ISSN (O): 2584-2196

INTERNATIONAL JOURNAL OF LEGAL AFFAIRS AND EXPLORATION

Volume 2| Issue 3

2024

ISSN (O): 2584-2196

RBI'S TOKENIZATION- A SUCCESS OR A SINK

Sethulakshmi.N.K

Final Year BA LL.B (H) Student of Sastra University, Thanjavur.

ABSTRACT

The proliferation of digital world provided new drives for credit- card based businesses and marketing by financial institutions towards reaching out to new markets and crediting opportunities for economic growth. This paper sets its background when Reserve Bank of India (RBI) came up with the recent guidelines in the field of both device based and card based tokenization in the year of 2019 and 2021 respectively. To the general understanding the tokenization can be simplified into the terms that the process of replacement of your original card details with a unique code which is called as token. Even though this process has been witnessing in our life on a daily basis general public are not fully aware of the process and it's functioning as well as its importance, the same has been evident from the questionnaire circulated among the public. Tokenization requires minimal changes to add strong data protection to existing applications. This paper focuses on the how tokenization differs from traditional encryption method along its effectiveness over the same. Also RBI guidelines has mentioned that consent is required for the tokenization process but the guidelines are silent about how this consent are obtained. In this paper the author made an attempt to solve this issue while looking into various definitions under Digital Personal Data Protection Act 2023. Thus the paper tries to find out solutions to various questions and contingencies like; whether the data used in tokenization comes under the purview of personal data under DPDP Act 2023, if yes, then can the consent can be obtained as per the regulations of the same Act. The authors also tried to find out what are the 'globally acceptable standards' mentioned in the RBI Guidelines for the purpose of tokenization. Therefore this paper revolves around like an interplay between DPDP Act and RBI guidelines along with IT Act 2000.

Key Words: *Tokenization, Token, Personal Data, Device based tokenization, COFT, Consent, Encryption.*

1. INTRODUCTION

The advent of card transactions started from 1980 where the Central Bank of India first introduced the Credit cards of Visa brand. The proliferation of digital world provided new drives for credit-card based businesses and marketing by financial institutions towards reaching out to new markets

and crediting opportunities for economic growth. Our paper sets its background when Reserve Bank of India (RBI) came up with the recent guidelines in the field of both device-based and card-based tokenization in the year of 2019 and 2021 respectively. To the general understanding the tokenization can be simplified into the terms that the process of replacement of your original card details with a unique code which is called as token. Even though this process has been witnessing in our life on a daily basis general public are not fully aware of the process and it's functioning as well as its importance, the same has been evident from the questionnaire circulated among the public. Tokenization requires minimal changes to add strong data protection to existing applications. Our paper focuses on the how tokenization differs from traditional encryption method along its effectiveness over the same. The guidelines issued by the RBI guidelines has also mentioned that consent of the card holder is required for the tokenization process but the guidelines are silent about how this consent are obtained. In this paper the authors made an attempt to solve this issue while looking into various definitions under Digital Personal Data Protection Act 2023. Thus, the paper tries to find out solutions to various questions and contingencies like; whether the data used in tokenization comes under the purview of personal data under DPDP Act 2023, if yes, then can the consent can be obtained as per the regulations of the same Act.

Adoption and usage of card payments can be determined by the number of debit and credit cards issued in a particular country. The usage of debit and credit cards are increasing day by day and India is standing in 2nd position with 886 million debit cards issued by 2020 and at 7th position with 60.4 million credit cards.[1] Similarly, the volume of card payments which indicates the acceptance of cards as preferred payment increased from 4.8 billion transactions in 2017 to 5.98 billion transactions in 2020.[2] At present, in 2023, it is expected that it will be above 6 billion transactions. But, while comparing it with the other countries of the world, India's share to the card transaction is very low. This is evident from the fact that the ratio of card payments to the Credit Information Company (CIC) is less than 1.[3] This indicates that people are less likely to choose card payments in comparison with other modes of payment namely the digital transactions, online banking, net banking etc.

[1] Benchmarking India's Payment Systems, July 2022, pg. 40.
[2] Benchmarking India's Payment Systems, July 2022, pg. 45.
[33] Benchmarking India's Payment Systems, July 2022, pg. 46.

2. LITERATURE REVIEW

R.Battula, The Economic Times (Jun 28, 2023): Card tokenization is a process that replaces sensitive credit card information with a unique identifier or token. This token is used for all transactions, reducing the risk of unauthorized access and fraud. It enhances security by eliminating the need to store sensitive information and promotes compliance with regulatory standards. Card tokenization also provides convenience for consumers and allows for seamless transactions across different platforms.

GB Iwasokun and Others (2018) : This summary discusses the importance of credit card information security and the use of encryption and tokenization-based systems to protect sensitive data. It highlights the advantages and superiority of such systems in terms of credit card security, key size, mobile alert, and tokenization. The summary also mentions the potential risks of unauthorized access and disclosure of unencrypted data. Tokenization is commonly used for structured data, such as payment card information or social security numbers. It provides an additional layer of security by replacing sensitive data with tokens that are meaningless to potential attackers. This reduces the risk of unauthorized access and disclosure of sensitive information. The article mentions the relative advantages and superiority of the system in credit card security, key size, mobile alert, and tokenization over some other systems. It implies that tokenization is more effective compared to traditional encryption methods in terms of credit card security. However, the article does not provide specific details or comparative analysis regarding the effectiveness of tokenization over traditional encryption methods. It primarily focuses on presenting an RSA encryption and tokenization-based system for credit card information security.

S.Banerjee, S.Shukla & KSR Menon (2022): The article highlights the limitations of the current approach taken by the Reserve Bank of India (RBI) in regulating financial data protection, which relies on piecemeal regulations and focuses primarily on card data security. The authors argue that a more holistic and principles-based approach is needed to address privacy risks in the payments industry. They suggest enacting a comprehensive data protection law that aligns with the principles embodied in the Data Protection Bill and integrating data protection jurisprudence with the regulation of financial data. The article calls for a shared regulatory mechanism between a specialized data protection authority and the RBI to effectively manage privacy risks. But the authors have not elaborated on how the DPBA 2023 can be connected with the protection of Financial Data.

3. WORKING OF CARD TRANSACTIONS

Earlier the cards were used only in the shops to make payments for our purchases. With the increased use of internet banking, nowadays, cards are also used for online payments. When we are making online payments, like prepaid orders, bill payments, booking a bus or train etc, we use the card number along with the CVV at the back side of the Card to make payments. This is where the need for tokenization raised. The Card numbers we enter in various websites without any second thought contain a lot of valuable information. Before reading more upon the concept of tokenization and to understand the process of card transactions, it is important to understand certain terms and concepts like Point of Sale (PoS) terminals, Card-on-File (CoF) transactions, token requester, card network, Merchant Account, Payment Service provider, Capturing and Settlement, Card issuer, Card authorization.

i. ***Card authorization:*** The process of card authorization is done by the card issuing bank (issuing bank). It is the process by which the success or failure of a bank transaction occurs. To put it simply, this process will decide whether to accept or decline the transaction request. If the Authorization is successful the transaction will be completed and the transaction if it declines then it means that the Authorization has not been accepted by the issuing bank. The request for authorization is received by the issuing bank from the Merchant via payment gateway.

ii. ***Card on File (CoF):*** Card-on-File refers to storing of the card information by the merchant in a file. The process of CoF will take place while the card is swiped in the Point-of-Sale terminals.

iii. ***Issuing Bank:*** The card issuer or issuing bank is an entity from which a person will receive her debit or credit cards. These issuing banks will transfer the transaction amount from their respective bank account to the merchant.

iv. ***Merchant Bank or Acquirer:*** The Merchant bank as the name describes is the bank of the Merchant. When a card payment is initiated by the Merchant, this bank will process the card for the merchant and it will connect it to the issuing bank to complete the payment.

v. ***Capturing or clearing and Settlement:*** Every card network will have their own clearing system to enable the card transactions. The process of clearing involves sharing the necessary transaction information by the Acquiring bank. Once the information is received by the Acquiring bank it will then with the help of card networks create a clearing file which will be verified by the issuing bank to validate the transaction. Thus, the Clearing can be defined as the process of sending the transaction related information and verification of the same as clear

or clean. After clearing the transfer of funds from the payee's account to the beneficiary will take place which is termed as Settlement.

vi. ***Payment System:*** A payment system will govern the entire card transactions. It will enable the payment between payer and the beneficiary. The payment system consists of clearing, payment or settlement.[4]

vii. ***Card Network:*** A card network can be defined as an organization formed and responsible for issuing credit or debit cards or both to the customers through banks. Each bank will avail a service of these kinds of card networks to issue cards to their customers. Usually, the name of the card network used by the particular bank is visible on the card itself. Examples of card networks include Visa, Mastercard, RuPay etc. This card network provides payment services to the banks by enabling the card payment transaction. The different stages of a card transaction like authorization, clearing and settlement will take place only through these card networks.

viii. ***Point of Sale (PoS) terminals:*** The Point-of-Sale terminals or in short PoS terminals are the software that is used by the Merchant to process the card transactions. In layman terms this is the card machine which is available in all the super markets, malls and other stores which accepts card transactions. As soon as the card is swiped along the side or shown over the screen, it will capture the card details and initiate the authorization procedure.

Thus, a brief process of a Card transaction will take place as follows:

i. The Merchant will initiate the payment by using the PoS.
ii. First the Card holder's identity is verified which is called Authentication.
iii. The PoS with the help of the Card network and Acquiring bank will send authorization requests to the issuing bank.
iv. Once the Authorization is done by the issuing bank, the acquirer will initiate the clearing process by sending the transaction information to the issuing bank.
v. The issuing bank in turn will complete the transaction by the process of settlement where the money will be credited to the Merchant's account from the card holder's bank account.

[4] The Payments and Settlements Systems Act, 2007; § 2(1)(i).

4. NEED FOR TOKENIZATION

In 2019 as per an article published by India Today Card details of 1.3 million Indian Payment cards have been put on sale on dark web, a website named Joker's stash, which is a site used by the cyber criminals for selling card data. In 2017 it was reported by Madhya Pradesh police cyber cell that bank account details like to which bank a card is linked to, its CVV number, phone numbers and email Ids were put on sale just for INR 500 (Indian Rupees Five Hundred). It was reported in The Economic Times in 2021that as per an individual cybersecurity researcher's research 10 crore Indian's card data were sold on dark web for undisclosed amount. As per his report this data was leaked from a predominant payment gateway Juspay. He also mentioned the disadvantage of PCI DSS as "if the hackers can find out the Hash algorithm used to generate the card fingerprint, they will be able to decrypt the masked card number".[5] It has been reported that cybercrime cases were increased in thrice the volume of crimes in 2022 while comparing it to 2017. It is pertinent to note that the online fraud during the card payments and online transfer are top in the list of the cybercrime across the Bengaluru city.[6] The cybercrime rate has increased tremendously in recent years to an extent that about 59% of the Indians have experienced cybercrime attacks in 2021 as per the survey conducted by Norton[7]. This increasing number of card data theft, cybercrimes and privacy concerns leads the RBI to take steps to protect the card data and that eventually sowed the seeds to the process of "*Card Tokenization".*

5. DECODING THE RBI GUIDELINES

Upon the various guidelines issued by the RBI, for the purpose of this paper, three notifications were important in the regard of tokenization. The first notification was issued in 2019 and its extended version and third notification in 2021. The first two notifications were related to device-based tokenization (DBT) and third one is related to Card-on-file tokenization (CoFT). Thus, RBI has come up with two types of tokenization through its guidelines. However, it has not provided any definition for each type of tokenization rather it defined the term 'tokenization' in general which this paper has mentioned in the previous part. Let us understand these two types of tokenization with an illustration.

[5] The Economic Times, https://economictimes.indiatimes.com/tech/technology/10-crore-indians-card-data-selling-on-dark-web-researcher/articleshow/80093994.cms, (last visited Oct. 22, 2023)
[6] The Economic Times, https://economictimes.indiatimes.com/news/india/cybercrime-cases-triple-in-bengaluru-in-six-years-card-payments/online-transfer-top-charts-of-fraud/articleshow/101704310.cms, (last visited Nov. 15, 2023)
[7] Indian express, https://indianexpress.com/article/technology/tech-news-technology/norton-survey-reveals-59-indians-have-dealt-with-cybercrime-in-past-12-months-7280071/, (last visited Nov. 15, 2023)

Suppose Ram, a customer, wants to purchase clothes for his upcoming birthday. He usually makes his purchases only from his favourite shop 'trendio'. This Trendio has both outlets and online based shopping facilities. If Ram choose to visit the nearby branch for his purchase and make payment through his card it will come under the CoFT. On the other hand, if he orders and makes payment online using the shop's website it will be covered by DBT. Thus, when a card payment is made through PoS in shops it will be dealt by CoFT and when it is done through the merchant's website it is dealt by DBT. Apart from the website-based purchase, DBT also covers transactions such as near field communication, contactless card-based transactions, in-app payments, QR code-based payments.

6. DEVICE BASED TOKENIZATION

The first rules governing the device-based tokenization was issued on January 08, 2019 by RBI. Primarily the notification focussed only on two devices namely mobile phones and tablets. The tokenization service will be offered by an authorised card payment network to any person who is requesting for the tokenization. The person who is requesting for a token is termed as 'token requester'. Generally, these token requesters are third party app providers like Amazon Pay or Google Pay (GPay) and similar other app providers who are enabling payment or transfer of money to other persons. Even though the devices in which tokenization can be carried out is restricted, it covers almost all the use cases. Use case/Channels refers to the method by which we initiate the payment and it includes in-app payments, QR code-based payments and other similar form of payments. The tokenization can be granted also to the token storage mechanisms like cloud storage or secure element storage or other similar mechanisms. For enhanced security Additional factor of authentication or PIN entry shall be applicable even for the tokenized cards. Card issuer is having an option to decide whether it can allow a token requestor to provide tokenization for its cards or not.

The Token Requestor before availing the services of tokenization should get its system certified by the card network. A simple process of certification would start from Token Requestor making a request to the Card Network to get its system certified. As soon as the Token Requestor get the certification, it is authorised to generate tokens for the customers holding and using the debit/credit card issued by that particular card network. While certifying the Token Requestor's systems, the card network shall analyse its hardware, level and extent of security granted by the system, the method by which the system stores and transmit the confidential information and features related to the authorised access of the app on identified device. The 'identified device' is nothing but combination of card, Token Requestor and the device of the user. The RBI has not prescribed any

specific method in which the certification needs to be done. It has left it to the option of the Card network carrying out the certification. Any certification or the security testing carried out by the card network should be in confirmation with any international best practice or globally accepted standards. This leads to lack of uniformity in the methods adopted by the card network and in turn question the reliability of the certification.

7. CARD ON FILE TOKENIZATION (CoFT)

The device-based tokenization was extended even for cards by the RBI through its Card on File Tokenization guideline issued in 2021. It has been mandated by the RBI in March 2021 that neither the payment aggregators nor the merchants on-boarded by them can store the card data or credentials of a card used by a customer.[8] In the CoFT, tokenization can be done only by the card issuers. The card issuers offering the tokenization service is called as Token Service Provider (TSP). A TSP can generate tokens only for the cards issued by them. For example, if Rupay is offering COFT services, it can create tokens only for the RuPay cards. But this is not the case in device-based tokenization where the any token requestor approved by the card network will generate token and single token requestor can get its system certified by various card networks so that it can create tokens for all those different cards.

8. TOKENIZATION OVER TRADITIONAL ENCRYPTION

Tokenization requires minimal changes to add strong data protection to existing applications. Traditional encryption solutions enlarge the data, requiring significant changes to database and program data schema, as well as additional storage. It also means that protected fields fail any validation checks, requiring further code analysis and updates. Tokens use the same data formats, require no additional storage, and can pass validation checks.

As applications share data, tokenization is also much easier to add than encryption, since data exchange processes are unchanged. In fact, many intermediate data use – between ingestion and final disposition – can typically use the token without ever having to de tokenize it. This improves security, enabling protecting the data as soon as possible on acquisition and keeping it protected throughout the majority of its lifecycle.

Within the limits of security requirements, tokens can retain partial clear text values, such as the leading and trailing digits of a credit card number. This allows required functions—such as card

[8] Reserve Bank of India, https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=12050&Mode=0 (last visited Nov. 15, 2023)

routing and "last four" verification or printing on customer receipts—to be performed using the token, without having to convert it back to the actual value.

This ability to directly use tokens improves both performance and security: performance, because there is no overhead when no de tokenization is required; and security, because since the clear text is never recovered, there is less attack surface available.

As data breaches rise and data security becomes increasingly important, organizations find tokenization appealing because it is easier to add to existing applications than traditional encryption. Since payments data flows are complex, high performance, and well defined, tokenization is much easier to add than encryption.

Therefore, traditional tokenization systems have several limitations that impact data usage and security. Most traditional tokenization systems fail to account for input data types during token generation, severely limiting support for analytics. Also, the lack of context around sensitive data inputs prevents most tokenization systems from securely managing the de tokenization process. While tokenization of cards has several benefits such as heightened security and faster checkouts, it is important to note that traditional tokenization systems have several limitations that impact data usage and security.

Moreover, the goal of RBI's tokenization effort is to protect all payment data. It will only increase the security of credit and debit card transactions with this new strategy to combat cybercrime.

9. CONSENT AND DPDPACT, 2023

After getting its system certified, the Token Requestor can create valid tokens when a customer is using its app. The RBI guidelines has clearly mentioned that before generating a token for a particular, consent of the card holder is required. Such consent should not be vague and ambiguous. It should an explicit consent given by the card holder to tokenise its card. This explicit consent is said to be given as soon as the card holder completes the Additional Factor Authentication or manually click the terms and conditions check box. However, the guideline is silent about the extent of the consent in the sense that it does not mentioned details with respect to what are all the information that need to be informed to the card holder to give his consent. It creates a question that whether just an explicit consent by entering an OTP or by clicking a check box is more than enough instead of an informed consent.

One of the important legislations dealing with *'consent'* would be Digital Data Protection Act, 2023. Section 6 of the Act has laid down the manner in which the Data Principal should give their

consent. To determine whether the criteria given for valid consent enumerated under Section 6 can be followed for consent given by the card holder, it is necessary to analyse whether the card holder, card information can be drag into the scope of the DPDP Act, 2023.

Section 2(h) of the 2023 Act defines the term *'data'* as representation of information, facts, concepts, opinions or instructions in a manner suitable for communication, interpretation or processing by human beings or by automated means.[9] Further '*personal data'* means any data about an individual who is identifiable by or in relation to such data.[10] And finally any personal data in digital form can be called as '*digital personal data'.*[11] Tokenization involves converting the primary card number or account number into a token. While processing the tokenization the Token Requestor app will ask the card holder to enter the card number, name as on the card and CVV in the back side of the card. An information can be generally defined as a fact or detail about someone or something.[12] Therefore, the information given in a card can be qualified as a data as given under Section 2(h) of the Act. Now it needs to be clarified whether this information can be termed as personal data. If that not all personal data can be given scope under the DPDP Act. Any data to be governed by DPDP Act should be *digital* personal data. Data is considered to be digital if it is collected digitally data is identifying or attributing towards a person it can be safely called as personal data under the Act. Data or information in a card is related to a card holder. When a card number is lawfully processed it is possible for the processor to know the details of the card holder like his name, name of the bank in which the card was registered and other such details. Thus, a card holder can be identified by the card data and he is related to the card data. Therefore, any information in the card can be treated as personal data under the Act. It is important here to note or if it is subsequently digitalised after the collection. In our case the card information was entered by the card holder for tokenization digitally in the Token Requestor's app. Thus, the Token Requestor is collecting the data digitally and he is processing such data further to create a token. Since the data in card is satisfying all the conditions under the DPDP Act to be a valid personal data it can come within the purview of the Act.

Next is to analyse whether the process of Tokenization can be considered as processing of personal data for lawful purpose under the Act so that the consent procedure and criteria given under Section 6 can be incorporated. Processing in relation to personal data means any set of operations

[9] Digital Data Protection Act, 2023; § 2(h).
[10] Digital Data Protection Act, 2023; § 2(t).
[11] Digital Data Protection Act, 2023; § 2(n).
[12] Oxford learner's Dictionaries, https://www.oxfordlearnersdictionaries.com/definition/american_english/information, (last visited Nov. 15, 2023).

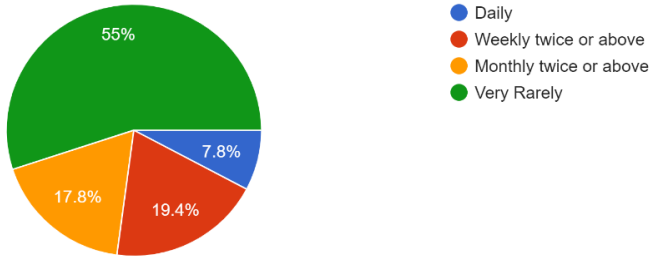
done on a digital personal data.[13] Such operations can either wholly be automated or partially automated. Processing also includes collection of such data, alignment and combination, storage, adaption, making available such data or restriction or erasure or destruction. During the process the tokenization the Token Requestor is collecting the data and processing it in such a manner that the collected data (actual card number) is stored with the card network and is replaced with the token. And the newly generated token is stored with the Token requestor for enabling payments.

From the above discussion it is clear that collection of card information and processing that information to create tokens can be treated as process of personal data under the DPDP Act, 2023. The process of tokenization was made mandatory by the RBI and thus it a processing of data for lawful purpose. Now if we look into the mode of consent which is required for processing the data, Section 6 of the Act states that *consent* given by the card holder (Data principal) should be *free, specific, informed, unconditional and unambiguous.* Such a consent from the data principal signifies that he is agreeing with the data fiduciary to process his personal data for that specified purpose. In case of Tokenization of cards, the card holders are giving consent by Additional factor Authentication without aware of the fact that they are consenting to tokenize their cards. The consent given by the card holder in such case may not be an informed consent. An informed consent is one when the person giving the consent is aware of the process for which he is giving his consent and with the available information he should be able to make a balanced judgment of whether or not choose that particular act.

A questionnaire was circulated among general public to check their awareness regarding tokenization. Around 200 people from various field participated in the survey which include students, employed and unemployed people. Out of which 91.5 % prefer Google Pay or any other UPI mode of payment method while very few opted for swiping cards in shops which was around 7.9%. While evaluating the frequency of device-based tokenization, 55% of public use cards swiping in shops very rarely. And around 20% of the survey participants use point of sale terminals for making payments weekly once or twice.

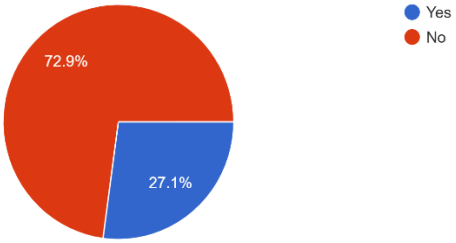
[13] Digital Data Protection Act, 2023; § 2(x).

Fig.1: Frequency of using point of sale terminals



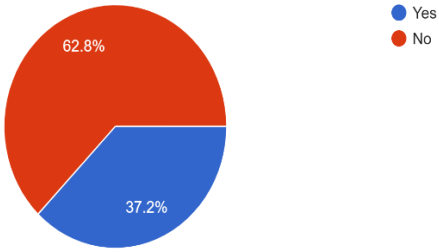
Even though the people participated uses both device based and mobile based payments around 72.9% of people are unaware of the process of tokenization, but at the same time 69% of people are aware of the card payment process.

Fig 2: Chart showing response for the awareness of tokenization processs



64.3% have noticed that the last 4 digits of their card number have been saved in the payment websites which they regularly use. Without knowing the process of tokenization around 62.7% of people gave consent for tokenization by entering OTP or clicking terms and conditions checkboxes during payments. 88.1% responded that they have not received any information from the bank with respect to tokenization.

Fig 3 showing majority of the people are unaware that entering OTP amounts to consent for tokenization



NPCI Tokenization System (Nts): National Payment Corporation of India (NCPI), an organisation established in the year 2008 by the combined efforts of RBI and Indian banks' Association, is responsible for smooth digital payments in our country. Unified Payments Interface (UPI), Bharath Interface for Money (BHIM), RuPay cards are some of the successful products owned

and operated by NPCI. It has introduced the NCPI Tokenization System (NTS) in 2021 which will enable the RuPay card to get tokenised. To become a Token Requestor any payment aggregator, merchant, acquiring banks or payments apps can get themselves certified with NTS to play the role of Token Requestor.[14] In India NTS is the predominant certification for the Token Requestor to render tokenization service.

If a Token Requestor is interested to participate in the BHIM UPI based payments, its system has to comply with the certifying criteria laid down by the NCPI BHIM. Any Third-Party Application Provider (TPAP) who wants to carry on the service of Token Requestor should get certification from the NCPI. A TPAP can be defined as a service provider to the Payment Service Providers (PSP) to enable payment successful by the user and a most prominent TPAP would be Google Pay (GPay) and Phone Pay. Further the TPAP is also taking the responsibility to ensure that their system is properly secured to function in the UPI platform. And in order to make sure its integrity it is under an obligation to follow and comply with various guidelines, laws, rules and regulations issued by the NCPI. It has been mandated by the NCPI to store the UPI related data of all the transactions done through a TPAP and also it cannot store such data outside India.[15] It has to make sure that such collected data is stored in a safe manner but at the same time it has to ensure that they can be accessed by the NCPI or RBI or their nominated agencies for the purpose of TPAP audits. A TPAP is not under an obligation to get approval from the RBI for rendering its service.

On the other hand, a Payment Service Provider (PSP) is an entity which is operating a payment system. PSP is a genre and TPAP is species. A PSP is generally a banking entity but any person can become a PSP upon getting certified and fulfilling the requisites. It will participate in the UPI by its own app or through a TPAP. But when same CUB is availing the service of Google Pay for enabling its customer's online payment, the Google pay is referred as a TPAP. A PSP is not only responsible for its own conduct but also under a pressure to make sure that systems of TPAP is complying with the appropriate rules and guidelines laid down by NCPI. Unlike TPAP, a PSP require authorisation from RBI to render services.

Quality Security Assessors (QSAs) authorised by the PCI Council will make annual testing and certifications for the TPAP. They will conduct system level security check, Network centre security check and risk tools analysis and provide Annual certification to the token Requestor who satisfies the testing criteria laid down by the PCI Council.

[14] NCPI, https://www.npci.org.in/PDF/npci/press-releases/2021/NPCI-Press-Release-NPCI-launches-NTS-platform-for-tokenization-of-RuPay.pdf , (last visited Nov. 15, 2023). NCPI launches NTS Platform for Card Tokenization.
[15] Roles and Responsibilities of TPAP, https://www.npci.org.in/what-we-do/upi/roles-responsibilities, (last visited Nov. 14, 2023)

A PIL was filed in 2020 before the High Court of Delhi by a financial economist Abhijit Mishra claiming that Google Pay acting as a PSP is violating the provisions of Payments and Settlements Act and is operating and providing payment services without getting authorisation from the RBI.[16] The petitioner has also accused the Google Pay for storing the Aadhar Card Information of Indian citizens without any authority and thus violating the Aadhar Act, 2016. Recently in August 2023 the Delhi High Court has finally dismissed the case by observing that *Goole Pay is mere third-party app provider which do not need authorisation from the RBI under the provisions of the Payment and Settlement Systems Act.* But when a similar contention was raised by PayPal in PayPal Payments Private Limited vs. Financial intelligence Unit India and Ors[17] the same Delhi High court has refused to hold the PayPal as TPAP. It has rejected the reliance made by the counsel on Abhijit Mishra vs. RBI & anr and decided against the petitioner and concluded it to be a Payment Service Provider (PSP). Thus, the line of difference lies in the nature of service provided and to whom and how it is provided.

10. CONCLUSION

This step of tokenization taken by the RBI is way towards more secure digital payments in the country. It has made the process much easier in comparison with the traditional encryption method. The responsibilities imposed upon the Token Requestor, merchants are coupled with severe penalties in the instances of contravention. Thus, it made the tokenization not a mere paper process but an actual reality. In addition to that yearly checking and certification process to ensure the safety of the payment system of the token requestor will enhance safety of the transactions on a periodical basis. However, the general public is not much aware of the process of tokenization and the fact that they are consenting to tokenize their card. This need to be redressed by creating more awareness about the process. RBI in this regard can mandate the issuing banks to communicate its card holder the details related to the tokenization of the cards. Recently, the Paytm has introduced the COFT facility and provided a flash advertisement in its app to make its users aware of the tokenization. Thus, tokenization as a process is a constructive step towards secure India's digital payments in its essence which need much more reach towards the layman.

[16] Business News, The Economic Times, https://economictimes.indiatimes.com/industry/banking/finance/gpay-does-not-need-rbi-authorisation-as-not-a-payment-system-operator-google-to-hc/articleshow/77108311.cms, (last visited Nov. 14, 2023)
[17] MANU/DE/4737/2023