

RBI Proposes Regulation for Safer Digital Payments

August 1, 2024 • vajiramandravi.com



What's in today's article?

- Why in the News?
- Authentication Process in Digital Payments
- What is Alternative Factor Authentication in Digital Transactions?
- News Summary

Why in the News?

- The RBI released a draft circular proposing an Alternative Factor Authentication for all transactions in a move to prioritize security of digital payments, according to its statement on July 31.

Authentication Process in Digital Payments

- Authentication in the context of digital payments is the process of verifying the identity of a user or the validity of a transaction to ensure security and prevent fraud.
- This process ensures that the person initiating the payment is authorized to do so and that the transaction is legitimate.

- **Basic Types of Authentication Methods for Digital Payments:**

- **Password-Based Authentication:** Users enter a unique password to confirm their identity.
- **PIN-Based Authentication:** Users enter a Personal Identification Number (PIN) to authorize transactions.
- **Biometric Authentication:** Utilizes unique biological characteristics such as fingerprints, facial recognition, or iris scans.
- **Two-Factor Authentication (2FA):** Combines two different methods of authentication, typically something the user knows (password) and something the user has (mobile device).
- **Usage:** Enhances security for online transactions and account access.
- **One-Time Password (OTP):** A temporary password generated for a single transaction or session, sent to the user's registered mobile number or email.
- **Token-Based Authentication:** Uses a hardware or software token to generate a unique code that the user must enter to authenticate.
- **Smart Card Authentication:** Involves the use of a smart card containing embedded integrated circuits to authenticate the user.
- **QR Code Authentication:** Users scan a QR code with their mobile device to authenticate and authorize payments.

What is Alternative Factor Authentication in Digital Transactions?

- Alternative Factor Authentication (AFA) refers to using unconventional or additional methods beyond the traditional authentication factors to verify the identity of a user in digital transactions.
- This approach enhances security by incorporating multiple layers of verification, making it more difficult for unauthorized users to gain access.

- **Types of AFA:**

- **Behavioural Biometrics:** Analyses patterns in user behaviour, such as typing speed, mouse movements, and navigation habits.
- **Device-Based Authentication:** Uses information about the device being used, such as its IP address, geolocation, and device ID.
- **Risk-Based Authentication:** Assesses the risk level of a transaction based on factors like transaction amount, location, and user behaviour.
- **Contextual Authentication:** Considers the context of the transaction, such as time of day, previous transaction history, and user preferences.
- **Push Notification Authentication:** Sends a push notification to a user's registered mobile device for transaction approval.
- **Voice Recognition:** Uses the user's unique voice patterns for authentication.
- **Email/SMS Verification Codes:** Sends a verification code to the user's registered email or phone number.
- **Geolocation Verification:** Uses the user's geographic location as an authentication factor.

- **Benefits of AFA:**

- **Enhanced Security:** By incorporating multiple and varied authentication factors, AFA significantly reduces the risk of unauthorized access and fraud.

- **Flexibility:** Provides users with various authentication options, improving the user experience.
- **Fraud Detection:** Helps in detecting fraudulent activities by analysing unusual patterns and behaviours.

News Summary

- On July 31, the **Reserve Bank of India (RBI)** released a **draft circular proposing Alternative Factor Authentication (AFA) for all digital transactions, emphasizing enhanced security for digital payments.**
- The draft outlines principles for authenticating digital payments, mandating an additional robust factor of authentication that must be dynamically generated and used only once.
- The type of **authentication factor will depend on various parameters, including the customer's risk profile and the transaction value.**
- The RBI also requires compulsory customer consent for introducing a new authentication factor, along with the option for customers to withdraw consent and deregister.
- Exemptions from this proposal include contactless card transactions below ₹5000, insurance premiums, credit card payments above ₹1,00,000, and other categories up to ₹15,000.

Stakeholders are invited to submit comments and feedback until September 15.

Q1. What is NPCI?

National Payments Corporation of India (NPCI) is an umbrella organization set up with the guidance & support of RBI & IBA for all retail payments in India.

Q2. When was UPI launched?

Unified Payments Interface, commonly referred to as UPI, is an Indian instant payment system as well as protocol developed by the National Payments Corporation of India in 2016. The interface facilitates inter-bank peer-to-peer and person-to-merchant transactions.

Source: [RBI proposes regulation for safer digital payments](#) | ET

Source: <https://vajiramandravi.com/current-affairs/rbi-proposes-regulation-for-safer-digital-payments/>

© Vajiram & Ravi. For personal use only.