Technical Specification for TSP Empanelment

Version 1.1

Document History

Date	Version	Description
20th May 2021	1.0	Base version of TSP Empanelment – Technical Standards
3rd Feb 2022	1.1	Production and Non-production connectivity models included.

Contents

1. Overview

- Bharat Bill Payment System is a unified recurring payment platform for India under the umbrella of NPCI Bharat BillPay Limited (NBBL), a fully owned subsidiary of National Payments Corporation of India (NPCI).

. Bharat Bill Payment System intends to offer interoperable and accessible recurring payment services to customers through digital and retail assisted channels enabling multiple payment modes, and providing instant confirmation of payment.

2. About this Document

2.1 TSP Definition

Technology Service Providers are entities that provide the below services to authorised entities like BBPCU, BBPOUs and other partners in the BBPS ecosystem from time to time

- Development and backend technical Support
- Enable in boarding new Billers/Merchants etc.
- Enabling channel integration/platform integration
- Enable new category developments and enhancements
- Enable new use cases and manage COU/BOU site
- New Innovation and features etc.

2.1 Purpose

This document will act as a standard operating procedure for technical service providers (TSP) to set up their systems with respect to Bharat Bill Payment Central Unit (BBPCU), get connected to BBPCU, execute the functionalities of TSP and be part of the Bharat BillPay Ecosystem.

This document sets out a broad approach to designing systems that will be setup or developed by different TSP's. It attempts to set general standards and create a consistent approach to the design and development of systems across the Bharat BillPay Ecosystem.

2.2 Scope

This document is applicable to technology service providers (TSP) providing application, infrastructure and other auxiliary services. Under this framework, following activities are covered & explained in detail in the subsequent sections:

- Eligibility Criteria
- TSP Certification
- On-boarding Standards
- Infrastructure Management
- Cryptographic Protections
- Data Management
- Security Management
- Risk Management
- Compliance Management

This shall enable standardization to the assessments that will be carried out by ecosystem partners to maintain high levels of security compliance with respect to the BBPS ecosystem. It is important to put safeguards in place so as to have right balance of Performance, Scalability and Availability.

This framework is applicable to Technology service providers for their participation through the regulated entities.

3. Eligibility Criteria

- Should be an Indian Company registered under appropriate Indian Companies Act.
- Should have minimum one-year experience is providing payment & technology solutions i.e., payment gateways, transaction processing platforms, CBS platforms etc.
- Should have a relevant corporate documentation for e.g. PAN/GST/ROC certificates etc.
- Should be compliant with all relevant provisions of regulation and law with regard to privacy, InfoSec, data localisation etc.
- Should be compliant with regard to the entire TSP Technical Standards and any such framework defined by BBPCU
- Any entity that fails to fulfil the above criteria's would not be eligible for certification/empanelment process

4. TSP Certification

4.1 Certification Types

A TSP can get certified in the following ways

A. Directly on the BBPS platform without a BBPOU
B. BBPS platform with a BBPOU

The following sections covers the types of certification in its entirety below.

4.1.1 Base Certification (COU, BOU, Both)

TSP will go through certification process for the first time in BBPS or when a BBPOU comes with a new TSP/In-house development.

4.1.2 Enhancement Certification (COU, BOU, Both)

The TSP & its BBPOU must undergo certification/s for any new enhancements or any new features included/implemented in BBPCU
The TSP can also test independently or undergo certification for any new enhancements or features

4.1.3 Add-on Channel Certification (COU)

BBPOU & TSP will come under ADD ON certification process for conditions delineated below:

- BBPOU in relation with the same TSP but for a different channel certification.

4.1.4 Recertification (COU, BOU, Both)

BBPOU & TSP will require recertification when the TSP with its respective BBPOU has not gone live in Production after completing certification for more than 6 months or has not completed relevant feature/enhancements within the stipulated timelines.

4.1.5 Others (BOU, Both)

The Biller OU and TSP would go under certification process for the below scenarios BBPOU selecting a different TSP for on-boarding multiple biller categories/ billers for Biller OU certification, the TSP and the BBPOU cannot both be the default OUs for the same biller, hence, where TSP is the default OU for a biller, the BBPOU cannot be default OU and vice versa. The relevant BBPS standards and circulars with regard to the BOU and TSP would be applicable.

4.1.6 Certification Environments

There are three stages that would be involved to complete the BBPS certification process, namely:

- **Sandbox Test:** To verify the necessary testing requirements like below.
- **Comfort Test:** To test and verify the possible structural / logical and compliance parameters
- **UAT:** To certify before integrating into the production line.

4.2 Validity

Once the TSP is successfully certified, it is valid for either up to one year or till any major changes done in the respective TSP application. During this period, TSP has to get on-boarded by directly doing UAT in case applicable.

4.3 Certification Mandates

TSP/BBPOUs must connect only from their certified environment to BBPCU certified environments – Sandbox, Comfort and UAT environment.

4.4 API Testing in Certification Environment

BBPS APIs given on the below path would be tested under certification environment, any enhancements or additional features/functions to be tested would be informed from time to time in the form of Circulars/Advisories
Link for BBPS APIs on BBPS Website:
https://www.bharatbillpay.com/images/library/circular/pdf/BBPS-API-Specifications-v14.0.pdf

5. On-boarding Standards & Documents

The key standards with regard to on-boarding of TSPs has been delineated below. Due consideration should be given to mitigating the possible reputational, legal and operational risks and ensuring that customer interests are not compromised in any manner.

- TSP can connect directly or through a BBPOUs infrastructure to ensure that it is capable of complying with various BBPS requirements, procedural guidelines, circulars and standards published from time to time

- There has to be a contractual agreement between the BBPOU and the TSP (based on BBPOUs internal best practices and requirements) including undertaking by the

TSP for compliance of the BBPS Procedural Guidelines, Standards, Circulars and any other guidelines in this regard

- The TSP while connecting directly on NPCI Net will have to submit a Terms & Conditions document as per standard format specified by BBPCU-(Annexure-I delineates the Terms and conditions document to be signed by TSP).

- In case the TSP to liaison with any of the BBPOU for any certification/ channel enablement, features enablement or any new enhancements then the BBPOU must submit a TSP Consent Form as Annexure II

- TSPs must comply with the BBPS System Audit Framework standards and relevant guidelines from time to time.

- TSP must also follow the Internal Infrastructure Security Audit scope as delineated in Annexure-III

The above standards for participating entities can be reviewed and revised by NBBL from time to time and such revisions will be binding on participants to whom the standards apply.

6. Gradation of TSP

TSP will be graded based on the estimated number of transactions to be processed per day at the time of empanelment. Transaction processed is inclusive of both fetch and payment transactions.

Transaction Processed per day (in Lakhs)	**Grade Level**	**Minimum Bandwidth Required**
0 <= 10L	1	8 MBps
10L & above	2	16 MBps

Based on the Grade level, appropriate network bandwidth needs to be provisioned.

Types of TSPs

- TSP for BBPOU applications (COU/BOU or Both)
- TSP for Non-BBPOU applications (TSPs who want to test new features/enhancements and offer the new use cases BBPOUs)

7. Infrastructure Management (Connectivity to NPCI Net)

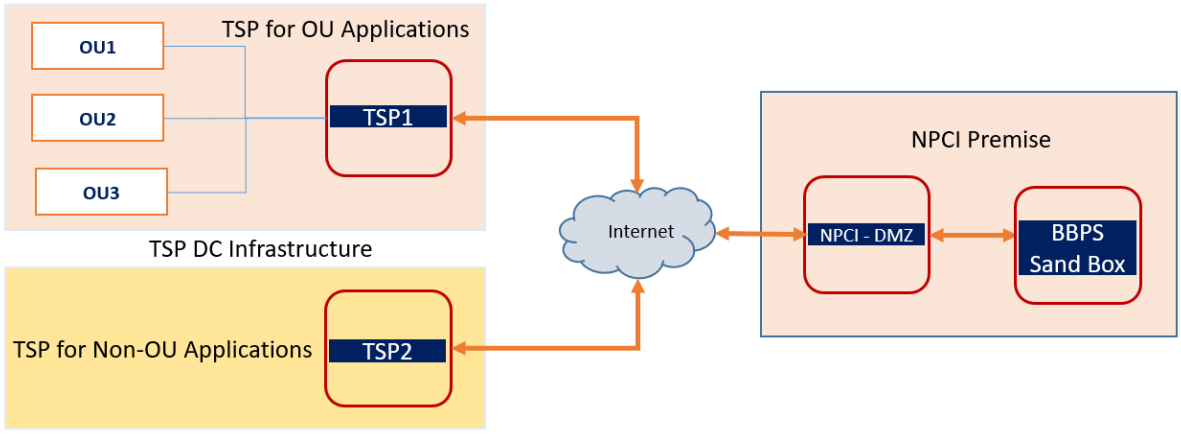
The TSP can connect to NPCI Net by following 3 ways

A. Pre-production Environment (Certification Environment) – Internet/MPLS network
B. Production Live Environment – MPLS Network

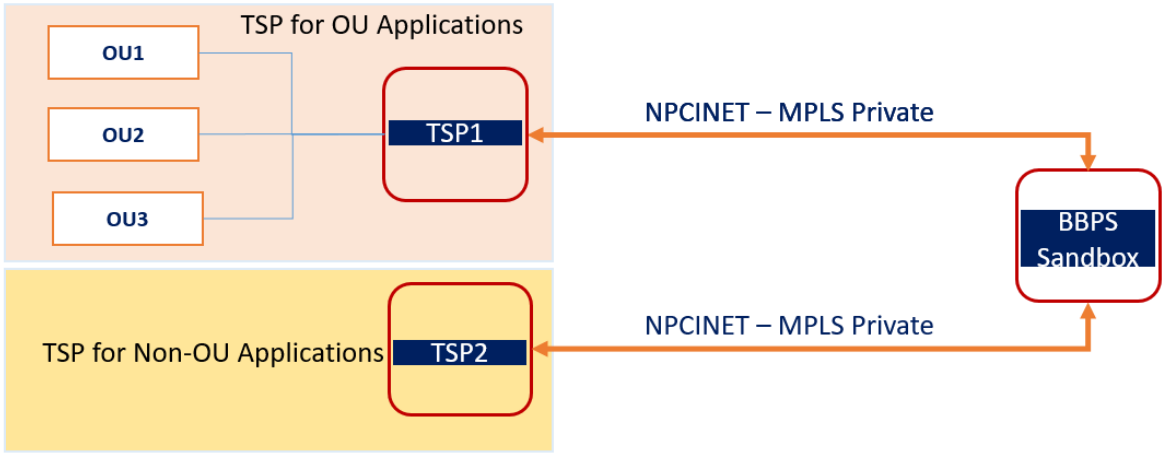
7.1 Pre-production Connectivity Methods (Certification Environment)

TSP connectivity for BBPS Certification environment would be using Internet/MPLS connected as depicted below, by SSL encryption

Pre-Production using Internet Connection



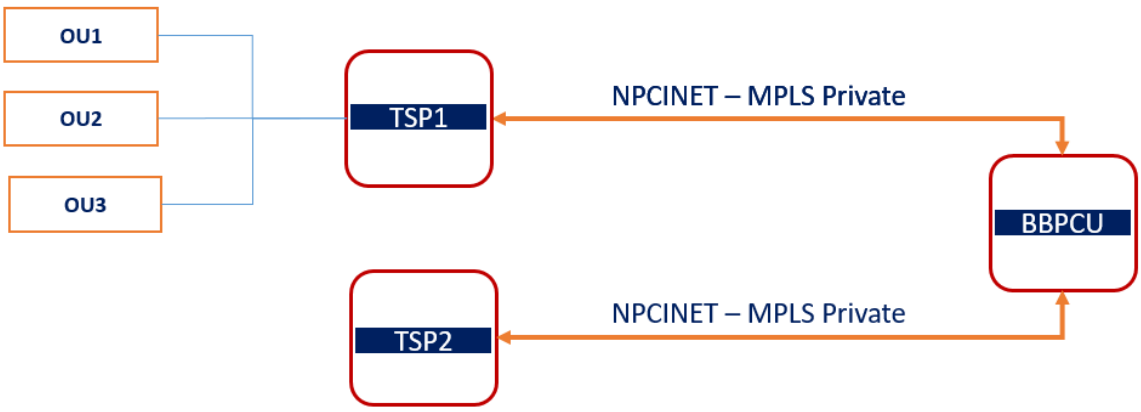
Pre-Production using MPLS for TSPs currently on NPCI Net



7.2 Production Connectivity

TSP connectivity for Production environment would be using NPCI Net via MPLS Private connection as highlighted below

Production using MPLS



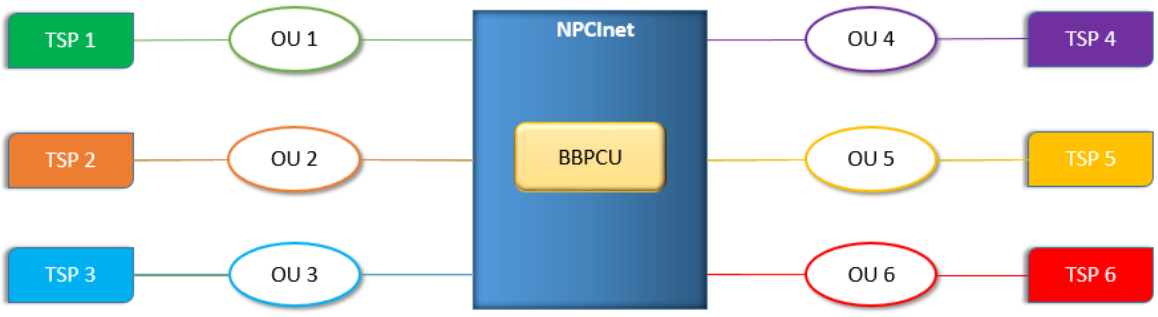
7.3 TSP Models

The below section highlights the various models currently existing and planned for future as a part of empanelment.

The flows represented below are of illustrative nature and a BBPOU can connect to multiple TSPs by adhering to BBPS guidelines, circulars, standards etc.

7.3.1 Case I - TSP services to BBPOUs

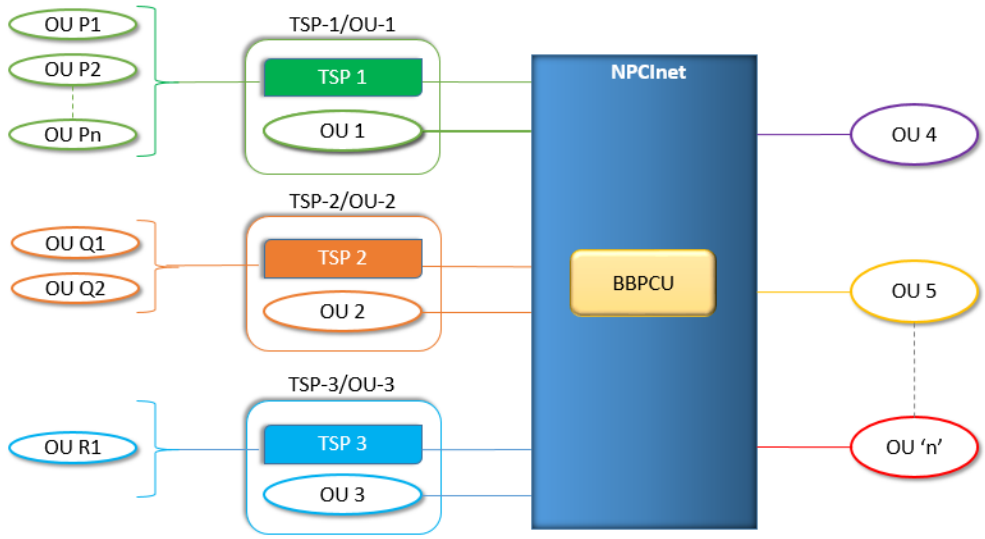
TSP/s provide application support/technical support to the Bharat Bill Payment Operating Units (BBPOUs-direct participants authorised by RBI) & transactions are routed to BBPOU Network to NPCI NET.



In this case, empanelment of the TSP is voluntary and the BBPOU and TSP must confirm the architecture and routing to BBPCU.

7.3.2 Case II – BBPOU acting as TSP

- Before BBPS came into existence, some of the entities used to manage the entire application and connectivity of the BBPOUs (majorly banks) & now these entities who have received license from RBI as BBPOU and are also providing TSP services to other BBPOUs for BBPS.
- Herein the TSP acts on behalf of the BBPOU who connects to the NPCI network directly and the billers/merchants on the other side as a BBPOU from their environment.
- In this instance the TSP hosts and connects and also originates the transactions, maintains the data of its client BBPOUs as well.

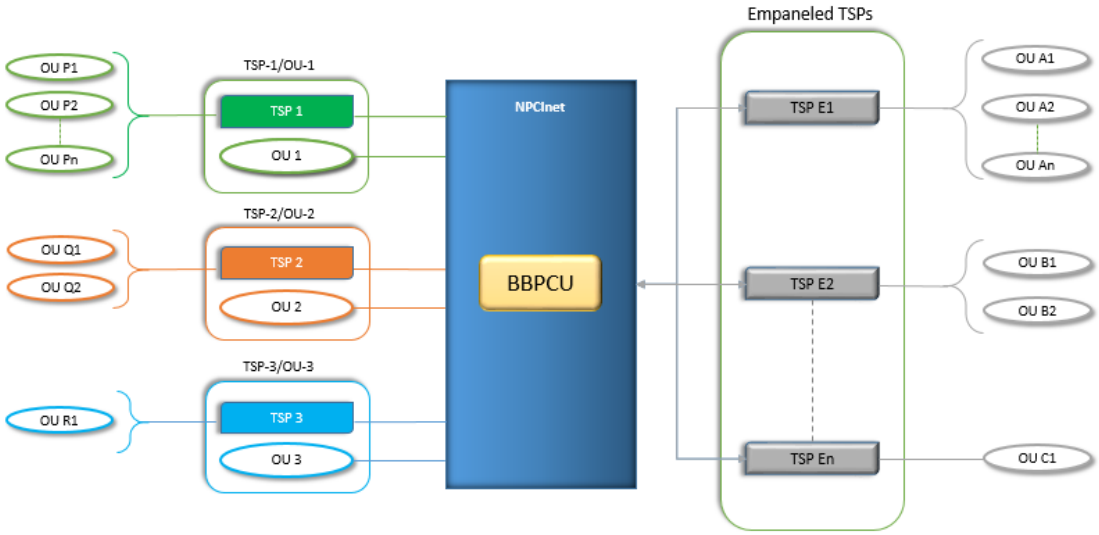


OU P1 = BBPOU1 having direct tie up with TSP1
OU P2 = BBPOU2 having direct tie up with TSP1
OU Q1 = BBPOU having direct tie up with TSP2
OU1 = BBPOU acting as TSP for multiple BBPOUs i.e. OU P1, OU P2 etc.

In this case, the TSP must get empaneled on NPCI Net.

7.3.3 Case III – Multiple TSPs empaneled through NPCINET

- Broad base TSPs having direct NPCI Net access and enable us to create a panel of TSPs who will be certified by NPCI as those who are technically competent and also BBPCU will facilitate implementation of enhancements which will benefit the entire ecosystem.



7.4 TSP Connectivity Mandates

- The TSPs will have to adhere to all the techno operational standards like infrastructure, bandwidth, downtime, TPS, scheme, circulars, enhancements etc.
- We will display the list of the TSPs who are empanelled with NPCI BBPS (and their specialisation) on Bharat Bill Pay and NPCI website.
- The TSPs who will be desirous of empanelment will sign a Terms and Conditions document for adherence to NBBL terms and conditions on scheme compliance, indemnification, etc.
- The empanelment would be applicable for the below
    - New TSPs desirous of direct connectivity
    - existing entities acting as TSPs with direct connectivity
    - existing entities with direct connectivity
- Must have separate infrastructure for OU and TSP not limited to
    - Applications, Servers and Network devices
    - ISP Links
- No interconnectivity must exist between the BBPOUs Managed by the same TSPs
- Connectivity between OUs must happen through BBPCU
- TSP development, Certification and Production environment should be separate for each managed OUs.
- BBPCU reserves the right to direct OU to move to different TSP, if any TSP fails to comply with mandatory requirements.
- Scheduled downtimes may be planned during 2nd or 4th Saturdays in between 02:00 to 04:00 AM IST.
- TSP's Technical, IT and Network teams should be made available during the entire course of such a scheduled downtime for verifications prior to commencement of the scheduled window and after completion of the scheduled window.

7.5 Network bandwidth

Typically, a TSP would need adequate bandwidth infrastructure to connect and communicate with BBPCU. As baseline standard, TSP should cater for a minimum 8 Mbps link to begin with

per OU in production environment. The bandwidth will be upgraded in proportion to estimated increase in TPS.

Usage of network bandwidth will be monitored continuously and the TSP will be advised to upgrade their bandwidth once the usage crosses threshold limits. SD-WAN solution must be implemented for increased throughput and optimum utilisation of network links (i.e. Primary and Secondary links).

7.6 Network IP and Port details

BBPCU SPOC will provide the IP and Port details on request while establishing connection with BBPCU. Similarly, TSP's should share their IP and Port details for integrating with different environments – Sandbox, Comfort, Certification, Production & DR (Disaster Recovery) sites.

- All TSP/BBPOUs have to ensure that for their application there is single bi-directional IP / Port irrespective of channels, role of BBPOU. Thus, for a BBPOU acting as both Customer and Biller BBPOU target IP has to be unique.
- IP and Port combination for all environments must be mutually exclusive.

7.7 Software Requirements

- BBPS does not mandate implementation of any specific software stack as long as they are capable of sending and receiving signed XML messages with BBPCU in the defined structure.

- The processing capacity of the application stack used must be benchmarked before on-boarding. And the application instance must be able to process minimum 250 TPS. The application performance benchmarking report must be shared with BBPCU for verification/validation.

7.1. Cryptographic Protections

The Bharat Bill Payment System will deal with the confidential information of the customers. It is thus imperative that the communication channel between the participants is secure and information flow takes place in most secure and encrypted format. Any breach in client confidentiality or data security can have a negative impact on the reputation of BBPS.

8.1 Data Security in Motion

BBPCU will only be able to communicate with TSP/BBPOUs that are part of BBPS Eco System.

During the transaction processing, when a message is getting transmitted between BBPOU and BBPCU, the TSPs must ensure that the data shared between them are encrypted and shared securely. The receiver of message needs assurance that the message has indeed been originated by the sender with public key of BBPCU TLS certificate and the latter should not be able to repudiate the origination of that message. This requirement is very crucial in BBPCU's secured processing environment with Private Key of BBPCU TLS certificate to obviate disputes over exchanged data.

Hence it has been decided to use the standard Digital signing to ensure the integrity. Digital signature is a cryptographic value that is calculated from the data and a secret key known only to the signer. Digital signature binds the BBPOU entity to the digital data. This binding can be independently verified by the receiving entity.

8.2 Digital Certificate

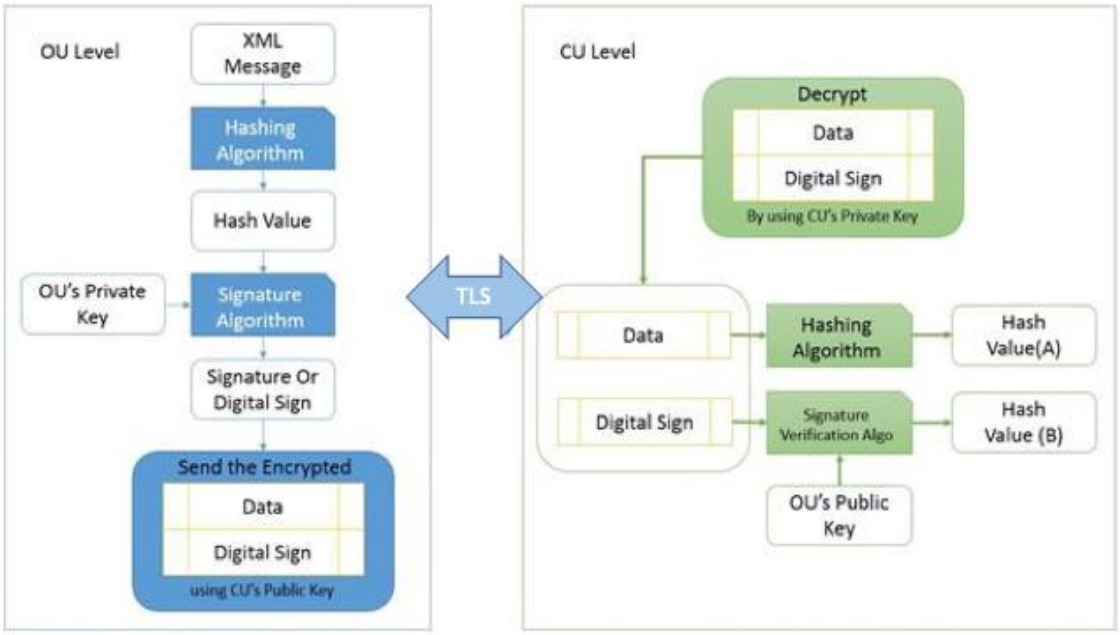
Digital certificates will be used to ensure the trustworthiness of public facing portals and websites of BBPCU. The digital certificate will contain a unique identifier for the entity, and also include the certificate authority that verifies the information contained in the certificate, date that the certificate is valid from and the date that the certificate expires.

As per requirements TSP empanelment needs two way SSL certificate and the payload has to be digitally signed using SHA2 and above algorithm with RSA (RSA 2048 bits' key) and the signature has to be embedded in the XML payload which will then be transmitted through a secure TLS channel.

8.3 Transport Layer Security (TLS)

- All REST API messages will be exchanged over minimum of TLS 1.2 and above standards.
- All file exchanges will be over HTTPS.
- All web pages will be exposed over HTTPS.
- All settlement files will be shared over HTTPS.
- The cipher suite selected by the server from the client's cipher suites and revealed in the Server Hello message is carried out during the TLS Handshake.

8.4 Message Security and Non-Repudiation



Note:

- SHA256 and above algorithm is used for hashing and 2-way TLS is followed using 2048-bit encryption.
- There should be no \n and \r formatting applied by the signature utility in the final XML file sent.
- TLS v1.2 is the minimum protocol for all API message exchanges.
- The TSP/OU's application should use minimum encryption/hashing standard by selecting AES256_SHA2 and above cipher suite during the TLS Handshake for receiving a request or response from BBPCU.

8.5 Data Security at Rest

- All sensitive data (data at rest) should be encrypted and stored. Minimum encryption and hashing standard of AES256_SHA2 and above must be used.
- All private keys should be stored preferably in HSM (FIPS 140-2 compliant device configuration).
- Public keys (certificates) to be stored securely in DB.

8. Data Management

9.1 Data Handling

- Accessing data from BBPCU can be done by authorized BBPOU after Appropriate level of authentication and authorization controls, that includes but not limited to Access control lists, role based access controls, central AD integration, TACACS, RSA, TOTP based Multifactor authentication.

- Data received and processed by the TSPs must be handled with utmost care. The data needs to processed and stored in a secure manner at TSP premise.
- All PII data received and processed must be classified and protection mechanism (Encryption) must be in place in accordance with the data classification.

9.2 Data Storage and Archival

- Transaction related data should be archived minimum for a period of at least 10 years.
- Complaints can be raised for transactions. So, transaction related to data one year from the date of a transaction should be made readily available by TSP at any given time for retrieval for raising complaints anywhere in the BBPS Eco system.
- The data stored in TSP/OU's databases should be secure, encrypted and in-line with the latest data security and data localization standards. Contractual agreement for no trans-border flow of data must be in place while opting for cloud-based solutions.
- Data should be stored within the jurisdiction of India

9.3 Data Privacy

- Customer Identity details (PII)., passed from Customer BBPOU to BBPCU should be masked (5 digits) before it is forwarded from BBPCU to Biller BBPOU E.g. Card Details, Account Number etc.
- Additional non-mandatory customer details like email, PAN card details passed from Customer BBPOU to BBPCU should be encrypted /Masked /hashed before sending if a Customer BBPOU wants to forward the same.
- For any Personally Identifiable information input by user and sent to BBPCU, TSP should have taken the consent from the BBPOU's.

9. Security Management

The below mentioned are minimum mandatory security requirements which shall be fulfilled by TSP at the time of connecting to BBPS and shall be always put in practice.

10.1 Application Security

- The participants must ensure that any form of code they share should be bare minimum obfuscated apart from incorporating additional runtime checks that can be added to the code.
- Application provided by TSP must be developed referencing common best practices in coding including but not limited to OWASP mobile Standards and other best practises of Secure Code development.

10.2 Infrastructure Security

- Vulnerability Assessment of the Servers (Web, App, DB, Operating System), networking and security devices that participated in the BBPS ecosystem hosted in TSP Premises every quarterly by a certified empanelled vendor.
- Black box penetration testing of the IT Servers, networking and security devices that participated in the BBPS ecosystem including applications that are exposed to Internet at least annually.

- Configuration Audit quarterly as per Centre for Internet Security (CIS) Benchmark for Servers, networking and security devices that participated in the BBPS ecosystem for all participants.
- TSP participating in BBPS must maintain connectivity of their network for the BBPS services on 24x7 basis with an uptime of not less than 99.99% yearly with similar DC and DR capacity for BCP .
- The sites must have dual Internet service provider links for redundancy.
- TSP should inform CU at least two weeks in advance for maintenance activity.
- TSP to cover the periodical changes and system enhancements within 60 days from the data of circular announcement from CU. Movement into Production environment should fall within the stipulated period with adequate testing and certification if any as appropriate.
- TPS must publish the performance and compliant status of their environment periodically on the website as CU does.

10. Risk Management

11.1 Fraud Risk Measures

- Every TSP shall be responsible to report any, fraud, cyber-attack or suspicious transaction immediately to csirt@npci.org.in and to managed BBPOU on daily basis.
- All TSPs should develop competencies to identify frauds through the usage patterns and taking appropriate measures to mitigate such risks.
- TSP/BBPOU in case of any major cyber-attack / fraud shall notify to NBBL and CERT-IN within 4 hrs of incident detection.
- Based on fraud investigation / analysis NPCI will notify impacted parties with the transaction details.

11. Compliance Management

It is imperative that sufficient due diligence must be exercised on an ongoing basis covering all aspects of the operations for various participants of BBPS.

- TSPs must comply with Mandatory standards – PCI DSS, ISO 27001 including but not limited to IT Act.
- The TSPs must carry out risk-focussed internal audits of their systems, operations, and comply with BBPS standards, BBPS Procedural Guidelines, RBI regulations and guidelines or any other guidelines in this regard.
- Internal Infrastructure security audit should be performed annually with reference to TOR System Audit framework by CERT-IN empanelled audit firms..
- TSP must submit the audit report to BBPCU immediately after audit. The report should mention critical observations, serious or persistent irregularities and non-compliance, and shortcomings of serious nature pointed that warrant immediate remedial measures.
- TSP would have **90 days** from the date of audit to close all the identified gaps. All closures MUST be revalidated by the same CERT-In empaneled auditor and the auditor must submit a Closure report with auditor comments. This closure report **MUST** be submitted by TSPs to BBPCU.

TSP must ensure that audit report and closure report is submitted to BBPCU within 45 days from the start of the next financial year.

- As mentioned in BBPS circulars, BBPCU may nominate, any other agency appointed by them to conduct audit with prior notice. The audit maybe conducted on an annual basis or as per the frequency decided by BBPCU. Prior intimation of 30 days would be given to the TSP.
- TSPs must be in compliance with the System Audit Framework document shared by BBPS.
- The TSP should put in place an effective internal audit programme to be carried out to audit their managed OU's for and their channels on similar lines with System Audit Framework.
- TSP must undertake system audits for their BBPOU to ensure that their Information Technology systems are protected from known, zero-day vulnerabilities arising out of hacking attempts, denial of service attacks. Adequate steps must be taken to ensure that the systems are able to maintain the transaction data integrity and the customer information confidential at all times.
- BBPCU reserves the right to call for internal Infrastructure Security audit report from the TSP.
- BBPCU reserves the right to audit TSP/ BBPOU with regards to the conduct of BBPS operations and compliance to PCI-DSS, ISO 27001 standards with prior intimation.
- In the event of non-compliance with the TSP Technical Standards, Procedural Guidelines, Circulars or any such guidelines released in this regard or any breach or violation identified as part of the Audit report, BBPCU reserves the right to impose penalty on the BBPOU or its respective TSP with prior intimation.
- BBPCU also reserves the right to temporarily or permanently suspend the Certification given to a certain TSP in case the TSP doesn't adhere with the norms, technical standards or any such guidelines in this regard
-
- Following would be the structure of Penalties in case of non-compliance with respect to Audit Reports

Sr. No.	Scenario	Action to be taken
1	TSP not submitting any audit reports in a year	a. NBBL will send letter to TSP's senior management team with regard to failure in submission of report (equivalent to Chief Technology Officer or Chief Operating Officer or above). b. Actions as per Sr no.3 and/or 4 whichever applicable.
2	TSP not able to close all gaps and submit closure report within 90 days from submission of audit report.	NBBL will send letter to TSP's senior management team with regard to failure in submission of report (equivalent to Chief Technology Officer or Chief Operating Officer or above).
3	TSP exceeding closure timelines by 60 days.	Penalty of INR 1,00,000 per month
4	TSP exceeding closure timelines by 90 days.	Suspend certification and stop new on-boarding of any BBPOU and stop catering to any BBPOU for new features, enhancements etc.

12. List of Abbreviations

API	Application Program Interface
BBPCU	Bharat Bill Payment Central Unit
BBPOU	Bharat Bill Payment Operating Unit
BBPBOU	Bharat Bill Payment Biller Operating Unit
BBPS	Bharat Bill Payment System
CA	Certificate Authority
DB	Database
FIPS	Federal Information Processing Standards
HSM	Hardware Security Module
HTTPS	Hypertext Transfer Protocol Secure
ID	Identity
IP	Internet Protocol
ISO	International Organization for Standardization
Mbps	Mega Bits Per Second
NBBL	National Bharat Bill Pay Limited
NPCI	National Payments Corporation of India
PAN	Permanent Account Number
PCI-DSS	Payment Card Industry Data Security Standard
PII	Personal Identification Information
RBI	Reserve Bank of India
REST	Representational State Transfer
RSA	Rivest, Shamir, and Adelman
SHA2	Secure Hash Algorithm 2
TCP / IP	Transmission Control Protocol / Internet Protocol
TSP	Technical Solution Provider
TLS	Transport Layer Security
TPS	Transactions Per Second
URL	Uniform Resource Locator
XML	Extensible Mark-up Language
XSD	XML Schema Definition

ANNEXURE I

TECHNICAL SERVICE PROVIDER (TSP) CONSENT/UNDERTAKING FORM

(On BBPOUs letter Head)

To

The SBU Head,
Bharat Bill Payment System (BBPS),
National Payments Corporation of India,
Unit 302, 3rd Floor, Raheja Titanium
Off Western Express Highway
Goregaon-East, Mumbai-400 063

Dear Sir,

1. We_____ (Name of the BBPOU) __;_pursuant to the _____ Agreement dated _____ with National Payments Corporation of India (NPCI), have agreed to participate in the Bharat Bill Payment System (BBPS) under Bharat Bill Payment Central Unit (BBPCU) and in the said context:

   We hereby appoint and authorise *<name of TSP/s>*___, having its registered office situated at _____, ("**TSP**") to act as our Technical Service Provider for our _____*<<Consumer Bharat Bill Payment Operating Unit (BBPOU) or/and Biller BBPOU certification>>* in compliance with circulars/guidelines issued by Reserve Bank of India ("RBI") and NPCI, from time to time, for all transactions across all payment modes and channels.

2. We agree and confirm that any addition of TSP(s) shall be intimated to BBPCU for initiation of Re-certification, at our costs and expenses.

3. We hereby agree and consent that all complaints relating to processed transactions received by BBPCU or us (Customer side BBPOUs) or any consumer would be attended to expeditiously by us and all possible help will be provided in this regard.

4. We consent and agree that TSP will be our responsibility and we ensure that such TSP adheres to and complies with the circulars/guidelines issued by RBI/NPCI from time to time.

5. We hereby agree that all data pertaining to Bharat Bill Payment System would be shared with RBI and NPCI/BBPCU from time to time by the TSP, if required

6. We further consent, undertake and confirm that BBPS service is provided by NPCI on an 'as-is' basis, and notwithstanding anything contained herein above, we shall indemnify and keep indemnified NPCI, from any and all claims, losses, expenses, damages, liabilities (including any investigative, legal and other expenses incurred in connection with, and any amounts paid or not paid in settlement of, any pending or threatened legal action or proceeding), costs, fines, penalties, taxes, assessments, punitive damages, fees (including advocate's/attorney's fees), judgments, awards, obligations (collectively referred to as "**Losses**"), suffered or incurred by NPCI, arising out of any liability created in the system with regard to illustratively identified as fraud, downtime connectivity, system or application vulnerabilities etc. owing to the TSP provided by us.

Yours faithfully,

Authorized signatory
(Name:)
(Designation:)
(Contact no:)
(Email:)

Date:

ANNEXURE II

BBPS System Audit Framework

Audit Process

Following steps would be repeated annually to ensure that the process is comprehensive & effective:

1. The Audit shall be conducted according to the Norms, Terms of References (TOR) and Guidelines issued by BBPS.

2. The TSPs must carry out risk-focussed internal audits of their systems, operations, and comply with BBPS standards, BBPS Procedural Guidelines, RBI regulations and guidelines or any other guidelines in this regard.
3. Internal Infrastructure security audit should be performed annually with reference to TOR System Audit framework by CERT-IN empanelled audit firms.. TSP must submit these audit reports annually to BBPCU.
4. As mentioned in BBPS circulars, BBPCU may nominate, any other agency appointed by them to conduct audit with prior notice. The audit maybe conducted on an annual basis or as per the frequency decided by BBPCU. Prior intimation of 30 days would be given to the TSP.
5. TSP must undertake system audits for their BBPOU to ensure that their Information Technology systems are protected from known, zero-day vulnerabilities arising out of hacking attempts, denial of service attacks. Adequate steps must be taken to ensure that the systems are able to maintain the transaction data integrity and the customer information confidential at all times.
6. BBPCU reserves the right to call for internal Infrastructure Security audit report from the TSP.
7. BBPCU reserves the right to audit TSP/ BBPOU with regards to the conduct of BBPS operations and compliance to PCI-DSS, ISO 27001 standards with prior intimation.
8. TSP must submit a status report to BBPS on the internal audits carried out by them during a financial year, within 45 days from the start of the next financial year. The status report should also mention critical observations, serious or persistent irregularities and non-compliance, and shortcomings of serious nature pointed out in the internal audit reports that warranted immediate remedial measures and the action taken.

Terms of Reference (ToR)

1. General Controls for Data Center Facilities – It must include

    a. Application access – Segregation of duties, Database & Application access etc.
    b. Maintenance access – Vendor engineers.
    c. Physical access – Permissions, logging, exception reporting & alerts.
    d. Environmental controls – Fire protection, AC monitoring etc.
    e. Fault resolution mechanism.
    f. Folder sharing and Back-up controls – Safeguard critical information on local desktops

g. Incidences of violations in last year & corrective actions taken

2. Software Change Control – It must include

    a. User awareness
    b. Processing of new feature request
    c. Fault reporting / tracking mechanism & process for resolutions
    d. Testing of New releases / Bug-fixes – Testing process (automation level)
    e. Version Control – History, Change Management process etc.
    f. Development / Test/ Production environment – Segregation
    g. New release in Production – Promotion, Release note approvals
    h. Production issues / disruptions reported during last year & corrective actions taken

3. Data communication / Network controls – It must include
    a. Network Administration – Redundancy, Monitoring, breakdown resolution etc.
    b. WAN Management – Connectivity provisions for business continuity.
    c. Encryption - Router based as well as during transmission
    d. Connection Permissions – Restriction on need to have basis
    e. Fallback mechanism – Backup connections controls etc.
    f. Incidences of access violations in last year & corrective actions taken

4. Security Controls – General office infrastructure – It must include
    a. Security Policy & quality of implementation of the same
    b. LAN security control and monitoring
    c. OS & Database Security controls & monitoring
    d. Internet connection controls – Firewall protection, Intrusion Detection System, Access rights and privileges.
    e. Virus protection – Controls to mitigate the Virus attacks / Outbreaks.
    f. Secured (digitally signed) e-mail with other entities like vendors and partners
    g. Incidences of security violations in last year & corrective actions taken

5. Access policy and controls

6. Electronic Document controls

7. General Access controls

8. Performance / Operational audit – It must include
    a. Comparison of changes in transaction volumes since previous audit
    b. Review of systems (hardware, software, network) performance over period

c. Review of the current volumes against the last Performance Test performed
d. Adherence to the defined processes.
e. Data localization SAR review
f. Compliance with RBI Regulations and guidelines issued from time to time as applicable to the Regulated Entities and System Participants.
g. Adherence to various SLAs, TATs.
h. Risk mitigation processes, including but not limited to pre-funding by Agent Institutions and Agents, followed by the BBPOU.
i. For non-bank TSPs, Audit reports / compliance certificates from sponsor banks with reference to the operations of the escrow account for holding the funds received towards bill payment through BBPS.
j. Quantum and nature of frauds, measure taken to prevent recurrences.
k. Number of complaints and nature of disputes and complaints. Effectiveness of the resolution framework, compliance with TAT and internal escalation mechanism.

9. Business Continuity / Disaster Recovery Facilities – It must include
    a. BCP manual, including Business Impact Analysis, Risk Assessment and DR process
    b. Implementation of policies
    c. Back-up procedures and recovery mechanism using back-ups.
    d. Storage of Back-up (Remote site, DRS etc.)
    e. Redundancy – Links, Equipment, Network, Site etc.
    f. DRS installation and Drills - Management statement on targeted resumption capability (in terms of time required & extent of loss of data)
    g. Evidence of achieving the set targets during the DRS drills in event of various disaster scenarios.
    h. Debrief / review of any actual event when the DR/BCP was invoked during the year

10. IT Support & IT Asset Management – It must include
    a. Utilization monitoring – including report of prior year utilization
    b. Capacity planning – including projection of business volumes
    c. Disposal – Equipment, Media, etc.
    d. Entity Specific Software

11. Electronic Waste Disposal

ANNEXURE III

TERMS AND CONDITIONS

These Terms and Conditions ("**Terms**") apply to and govern the technology service provider empanelment and certification program ("**Program**") facilitated by NPCI Bharat BillPay Limited ("**NBBL**", "**We**", "**Us**" and "**Our**") through [•] ("**Website**"). Please read these Terms carefully before accessing or using the Program or Website. By accessing, or using or registering on the Website, the TSP agrees to be bound by the Terms.

1. **DEFINITIONS:** The following words and phrases shall have the meanings as set below unless the context indicates otherwise:

1.1 "**BBPS Ecosystem**" shall mean the technical ecosystem of Bharat Bill Payment System.

1.2 "**BBPCU**" shall mean the Bharat Bill Payment Central Unit.

1.3 "**BBPOU**" shall mean the Bharat Bill Payment Operating Unit.

1.4 "**Certification**" or "**Certified**" or "**Certifying**" shall mean the process through which the application, infrastructure and/or other auxiliary services developed by a TSP in connection with the BBPS Ecosystem is verified and certified by NBBL to be compatible with the BBPS Ecosystem.

1.5 "**Certification Documentation**" means Certification documents, technical specifications, circulars, notifications or any other instruction/ communication issued by NBBL in relation to the Certification, from time to time, including any information security requirements.

1.6 "**TSP**" shall mean and include any technology service provider including BBPOU providing application, infrastructure and other auxiliary services in connection with the BBPS Ecosystem.

Interpretations: (a) the singular includes the plural (and vice versa); (b) reference to the words "include" or "including" shall be construed without limitation; and (c) any term capitalised but not defined shall have the same meaning as ascribed to it in the General Clauses Act, 1897; (d) headings are given for ease of reference only and shall not affect interpretation.

2. PURPOSE AND ARRANGEMENT

2.1. Pursuant to the Program, NBBL intends to enable the eligible TSPs to develop their systems with respect to BBPCU, get connected to BBPCU, test the functionalities of their system within the BBPS Ecosystem and be part of the BBPS Ecosystem. In order to ensure expeditious onboarding of a TSP whose system is developed and compatible with BBPS Ecosystem, NBBL will certify the systems/products/services of the TSPs who comply with the Certification Documentation and procedures set by NBBL from time to time.

2.2. The TSPs willing to participate in the Program shall be eligible as per the eligibility criteria set out by NBBL from time to time. NBBL reserves a right to modify the eligibility criteria and to reject any application of a TSP to be onboarded for the Program at its sole discretion.

2.3. Further, subject to these Terms and payment of appropriate fees as provided below, the Program will allow TSPs to access product specifications and other technical information pertaining to products and services of NBBL ("**Specification**") for the purpose of obtaining Certification from NBBL. For the purpose of obtaining access to the Specification, the TSP shall have to apply with NBBL to provide necessary hardware and shall create an account ("**TSP Account**") by submitting such details as may be required by NBBL including registered mobile number, organisation name, authorised representative name, email address, website, etc. When the TSP registers to open the TSP Account, TSP agrees to provide certain personal information about the TSP and its representative which may include without limitation personal information such as name, e-mail address, mobile number, passwords and other relevant details. The TSP agrees to provide true, accurate, current, and complete information and documents and, for as long as the TSP continue to use the TSP Account, to update such information to keep it true, accurate, current, and complete. If NBBL has grounds to suspect that such information is untrue, inaccurate, not current, then NBBL has the right to indefinitely suspend or terminate the TSP Account and refuse to provide the TSP with access to TSP Account.

2.4. Subject to the Terms, NBBL grants to the TSP a revocable, non-exclusive, non-sub licensable, non-transferable and limited right to use the Specification solely for accessing and using such Specification strictly for the purpose of obtaining Certification from NBBL and as per the terms and conditions as provided in the Certification Documentation, till the time the access to TSP Account is terminated in accordance with these Terms. As between the TSP and NBBL, NBBL owns the Specification and any modification thereto. The Specifications are protected under Indian and international laws. Any unauthorized use of the Specifications may violate copyright, patents, trademark, and other applicable

national or international laws. NBBL reserves the right to modify, suspend, or discontinue the APIs at any time with or without notice to the TSP. The TSP shall, as per process prescribed by NBBL, procure ensure that its products and services as Certified by NBBL are updated and modified from time to time to be compatible with any updates and modifications made by NBBL to its products and services. NBBL reserves the sole right to may make changes to the Specifications, at any time and it will endeavour to provide reasonable notice of the same.

2.5. The TSP agrees and undertakes to at all times comply with the Certification Documentation including after the Certification of the products and services and in the use case environment. The Certification shall be subject to compliance of the TSP of its obligations and responsibilities under the Certification Documentation, including the service level requirements, as may be provided by NBBL from time to time. The TSP understands that any breach of the provisions of this Clause may result in forthwith revocation of the Certification and debarment of the TSP from further engaging with NBBL, NPCI and/or its affiliates at the sole discretion of NBBL.

2.6. The TSP agrees and undertakes to keep all information of NBBL in relation to Website, Specification and NPCINet confidential and shall use it solely for the purpose of availing services in accordance with the Terms.

3. CERTIFICATION PROCESS

3.1. A TSP can get Certified either directly or through a BBPOU. In case where the TSP is Certified through a BBPOU, the BBPOU shall be responsible for ensuring compliance of the Certification Documentation by the TSP. The TSP or its associated BBPOU shall be liable to undergo Certification in various situations as listed in the Certification Documentation, including but not limited to:

3.1.1. When interacts with the BBPS Ecosystem for the first time.

3.1.2. For any new enhancement or any new features included/implemented in BBPCU.

3.2. For the purpose of Certification including testing along with the BBPS Ecosystem, the TSP shall have access to the applications of NBBL including the in-house secured network connectivity enabled by NBBL ("**NPCINet**"). The TSP shall be required to comply with the relevant guidelines to access the NPCINet and shall at all times adhere to the technical access specifications provided by NBBL for the purpose of accessing and using the NPCINet. The TSP shall access to NPCINet solely from the certified systems of the TSP and for the limited purpose of obtaining the Certification.

3.3. TSP agrees and understands that the access to NPCINet and other applications provided by the NBBL including Sandbox shall be solely for development and testing purposes for the purpose of Certification and at no time shall such access or Certification be considered as permission for going live by NBBL. NBBL shall not allow any live transactions through NPCINet, or other applications provided by NBBL pursuant to the Program. Further, the TSP shall be responsible for maintaining necessary infrastructure, bandwidth and network connectivity for the purpose of accessing and using the NPCINet and other applications provided by NBBL for the purpose of Certification.

3.4. TSP agrees and understands that, subject to adherence of these Terms and the Certification Documentation by the TSP, the Certification shall be valid for a period of [•] months from the date of Certification or till any major changes are done in the TSP application/product/services. During this validity of the Certification, TSP has to get on-boarded by directly doing UAT in case applicable. Notwithstanding anything to the contrary contained herein, NBBL reserves the right to cancel any Certification or remove the TSP from the Program, at its sole discretion.

4. RESTRICTIONS

4.1. The TSP undertakes that it shall not: (1) use the Specifications, NPCINet or any other information shared by NBBL for anything other than in accordance with these Terms; (2) make any copies of the Specifications or disclose to any person, modify, adapt, create derivative works of, reverse engineer, decompile, reverse compile, or disassemble, the Specifications or any derivative work or attempt to extract the source code from any Specifications; (3) distribute, sell, lease, rent, lend, sublicense, encumber, assign, transfer in any manner whatsoever, or provide any access to the Specifications or the NPCINet, in full or part, to any third persons in any manner whatsoever, other than as approved by NBBL in writing; (4) allow or agree to the Specifications or NPCINet or any hardware connected thereto to become subject of any charge, lien or encumbrance; (5) interfere with or disrupt the Specifications or NPCINet or the servers or networks providing the Specifications or NPCINet or upload or otherwise transmit to NBBL or any of its systems (whether through API calls, or NPCINet or otherwise) any material containing software viruses, harmful code or other computer code, files or programs designed to interrupt, destroy or limit the functionality

of any software or hardware; (6) use Specifications or NPCINet or Specifications functionality in breach of any applicable law or in any activity that is in violation or breach of applicable law.

4.2. The TSP acknowledges that any usage of the NPCINet as a medium of communication is prone to security breach and therefore, TSP shall be under the duty of special care to take extra and special care to ensure there is no security breach in any manner whatsoever related to the NPCINet and Specifications and shall adhere any data security and connectivity guidelines or requirements mandated by NBBL. Further, TSP shall be responsible to report any, fraud, cyber-attack or suspicious transaction immediately to csirt@npci.org.in and to the relevant BBPOU on daily basis.

4.3. Any access and use of the TSP Account by the TSP, notwithstanding any security breach at TSP's end shall be deemed to be by the TSP's authorised person only and shall irrevocably and unconditionally bind the TSP vis-a-vis NBBL and any other persons or entities involved and shall always amount to authentic and authorised use by, for and on the TSP's behalf. The TSP alone shall be liable and responsible for any such security breach and consequences thereof and shall not hold NBBL responsible in any manner whatsoever.

4.4. TSP acknowledges that NBBL is solely a facilitator for empanelment and certification of the TSP for the purpose of ease of on-boarding of TSP in a live environment for the benefit of the customers at large. The Program shall in no manner be deemed to be a commitment from NBBL or any of its affiliates to on-board the TSP on the BBPS Ecosystem.

4.5. TSP agrees not to display, upload, modify, publish, transmit, store, update or share any information that,— (i) belongs to another person and to which the TSP does not have right to do the foregoing; (ii) is defamatory, obscene, pornographic, paedophilic, invasive of another's privacy, including bodily privacy, insulting or harassing on the basis of gender, libellous, racially or ethnically objectionable, relating or encouraging money laundering or gambling, or otherwise inconsistent with or contrary to the laws in force; (iii) is harmful to child; (iv) infringes any patent, trademark, copyright or other proprietary rights; (v) violates any law for the time being in force; (vi) deceives or misleads the addressee about the origin of the message or knowingly and intentionally communicates any information which is patently false or misleading in nature but may reasonably be perceived as a fact; (vii) impersonates another person; (viii) threatens the unity, integrity, defence, security or sovereignty of India, friendly relations with foreign States, or public order, or causes incitement to the commission of any cognisable offence or prevents investigation of any offence or is insulting other nation; (ix) contains software virus or any other computer code, file or program designed to interrupt, destroy or limit the functionality of any computer resource; (x) is patently false and untrue, and is written or published in any form, with the intent to mislead or harass a person, entity or agency for financial gain or to cause any injury to any person.

5. FEES AND PAYMENT TERMS

5.1. In consideration for providing the Certification and connectivity to the NPCINet and other applications of NBBL including the hardware in relation thereto, TSP shall be responsible for pay such Certification charges, hardware charges, connectivity charges and such other charges as may be communicated by NBBL from time to time on the Website or Certification Documentation or circulars and notifications.

5.2. Any changes to the fee/pricing for the Program or the Certification or network connectivity will be made through the Website/Certification Documentation/circular communicated through email, posting on the Website or such other manner as deemed fit by NBBL and such changes shall automatically become effective immediately after NBBL sends such communication. In case of any dues payable by TSP to NBBL for the Program / Certification/ network connectivity and related hardware, NBBL reserves a right to set-off such amounts against any payments to be made by NBBL or its associated or affiliates to the TSP under any agreement or arrangement.

6. TERMINATION

6.1. These Terms are effective unless and until terminated by NBBL. TSP may terminate the access to the Website by giving NBBL a prior written notice of not less than 30 (thirty) days. NBBL may terminate, suspend, or modify TSP's registration with, or access to the Website, without notice, at any time and for any reason including breach of these Terms or Certification Documentation, change in applicable laws and initiation of bankruptcy or insolvency proceedings against the TSP. Upon termination for any reason, all rights granted by NBBL to TSP with respect to the Program, Website and Specifications shall immediately cease and TSP agrees to immediately stop using the Program, Website, NPCINet and Specifications.

7. LIABILITY

7.1. Save as provided in the Terms and the Certification Documentation, neither NBBL nor its subsidiaries, or service providers (or the respective officers, directors, employees, or agents of any such entities) (collectively, "**NBBL Parties**") make any promises about the Website, Program, NPCINet or Certification or Specifications. The Program, Certification, NPCINet and Specifications are provided on "as is", "with all faults" and "as available" basis and the entire risk as to the quality and performance of the Website, Program, NPCINet, Certification or Specifications are with the TSP. NBBL expressly disclaims all warranties of any kind, whether express, implied, or statutory, with respect to the Website, Program, NPCINet, Certification or Specifications (including, but not limited to, any implied or statutory warranties of merchantability, fitness for a particular use or purpose, title, and non-infringement of intellectual property rights). Without limiting the generality of the foregoing, NBBL makes no warranty that the Website, Program, NPCINet, Certification or Specifications will meet TSP's requirements or that the access to Website, Program, NPCINet or Specifications will be uninterrupted, timely, secure, or error free or that defects in the Website, Program, NPCINet or Specifications will be corrected. NBBL makes no warranty as to the results that may be obtained from the use of the Website, Program, NPCINet, Certification or Specifications or as to the accuracy, quality or reliability of any data, information and advice obtained through the Website, Program, NPCINet, Certification or Specifications. NBBL disclaims any warranties for viruses or other harmful components in connection with the Website, NPCINet or Specifications.

7.2. In no event will any of the NBBL Parties be liable for any indirect, special, consequential, punitive, or exemplary damages (including, without limitation, those resulting from loss of revenues, loss of goodwill, loss of data, business interruption, or other intangible losses), arising out of or in connection with Website, Program, NPCINet, Certification or Specifications (including, without limitation, use, inability to use, or the results of use of Website, Program, NPCINet or Specifications, unauthorized access to or alteration of the Website, Program, NPCINet or Specifications, or any other matter relating to the Website, Program, NPCINet, Certification or Specifications). To the extent that any of NBBL Parties may/have not, as a matter of applicable law, disclaim any implied warranty or limit its liabilities, the scope and duration of such warranty and the extent of such party's liability shall be the minimum permitted under such applicable law.

7.3. The TSP agrees to indemnify, defend, and hold harmless each of NBBL Parties from and against any and all claims, liabilities, damages, losses, costs, expenses, or fees (including reasonable attorneys' fees) that such parties may incur or suffer as a result of or arising from or in connection with breach or violation of these Terms or arising out of violation of any applicable laws, regulations or breach of intellectual property rights or fraudulent transactions or otherwise use of the Website, Program, NPCINet, Certification or Specifications. NBBL reserves the right to assume the exclusive defence and control of any matter otherwise subject to indemnification by TSP and, in such case, TSP agrees to cooperate with NBBL' defence of such claim. This clause shall survive the expiry or termination of Program, for a period of three years from the date termination thereof.

7.4. In the event of non-compliance with the TSP Technical Standards, Procedural Guidelines, Circulars or any such guidelines released in this regard or any breach or violation identified as part of the Audit report, BBPCU reserves the right to impose penalty on the BBPOU or its respective TSP with prior intimation.

7.5. BBPCU also reserves the right to temporarily or permanently suspend the Certification given to a certain TSP in case the TSP doesn't adhere with the norms, technical standards or any such guidelines in this regard

7.6. Following would be the structure of Penalties in case of non-compliance with respect to Audit Reports

Sr. No.	Scenario	Action to be taken

1	TSP not submitting any audit reports in a year	a. NBBL will send letter to TSP's senior management team with regard to failure in submission of report (equivalent to Chief Technology Officer or Chief Operating Officer or above). b. Actions as per Sr no.3 and/or 4 whichever applicable.
2	TSP not able to close all gaps and submit closure report within 90 days from submission of audit report.	NBBL will send letter to TSP's senior management team with regard to failure in submission of report (equivalent to Chief Technology Officer or Chief Operating Officer or above).
3	TSP exceeding closure timelines by 60 days.	Penalty of INR 1,00,000 per month
4	TSP exceeding closure timelines by 90 days.	Suspend certification and stop new on-boarding of any BBPOU and stop catering to any BBPOU for new features, enhancements etc.

8. GOVERNING LAW AND JURISDICTION

These Terms and the relationship between TSP and NBBL shall be governed by the laws of India and competent courts and forums at Mumbai, Maharashtra shall have exclusive jurisdiction in any proceedings arising out of the use of the Website, Program, NPCINet, Certification, Specifications or these Terms. NBBL may, however, in its absolute discretion commence any legal action or proceedings arising out of these Terms in any other court, tribunal or other appropriate forum, and TSP hereby consent to that jurisdiction.

9. GENERAL

9.1. These Terms read with the Certification Documentation constitute the entire agreement between the TSP and NBBL with respect to the Program, superseding any prior agreements or negotiations between TSP and NBBL with respect to the same. NBBL shall neither be liable to the other nor shall be in default if, and to the extent that, the performance or delay in performance of any of its obligations under these Terms is prevented, restricted, delayed or interfered with due to circumstances beyond the reasonable control of NBBL or any force majeure event. The failure of NBBL to exercise or enforce any right or provision of the Terms shall not constitute a waiver of such right or provision. If any provision of the Terms is found by a court of competent jurisdiction to be invalid, TSP nevertheless agree that the court should endeavour to give effect to the intentions of NBBL and the TSP as reflected in the provision, and that the other provisions of the Terms remain in full force and effect. The Terms, and any rights and licenses granted or obligations hereunder, may not be transferred or assigned by the TSP to any other Person, but may be transferred or assigned by NBBL without restriction.

9.2. The TSP agrees that NBBL, its subcontractors and service providers, may hold, process and use the information of the TSP and other information received by NBBL from the TSP in relation to the Program, for providing the assistance, any analytical purposes including to improve the Program or the Website or to offer additional features to the TSP. The TSP agrees that NBBL may disclose to a Person any information of or related to the TSP, received by NBBL in relation to the Program, as may be permitted under law or reasonably necessary for compliance with any legal directive, for fraud prevention purposes or where the TSP has consented to such disclosure. The TSP hereby authorises NBBL to share TSP's information or

information collected during the course of TSP's usage of the Program with third parties in an anonymised or de-identified manner.

9.3. By acceptance of the Terms and usage of the Website and Program, the TSP represents and warrants that the TSP has the authority to accept the Terms and represents, warrants, and agrees that the TSP has read, understood, and agree to be bound by the Terms and Certification Documentation. All Certification Documentation posted on the Website or otherwise notified to the TSP, are hereby incorporated by reference into the Terms.

9.4. All communications will be sent to TSP's address / email id provided in the application form. In case contact details provided by the TSP to NBBL, are longer valid or in use, or TSP intends to change them, the TSP shall promptly provide NBBL updated contacts details on [●*insert email*] or in such other manner as may be prescribed by NBBL.

10. MODIFICATIONS TO THESE TERMS AND CONDITIONS

NBBL may, in its sole and absolute discretion, amend or supplement these Terms at any time. NBBL will post notice of such changes on the Website or notify TSP in any other manner as decided by NBBL. The TSP shall be responsible for regularly reviewing these Terms as may be posted on the Website. If TSP objects to any such changes, the TSP's sole recourse shall be to cease using the Website and the Program, on immediate basis. The continued use of the Website and/or Program, by the TSP, following notice of any such changes shall indicate TSP's acknowledgement of such changes and agreement to be bound by the revised terms and conditions.

11. GRIEVANCE OFFICER

In accordance with Information Technology Act, 2000 and rules made there under, the name and contact details of the Grievance Officer are provided below:

Designation: [●]
Address: [●]
Phone: [●]
Email: [●]

The TSP may register its complaints regarding the Program or any other issue relating to these Terms with the above-mentioned Grievance Officer. Every attempt shall be made to offer the TSP suitable and appropriate solutions.