storage, transaction processing, etc.

v. Card networks shall get the card issuers / acquirers, their service providers and any other entity involved in payment transaction chain, certified in respect of changes done for processing tokenised card transactions by them.

vi. All certification / security testing by the card network shall conform to international best practices / globally accepted standards.

Registration by customer

vii. Registration of card on token requestor's app shall be 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.

viii. AFA validation during card registration, as well as, for authenticating any transaction, shall be as per extant Reserve Bank instructions for authentication of card transactions.

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

x. Customers shall be given option to set and modify per transaction and daily transaction limits for tokenised card transactions.

xi. Suitable velocity checks (i.e., how many such transactions will be allowed in a day / week / month) may be put in place by card issuers / card network as considered appropriate, for tokenised card transactions.

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

Secure storage of tokens

xiii. Secure storage of tokens and associated keys by token requestor on successful registration of card shall be ensured.

Customer service and dispute resolution

xiv. 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. Card network, along with card issuers and token requestors, shall put in place a system to immediately de-activate such tokens and associated keys.

xv. Dispute resolution process shall be put in place by card network for tokenised card transactions.

Safety and security of transactions

xvi. Card network shall put in place a mechanism to ensure that the transaction request has originated from an "identified device".

xvii. Card network shall ensure monitoring to detect any malfunction, anomaly, suspicious behaviour or the presence of unauthorized activity within the tokenisation process, and implement a process to alert all stakeholders.

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

Annex 2

Reporting format for tokenisation service by authorised card networks

(DPSS.CO.PD.No.1463/02.14.003/2018-19 dated January 08, 2019)

(to be furnished by 10th of each month)

Name of authorised card network: ……..

Report for the month: …….

Sr. No.	Name of token requestor	Brand name, if any, of the service	Use cases enabled (contactless – NFC / MST, in-app, QR code-based, etc.)	Token storage mechanism employed	Effective date of arrangement	No. of cards registered		
						Credit Cards	Debit Cards	Prepaid Cards

Note: Above data shall be as at end of month

Sr. No.	Name of token requestor	Transaction data for the month*					
		Credit Cards		Debit Cards		Prepaid Cards	
		Number	Value (in Rs.)	Number	Value (in Rs.)	Number	Value (in Rs.)

*Transaction data to be provided for each use case enabled by the card network

---