ADVOCATES & SOLICITORS

AK & PARTNERS

Legal & Regulatory Advisors India

WHITEPAPER

PRINCIPLE-BASED FRAMEWORK FOR ALTERNATIVE AUTHENTICATION OF DIGITAL PAYMENTS IN INDIA

Office: +91 11 41727676

Mobile: +91 9560439503 | 8586074575

Email- anuroop@akandpartners.in.

C 18, Third Floor, LSC 1, C Block Market,
Vasant Vihar, New Delhi
110057

1. Background

The Reserve Bank of India (**RBI**) , in its Statement on Developmental and Regulatory Policy dated February 08, 2024, has noted how it has promoted the use of Additional Factor of Authentication (**AFA**). Although no specific method is prescribed, most industry players in India use an SMS-based One Time Password (**OTP**). However, RBI has noted how many alternative authentication methods have emerged for digital payments. RBI now proposes to issue a principle-based framework for the authentication of digital payment transactions. Since the release of the news, the market has been abuzz with anticipation of what these new regulatory guidelines shall entail and their implications for the digital payments ecosystem in India. Interestingly, the same RBI document also mentions how it aims to enhance the robustness of Adhaar Enabled Payment Systems (AePS), which also happens to be an alternative authentication mechanism. It will be interesting to see if Adhaar biometric-based authentication is allowed for payment transactions since this was disallowed by the Supreme Court in 2019.[1]

This whitepaper outlines what to expect from the guidelines for market preparation.

2. Rule-based vs. Principle-based vs. Risk-based approach

Rule-based approach	Principle-based approach	Risk-based approach
Prescribes in detail the do's and don'ts.	Broad principles and approaches is provided; implementation is left to market participants.	The regulator creates thresholds based on the risk perception of a regulated entity and prescribes a framework for risk management.
A regulated entity prepares a checklist of what is and is not allowed, reviews its existing processes and modifies accordingly.	A regulated entity prepares a flowchart mapping its stakeholders and the 'what if scenarios', defines vision, outlines options available, and chooses the option that meets the cost + risk mitigation criteria.	The regulated entity checks its position in the threshold and creates an internal risk management framework basis regulatory requirements + its own business model.
Focus on meeting exact requirements.	Focus on goals and outcomes rather than inputs	Focus on numbers and ratios
Tick box approach	Creative compliance	Financial compliance
Requires legal approach to compliance	Requires legal approach, which is techno-commercial	Requires financial approach to compliance
RBI Guidelines on Digital Lending and Outsourcing of IT and Financial Services	RBI Guidelines on Information Technology, Risk, Controls and Assurance Practices	RBI Scale-Based Regulations; Guidelines on Non-Performing Asset (NPA), Capital Adequacy, Income Recognition

[1] K.S. Puttaswamy (Aadhaar-5 J.) v. Union of India, (2019) 1 SCC 1

3. What to expect?

Framing of guiding principles that a Regulated Entity should bear in mind and prepare its internal policy

The RBI guidelines may provide key principles to be considered while adopting alternative authentication technologies. The most likely principles include consumer protection, safety and security, trust-based systems, and cost-effectiveness. This is similar to the RBI Fair Practice Code for lending in India. Based on these principles, the regulated entity may be required to adopt an internal policy for authentication methods offered and the perceived risk and advantage of the method through board resolution.

Due Diligence of Third-Party Vendor and Outsourcing Requirements

Since the policy aims to promote innovative alternative authentication methods, this is most likely to happen for regulated entities through the onboarding of fintech vendors who provide such authentication tools and products. Taking a leaf from the digital lending guidelines, requirements for vendor infosec due diligence and contractual requirements like business continuity plans and audit rights of subcontractors are likely.

Cards or Digital Payments?

Since the policy aims to promote digital payment innovation, the guidelines shall likely cover app-based payments and prepaid instruments but exclude debit card and credit card transactions.

Threshold and Classification

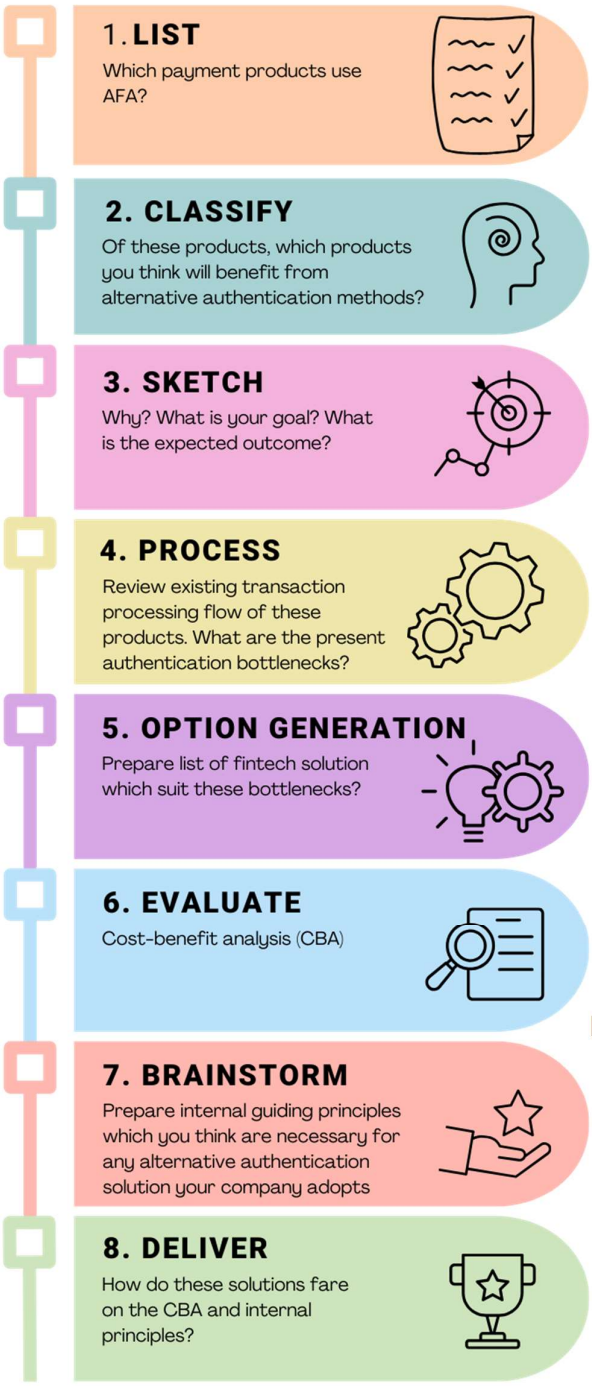
Similar to the existing Know Your Customer (KYC) Guidelines, it is likely that alternative authentication methods shall be made available to certain classifications of customers. For example, offline authentication processes may be allowed to customers who do not have access to the internet to promote financial inclusion. Similarly, different levels of security may be prescribed for different threshold values of transactions.

Mr Shaktikanta Das, Governor of RBI, at Payment System Operators (PSO) conference, Kochi, 18 March 2023

"Introduction of Additional Factor of Authentication (AFA) for card-based e-commerce and online transactions, which was later extended to other payment modes and channels, is a success story in Indian payment systems. Simple measures like provision of switch on / switch off facility for card transactions have positively impacted the trust of cardholders in digital payments. In all these initiatives, the Reserve Bank has kept customer convenience and safety as the prime objective... There have been instances in the past when companies which dominated their market segment have failed to anticipate winds of change and did not innovate on products and processes. Consequently, they have become almost extinct... At times, some PSOs display unwillingness to comply with regulatory instructions, citing various reasons like cost of carrying out system-level changes. In this digital age, there is a necessity to constantly upgrade the systems so as to remain relevant and increase efficiency. Legacy systems must be updated to bring them in line with changing realities. While any system may be presumed to be resilient and safe, a single bad experience of the customer with digital payments may drive him away to other channels or modes of payments. PSOs have a big responsibility here."

4. How to start preparing?

Implementing principle-based frameworks requires higher levels of preparedness for regulated entities. However, they also create greater legroom for product innovation and customer outreach. To make the most of the impending regulations, here are some of the things regulated entities can do to start preparing. For fintechs with product offerings, knowing how the regulated entity will map its risks and requirements is important to prepare the correct pitch.



Notice how we suggest preparing your internal principles only after talking to existing authentication service providers- those who are already innovating products in the market may be able to give you hands-on information on the present problems that products resolve any problems that their competitors do not resolve.

DISCLAIMER

This document is for general information purposes only. This document may contain copyrighted material on a fair-use basis. If you wish to use any copyrighted material from this update beyond 'fair use', please obtain permission from copyright owners. Please obtain customised, professional advice before using this information for business purposes.

FOR MORE INFORMATION, CONTACT US AT

Office: +91 11 41727676
Email- info@akandpartners.in.

C 18, Third Floor, LSC 1, C Block Market,
Vasant Vihar, New Delhi
110057