



भारतीय रिज़र्व बैंक  
RESERVE BANK OF INDIA

वेबसाइट : [www.rbi.org.in/hindi](http://www.rbi.org.in/hindi)

Website : [www.rbi.org.in](http://www.rbi.org.in)

ई-मेल/email : [helpdoc@rbi.org.in](mailto:helpdoc@rbi.org.in)



संचार विभाग, केंद्रीय कार्यालय, शहीद भगत सिंह मार्ग, फोर्ट, मुंबई - 400 001

Department of Communication, Central Office, Shahid Bhagat Singh Marg, Fort, Mumbai - 400 001 फोन/Phone: 022 - 2266 0502

July 31, 2024

## Draft Framework on Alternative Authentication Mechanisms for Digital Payment Transactions

Over the years, the Reserve Bank of India has prioritised security of digital payments, in particular the requirement of Additional Factor of Authentication (AFA) for making payments. No specific factor was mandated for authentication, but the digital payments ecosystem has primarily adopted SMS-based OTP as AFA. While OTP is working satisfactorily, technological advancements have made available alternative authentication mechanisms.

Therefore, as announced in the [Statement on Developmental and Regulatory Policies dated February 08, 2024](#), RBI has today released a draft "[Framework on Alternative Authentication Mechanisms for Digital Payment Transactions](#)" to enable the ecosystem to adopt alternative authentication mechanisms. This will widen the choice of authentication factors available to Payment System Operators and users.

Comments / feedback on the draft framework may be sent by [email](#) or by post to the Chief General Manager-in-Charge, Department of Payment and Settlement Systems, Reserve Bank of India, Central Office, 14th Floor, Shahid Bhagat Singh Marg, Mumbai-400001, **on or before September 15, 2024**.

Press Release: 2024-2025/809

(Puneet Pancholy)  
Chief General Manager



भुगतान और निपटान प्रणाली विभाग, केंद्रीय कार्यालय  
नीति प्रभाग

**DRAFT FRAMEWORK FOR COMMENTS**

CO.DPSS.POLC.No. S \*\*/ 02-14-015 / 2024-2025

Date of issue

All Payment System Providers and Payment System Participants (banks and non-banks)

Dear Sir / Madam,

**Framework on Alternative Authentication Mechanisms for Digital Payment Transactions - DRAFT**

Reserve Bank of India had mandated additional factor of authentication (AFA) for all transactions undertaken using cards, prepaid instruments and mobile banking channels. While no specific factor was mandated for authentication, the digital payments ecosystem has primarily adopted SMS-based OTP as AFA.

2. As announced in [Statement on Developmental and Regulatory Policies dated February 08, 2024](#), in order to enable the payments ecosystem to leverage the technological advancements and implement alternative authentication mechanisms, it has been decided to publish a **Framework on Alternative Authentication Mechanisms for Digital Payment Transactions**. The framework placed in [Annex](#) provides the broad principles which have to be complied with by all the participants in the payment chain while using various forms of authentication.

3. All Payment System Providers and Payment System Participants (banks and non-banks) shall ensure compliance with this framework within three months from the date of issue of these directions. These directions are issued under Section 18 read with Section 10(2) of the Payment and Settlement Systems (PSS) Act, 2007 (Act 51 of 2007).

Yours faithfully,

Chief General Manager-in-Charge

Encl.: Annex

**Framework on Alternative Authentication Mechanisms for Digital Payment  
Transactions - DRAFT**

**1. Applicability**

The framework applies to all Payment System Providers and Payment System Participants, as defined in Payment and Settlement Systems (PSS) Act, 2007.

**2. Definitions:**

In this framework, unless the context otherwise requires, the terms herein shall bear the meanings assigned to them below —

- a. **Additional Factor of Authentication (AFA):** Use of more than one factor for authentication of a payment instruction<sup>1</sup>.
- b. **Authentication:** Process of validating and confirming the credentials of the customer who is originating the payment instruction.
- c. **Card Present transaction:** A transaction that is carried out through the physical use of card at the point of transaction. It is also known as a face-to-face or proximity payment transaction.
- d. **Digital Payment Transaction** shall have the same meaning as “Electronic Funds Transfer” as defined in the Payment and Settlement Systems Act, 2007.
- e. **Factor of Authentication:** Any credential input by the customer which is verified for the purpose of confirming the originator of a payment instruction. The factors of authentication are broadly categorised as below:
  - i. Something the user knows (such as password, passphrase, PIN)
  - ii. Something the user has (such as card hardware or software token)
  - iii. Something the user is (such as fingerprint or any other form of biometrics)
- f. **Issuer:** Bank / non-bank where the customer’s account (deposit account / credit line or PPI balance) is maintained. Issuers verify user credentials and provide confirmation of debit to the account on receipt of payment instruction.
- g. **Technology Service Provider (TSP):** Provider of technology infrastructure adopted by the Issuer for implementing the authentication process. In addition to software-

---

<sup>1</sup> As defined in section 2(g) of PSS Act, 2007

based solution providers, this will include device manufacturers and hardware solution providers who provide such technology.

- h. **Token Service Provider:** An entity which tokenises the card credentials and de-tokenises them, whenever required. It includes card networks and card issuers.

### **3. Principles for authentication of Digital Payment Transactions:**

The technology and process deployed for authenticating a payment instruction by the Payment System Provider / Payment System Participant(s)<sup>2</sup> shall comply with the following principles:

#### **a. Mandatory additional factor of authentication:**

All digital payment transactions shall be authenticated with an additional factor(s) of authentication (AFA), unless exempted otherwise in this framework.

#### **b. Dynamically created:**

All digital payment transactions, other than card present transactions, shall ensure that one of the factors of authentication is **dynamically created**, i.e., the factor is generated after initiation of payment, is specific to the transaction and cannot be reused.

#### **c. Robust:**

The first factor of authentication and the AFA shall be from different categories, as defined in para 2(e) of this framework.

#### **d. Risk based approach to authentication:**

Issuers may adopt a risk-based approach in deciding the appropriate AFA for a transaction, based on the risk profile of the customer and / or beneficiary, transaction value, channel of origination, etc.

#### **e. Transaction Alerts:**

Issuers shall have a system of alerting the customer in near real time for all eligible<sup>3</sup> digital payment transactions.

#### **f. Customer consent:**

Issuers shall obtain explicit consent before enabling any new<sup>4</sup> factor of authentication for

---

<sup>2</sup> Payment System Provider and Payment System Participant will have the same meaning as defined under Payment and Settlement Systems Act, 2007

<sup>3</sup> All digital payment transactions except [small offline transactions](#)

<sup>4</sup> Introduced by the issuer after issuance of this circular.

the customer. The customer shall also be provided a facility to deregister from using the new factor of authentication.

**g. Responsibility of the issuer:**

- i. Issuer shall ensure the robustness and integrity of the process or technology of the authentication factor before deploying the same.
- ii. Issuer shall be liable for the process and technology deployed for authenticating a digital payment transaction.

**h. Third-party arrangements:**

- i. Issuer shall not enter into any exclusivity arrangement with any Payment Service Provider / Technology Service Provider - which could limit its ability to deploy alternative authentication solutions.
- ii. For transactions involving tokenised cards on various devices in line with RBI directions on [“Tokenisation – Card Transactions” dated January 8, 2019](#), as amended from time to time, Issuer / Token Service Provider shall ensure that the device environment supports tokenisation on a non-exclusive basis.

**4. Exemptions from customer authentication:**

The following are exempted from the AFA requirement:

**a. Small value contactless card payments:**

Small value card present transactions for values upto ₹5000/- per transaction in contactless mode at Point of Sale (PoS) terminals. (Reference: [DPSS.CO.PD.No.2163/02.14.003/2014-2015 dated May 14, 2015](#) and [DPSS.CO.PD No.752/02.14.003/2020-21 dated December 04, 2020](#))

**b. E-mandates for recurring (other than the first) transactions:**

Transactions in respect of: a) subscription to mutual funds; b) payment of insurance premium and c) credit card bill payments, for values upto ₹1,00,000, and in respect of all other categories, for values upto ₹15,000/-. (Reference: [CO.DPSS.POLC.No.S-882/02.14.003/2023-24 dated December 12, 2023](#) and other related circulars issued by RBI on “Processing of e-mandates for recurring transactions”)

**c. Utility through select Prepaid Instruments / NETC:**

The following categories of instruments/systems:

- i. Prepaid Instruments (PPIs) issued under PPI – Mass Transit Service and Gift PPIs. (Reference: [CO.DPSS.POLC.No.S-479/02.14.006/2021-22 dated August 27, 2021](#)).
- ii. Transactions in the National Electronic Toll Collection (NETC) System (Reference: [DPSS.CO.PD No.1227/02.31.001/2019-20 dated December 30, 2019](#)).

**d. Small value digital payments in offline mode:**

Offline payment transactions up to a value of ₹500/-. (Reference: [CO.DPSS.POLC.No.S1264/02-14-003/2021-2022 dated January 03, 2022](#)).

5. This framework consolidates the authentication related directions issued by the Reserve Bank, from to time, as listed in [Appendix](#).

\*\*\*\*\*

## Appendix

(Reference: CO.DPSS.POLC.No. S \*\*/02-14-015 / 2024-2025 dated \*\*\*\* \*\*, \*\*\*\*)

No	Circular No.	Date	Subject
1.	<a href="#">RBI / DPSS No. 1501 / 02.14.003 / 2008-2009</a>	February 18, 2009	Credit/Debit Card transactions-Security Issues and Risk mitigation measures
2.	<a href="#">RBI / DPSS No. 2303 / 02.14.003 / 2009-2010</a>	April 23, 2010	Credit/Debit Card transactions-Security Issues and Risk mitigation measures for IVR transactions
3.	<a href="#">RBI / DPSS No.914/02.14.003/2010-2011</a>	October 25, 2010	Credit/Debit Card transactions-Security Issues and Risk mitigation measures for Card Not Present Transactions
4.	<a href="#">DPSS.CO.No.1503/02.14.003/2010-2011</a>	December 31, 2010	Security Issues and Risk mitigation measures related to Card Not present transactions
5.	<a href="#">DPSS.CO.PD 2224/02.14.003/2010-2011</a>	March 29, 2011	Security Issues and Risk mitigation measures - Online alerts to the cardholder for usage of credit/debit cards
6.	<a href="#">DPSS.PD.CO. No.223/02.14.003/2011-2012</a>	August 04, 2011	Security Issues and Risk mitigation measures related to Card Not Present (CNP) transactions
7.	<a href="#">DPSS.PD.CO.No.513/02.14.003/2011-2012</a>	September 22, 2011	Security Issues and Risk mitigation measures related to Card Present (CP) transactions
8.	DPSS.CO.PD.No.1910/02.14.003/2011-12	April 17, 2012	Security Issues and Risk mitigation measures related to Card Present (CP) transactions
9.	<a href="#">DPSS (CO) PD No.2377/02.14.003/2012-13</a>	June 24, 2013	Security and Risk Mitigation Measures for Card Present and Electronic Payment Transactions
10.	<a href="#">DPSS (CO) PD No.719/02.14.011/2013-14</a>	September 27, 2013	Security and Risk Mitigation Measures for Card Present Transactions
11.	<a href="#">DPSS (CO) PD No.1164/02.14.003/2013-14</a>	November 26, 2013	Security and Risk Mitigation Measures for Card Present Transactions
12.	<a href="#">DPSS.PD.CO. No.371/02.14.003/2014-2015</a>	August 22, 2014	Security Issues and Risk mitigation measures related to Card Not Present (CNP) transactions
13.	<a href="#">DPSS.CO.PD.No.2163/02.14.003/2014-2015</a>	May 14, 2015	Card Payments – Relaxation in requirement of Additional Factor of Authentication for small value card present transactions
14.	<a href="#">DPSS.CO.PD.No.448/02.14.003/2015-16</a>	August 27, 2015	Security and Risk Mitigation Measures for Card Present and Electronic Payment Transactions – Issuance of EMV Chip and PIN Cards
15.	<a href="#">DPSS.CO.PD.No.2895/02.10.002/2015-2016</a>	May 26, 2016	ATMs - Security and Risk Mitigation Measures for Card Present (CP) Transactions

16.	<a href="#">DPSS.CO.PD.Mobile Banking.No./2/02.23.001/2016-2017</a>	July 14, 2016	Mobile Banking circular
17.	<a href="#">DPSS.CO.PD No.812/02.14.003/2016-17</a>	September 15, 2016	Security and Risk Mitigation Measures for Card Present and Electronic Payment Transactions – Issuance of EMV Chip and PIN Cards
18.	<a href="#">DPSS.CO.PDNo.1431/02.14.003/2016-17</a>	December 06, 2016	Card Not Present transactions – Relaxation in Additional Factor of Authentication for payments upto ₹2,000/- for card network provided authentication solutions
19.	<a href="#">DPSS.CO.PD No.752/02.14.003/2020-21</a>	December 04, 2020	Card transactions in Contactless mode - Relaxation in requirement of Additional Factor of Authentication
20.	<a href="#">CO.DPSS.POLC.No.S479/02.14.006/2021-22</a>	August 27, 2021	Master Directions on Pre-paid Payment Instruments
21.	<a href="#">DPSS.CO.PD.No.1810/02.14.008/2019-20</a>	March 17, 2020	Para 12.3 of Guidelines on Payment Aggregators (PAs)