KHAITAN & CO
ADVOCATES SINCE 1911

25 September 2024

Principle-Based Framework for Authentication of Digital Payments: A Step Towards Increasing Trust Towards Digital Payments

INTRODUCTION

The Reserve Bank of India (RBI) released the '*Draft Framework on Alternative Authentication Mechanisms for Digital Payment Transactions*' (Draft Framework) on 31 July 2024. The Draft Framework advocates the usage of Additional Factor of Authentication (AFA) for digital payment transactions by all Payment System Operators (PSO) and Payment System Participants (PSP). RBI in its 'Statement on Developmental and Regulatory Policy' dated 8 February 2024 had earlier announced adoption of a principle-based framework for authentication of digital payment transactions. The Draft Framework now sets clear guidelines for the authentication of digital payment transactions to bolster trust in digital payments ecosystem.

1. RISKS IN PAYMENT SYSTEMS

Digital payments in India have witnessed consistent growth year-on-year, with 13.46% increase in digital payments by value from June 2023 to June 2024, owing to the increasing penetration of internet and adoption of digital payment instruments. On the other hand, there has been 81.13% year-on-year frauds increase in domestic payments. Such frauds have necessitated the requirement for enabling strong authentication mechanisms to validate the credentials of the person originating or confirming a payment instruction.

The existing authentication factors have been susceptible to various commonly known security threats, such as:

(i) Phishing. Deceiving to click on fraudulent links posing as website of legitimate financial institutions and extracting usernames, PINs, passwords and such other private credentials.

(ii) Smishing. Similar to phishing, except that the fraudulent link is sent to the user through a text message. Such links may also download malwares on the user's device, which may be employed to extract the private credentials inputted / stored on the device.

(iii) Vishing. Fraudulent calls or voicemails soliciting personal information and private credentials.

(iv) Brute force attack. Hacking through trial and error to crack passwords or such other login credentials.

2. EXISTING FACTORS OF AUTHENTICATION

Username, password, PIN, One-Time-Passwords (OTP) etc. are the most commonly used factors for authentication of digital payments. OTP, a unique numeric / alphabetic / alpha-numeric PIN that is sent to the user for confirming a payment transaction, is the most commonly used factor. While OTP is dynamic in nature and negates the risk of the credential being leaked, it is still prone to phishing.

A Two-Factor Authentication (2FA) requires a combination of two separate factors to authenticate a payment. A typical example of 2FA is seen in Unified Payments Interface (UPI) where a user undertakes two layers of authentication, *viz.*, (i) authentication of the device at the time of setting up their UPI account on the user's particular mobile device through an SMS (device binding), and (ii) requiring the UPI PIN at the time of each payment. Thereby, the risk of fraud is minimised since a potential fraudster would require both SIM card (a physical identifier of the user), as well as the UPI PIN (a cognitive credential), to initiate a UPI transaction.

3. EXTANT REGULATORY FRAMEWORK

Currently, there are scattered regulatory stipulations on different regulated entities for authentication of payment instructions. The table below sets out the key requirements prescribed under the existing regulatory framework.

#	REGULATORY FRAMEWORK	REGULATED ENTITIES	KEY AUTHENTICATION REQUIREMENTS
1.	Master Directions on Prepaid Payment Instruments, 2021	Prepaid Payment Instrument (PPI) issuers	• Mandatory 2FA for any wallet transaction involving debit to wallet. • Same 2FA requirements as applicable to debit cards. • 2FA not mandatory for Gift PPIs and PPIs for Mass Transit Systems (PPI-MTS).
2.	Master Direction on Digital Payment Security Controls	Scheduled commercial banks, small finance banks, payments banks and credit card issuing NBFCs	• Mandatory multi-factor authentication for payments through electronic modes. • One of the authentication factors to be dynamic or non-replicable – recommended OTPs, device binding, biometric, hardware tokens, EMV chip cards, etc. • Risk based adaptive determination of authentication factor. • Alerts to be implemented for payment transactions. • Blocking of access to payment product / service after a set number of failed log-in or authentication attempts.
3.	Card transactions in Contactless mode - Relaxation in requirement of Additional Factor of Authentication	Scheduled commercial banks, cooperative banks, Non-bank PPI issuers, authorised card payment networks	• Relaxation of AFA requirement for card present contactless point-of-sale transactions (commonly known as 'tap & pay' or 'NFC' payments) up to transaction value of INR 5,000.
4.	Master Circular – Mobile Banking transactions in India – Operative Guidelines for Banks	Scheduled commercial banks and cooperative banks	• Mandatory 2FA for mobile banking. • One of the factors to be a generated mPIN or any higher standard; with mPIN recommended to be end-to-end encrypted. • Where phone number is not used as an identifier, separate login ID and password is recommended for authentication.
5.	Internet Banking Facility for Customers of Cooperative Banks	Cooperative banks	• Suitable security measures to be adopted for web applications. • Re-establishment of session after interruption shall require normal user authentication. • Recognition of three categories of factors (cognitive, tangible, and biometric). • Introduction of 2FA for internet banking – primarily a combination of password and OTPs.

4. KEY STIPULATIONS IN THE DRAFT FRAMEWORK.

The Draft Framework underscores the concerns in authenticating digital payments and providing for a uniform authentication framework applicable to all PSOs and PSPs. In case the Draft Framework is notified in its existing form, all PSPs and PSOs will be required to ensure compliance with the framework within 3 months from the date of issuance of the framework.

The Draft Framework prescribes the following notable stipulations:

(a) *Proposed definitions*.

Under the Draft Framework, Authentication is defined as '*the process of validating and confirming the credentials of the customer originating any payment instruction*'. Usage of more than one factor for authentication of a payment instruction is referred to as AFA. The definition of 'digital payment transaction' has been harmonised with the definition of 'electronic funds transfer' prescribed under the Payment and Settlement Systems Act 2007. Issuer is defined as '*the bank / non-bank where the customer's account is maintained and who verifies user credentials and provides confirmation of debit to the account on receipt of payment instruction*'.

(b) *Categorisation of factors of authentication*.

#	CATEGORY OF AUTHENTICATION FACTORS	EXAMPLES
1.	Something that the user knows (cognitive factor)	Password; PIN; security questions
2.	Something that the user has (tangible factor)	ATM card; smart card; device identifiers; software tokens
3.	Something that the user is (biometric factor)	Fingerprint; face ID; iris

(c) *Requirements for factors of authentication*.

The Draft Framework mandates AFA to be implemented for all digital payment transactions, except for certain exempted categories of digital payments (*as detailed below*). Additionally, one of the factors of authentication, other than for card present transactions, has to be (i) unique and dynamically created at the time of initiation of payment, which cannot be reused (like an OTP); and (ii) the first factor and the AFA has to mandatorily belong to separate categories of authentication factor.

(d) *Exempt transactions*.

In line with extant regulatory relaxations *vide* various notifications by the RBI, the following payment transactions are exempted from the AFA requirement under the Draft Framework as well:

(i) Small value contactless card payments. Card present transactions for values up to INR 5,000 per transaction in contactless mode at point-of-sale terminals.

(ii) E-mandates for recurring transactions. Subscription of mutual funds, payment of insurance premium, and credit card bill payments for values up to INR 1,00,000, and all other recurring transactions of values up to INR 15,000 (except for the first transaction, which shall require AFA).

(iii) Select PPI and National Electronic Toll Collection (NETC) payments. PPI-MTS, Gift PPIs and transactions in NETC system.

(iv) Small value digital payments in offline mode. Offline payment transactions up INR 500.

(e) *Obligations on Issuers*.

The responsibility of ensuring the effectiveness of the authentication mechanism is placed on Issuers and they shall assume liability for the process and technology adopted for authentication. Further, the Draft Framework imposes the following additional obligations on Issuers:

(i) Risk based implementation of AFA. Adopting a risk-based approach in determining the appropriate AFA to be implemented for a transaction. Such risk assessment shall be based on the risk profile of the customer and / or beneficiary, transaction value, payment origination channel, etc.

(ii) Payment Alerts. Alerting the customers on a near real-time basis for any digital payment transaction other than offline transactions of a value of up to INR 500.

(iii) Customer consent. Obtaining explicit customer consent prior to enabling any new factor of authentication for such customer. The Issuer must also provide the customer with a facility to deregister from using the new factor of authentication.

(iv) Third-party arrangements. Abstaining from any exclusivity arrangement with any payment / technology service provider, such that it limits the Issuer's ability to implement any alternative authentication mechanism.

COMMENTS

The Draft Framework provides clarity on baseline safeguards and practices for authentication of digital payments. While the onus is on the Issuers to implement appropriate authentication requirements on a risk-based approach, a standard threshold-based framework is not prescribed for such risk assessment. The key actionable for Issuers would therefore be implementing the appropriate AFA for its users having varying degree of awareness and technological savviness.

It would be also interesting to witness the implementation of the proposed requirements under the Draft Framework for devices with limited features (without face ID detectors, or fingerprint scanners). In such cases, device binding (tangible credential) along with PIN / OTP (cognitive credential) becomes the only viable form of AFA. However, device binding processes may not be feasible for payment interfaces that operate on a website (and not a native mobile application). Such operational challenges should be taken into account before notification of the Draft Framework in its final form.

Further, while a consent-based framework for implementation of authentication factors is user-centric; where users deny their consent to usage of biometrics, it may inevitably result in denial of service to the user even when the user may be willing to adopt a convenient combination such as password + OTP. This is because both passwords / PINs and OTP belong to the same category of factors of authentication. Such challenges also require careful consideration.

- *Smita Jha (Partner); Pritish Mishra (Principal Associate); Jino Mathews Raju (Associate) and Nayana J M (Associate)*

For any queries please contact: editors@khaitanco.com

AMBITION STATEMENT

"Our ambition is to be a respectable law firm providing efficient and courteous service, to act with fairness, integrity and diligence, to be socially responsible and to enjoy life. We should put greater emphasis on working in consonance with our aforesaid values than on maximizing earnings. Earn we should but with dignity and pleasure."

Khaitan & Co is a premier full-service Indian law firm with 25+ practice areas, over 1,000 lawyers, including 200+ partners. To know more about us, please visit www.khaitanco.com

KHAITAN & CO ADVOCATES SINCE 1911