TECHNICAL SPECIFICATION FOR TSP EMPANLEMENT

Version 1.0

BBPS TECHNOLOGY TEAM

NPCI BHARAT BILLPAY LTD.

Document History

Date	Version	Description
21st June 2021	1.0	Base version of TSP Empanelment – Technical Standards

Contents

1. Overview

Bharat Bill Payment System is a unified bill payment system for paying recurring bills across India. BBPS offers an interoperable and accessible bill payment services to customers through multiple channels and network of agents enabling multiple payment modes, and providing instant confirmation of payment. Bharat Bill Payment System is an integrated platform under the umbrella of NPCI Bharat BillPay Limited (NBBL), a wholly owned subsidiary of NPCI.

2. About this Document

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 BBPS Ecosystem.

This document sets out a broad approach to designing systems that may 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 BBPS ecosystem.

2.2 Scope

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

- Eligibility Criteria
- On-boarding Standards
- TSP Certification
- 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 and registered under appropriate Indian Companies Act.
- Should have experience is providing payment solutions i.e., payment gateways, transaction processing platforms, CBS platforms etc.
- Should be a profit earning organization- should have not incurred loss and have a positive net worth for 3 consecutive financial years
- Should not be black listed by any of the Banks/Central Govt/State Govt/PSU/Govt bodies
- 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.

4. TSP Certification

4.1 Certification Flow

The following sections covers the certification Process in its entirety below.

4.1.1 Base Certification

BBPOU 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

The TSP must undergo certification/s for any new Enhancements included/implemented in BBPCU

4.1.3 Add-on Channel Certification

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

- OU in relation with the same TSP but for a different channel certification.
- OU in relation with same In- house solution provider but for a different initiating channel.

4.1.4 Recertification

BBPOU will come under recertification process when OU has not gone live in Production after completing certification for more than thirty days. Recertification must also be performed annually once.

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.

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

- **Sandbox Test environment:** To verify the necessary testing requirements like below.
- **Comfort Environment:** To test and verify the possible structural / logical and compliance parameters
- **UAT Environment:** 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 may on-board s by directly doing UAT if applicable.

4.3 Certification Mandates

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

5. On-boarding Standards

While on-boarding technical service providers (TSPs) must ensure that adequate precautions are taken. While on-boarding these entities, ensure only bonafide entities are made participants of the BBPS ecosystem and Bharat BillPay brand promise is not diluted. 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 may connect directly or through a BBPOU Institution's infrastructure to ensure that it is capable of complying with various BBPS requirements, Procedural Guidelines and standards.
- There should be a proper contractual agreement between the BBPOU and the TSP, including undertaking by the TSP for compliance of the BBPS Procedural Guidelines, Standards, Circulars and guidelines on Bharat BillPay brand guidelines and any other guidelines in this regard.
- TSPs must comply with BBPS System Audit Framework standards

The above standards for participating entities may 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 (in Lakhs)	Grade Level	Minimum Bandwidth Required
0 <= 10L	1	8 MBps
10L & above	2	16 MBps

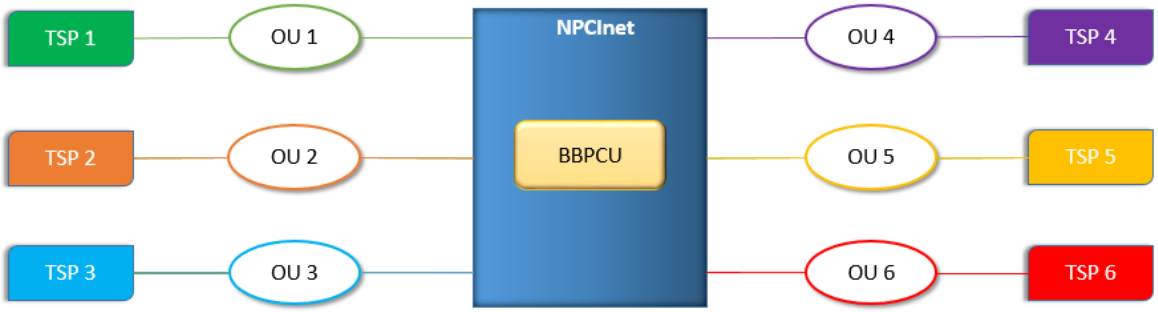
Based on the Grade level, appropriate network bandwidth needs to be provisioned.

7. Infrastructure Management

7.1 Connectivity Models

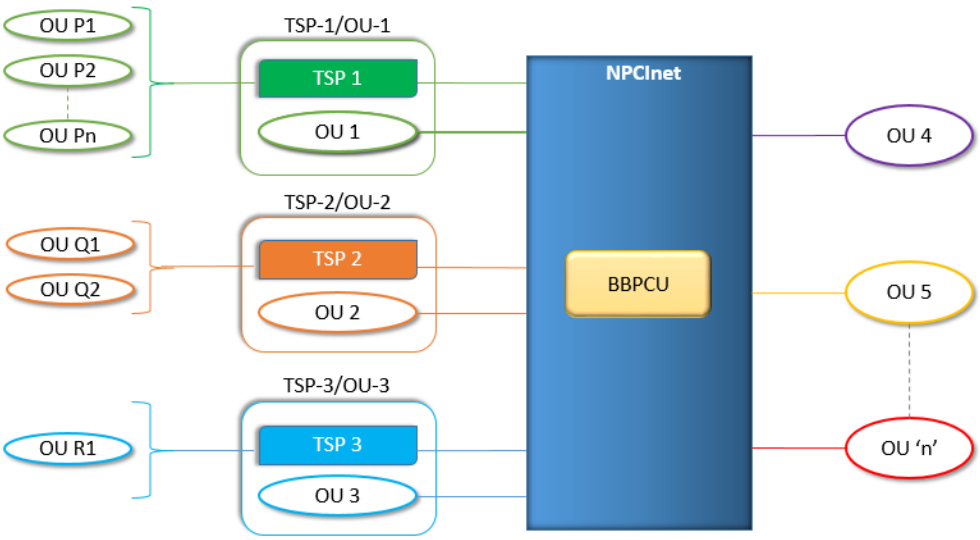
7.1.1 Case I - TSP services to BBPOUs

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.



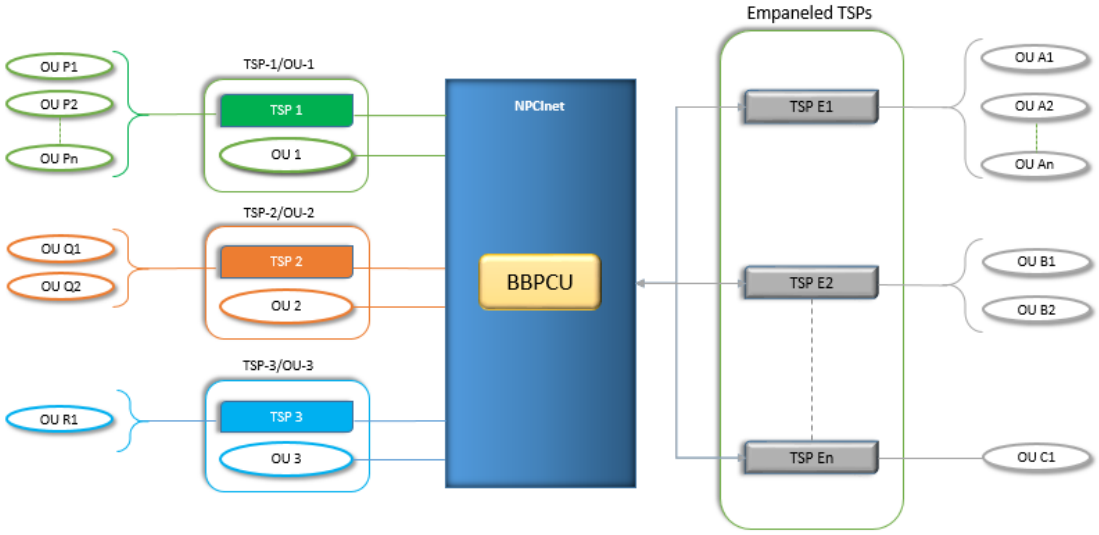
7.1.2 Case II – BBPOU acting as TSP

- 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.



7.1.3 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.



7.2 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) to enable the OUs to make right decision with regard to TSPs for engagement
- The TSPs who will be desirous of empanelment will have enter into an agreement with NPCI for adherence to NPCI terms and conditions, scheme compliance, indemnification, etc.
- The empanelment would be applicable for new TSPs and also existing entities acting as TSP 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 TSP Managed OUs
- 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
- 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.

7.3 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. 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).

7.4 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.

7.5 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.

8. 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 Ecosystem.

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

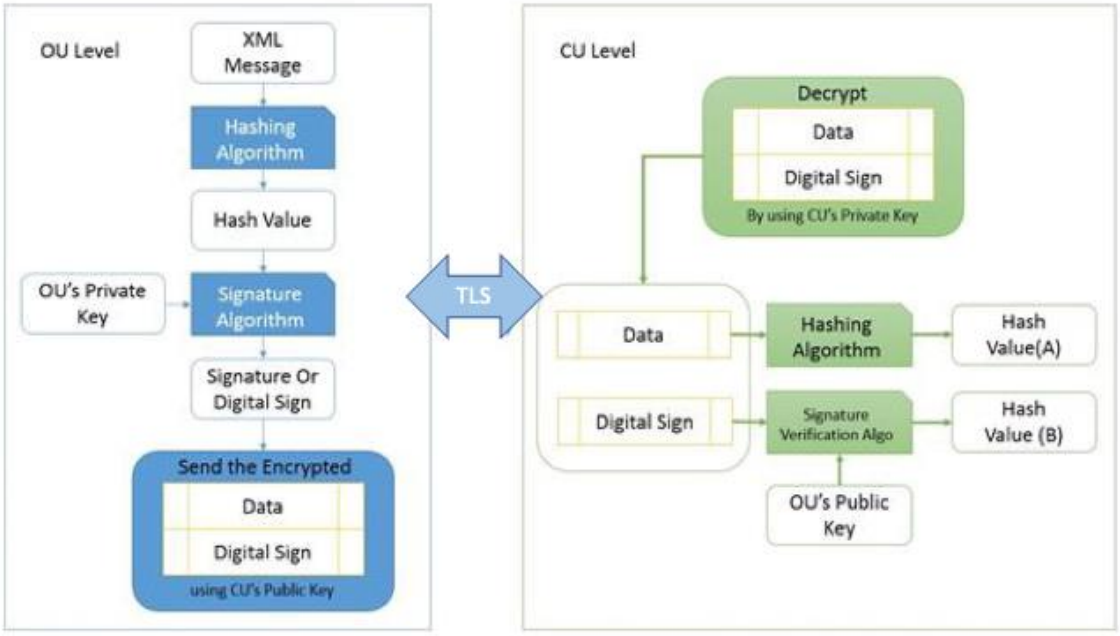
Digital certificates will be used to ensure the trustworthiness of public facing portals and websites of BBPCU. The digital certificate will contain a unique identifier for the entity, and also include the certificate authority that verifies the information contained in the certificate, date that the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

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 (v1.3), i.e. HTTPS.
- 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 compression.

- When a TLS connection is established, a handshaking, known as the TLS Handshake Protocol, occurs where a client hello (Client Hello) and a server hello (Server Hello) message are passed. First, the client sends a list of the cipher suites that it supports, in order of preference. Then the server replies with the cipher suite that it has selected from the client's list.
- There should be no \n and \r formatting applied by the signature utility in the final XML file sent.
- TLS v1.3 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 compliant device configuration).
- Public keys (certificates) to be stored securely in DB.

9. Data Management

9.1 Data Handling

- Accessing data from BBPCU can be done by authorized BBPOU after several levels (Network, application) of authentication and authorization.
- 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 may 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.

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
- 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.

10. 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.
- 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.

11. Risk Management

11.1 Fraud Risk Measures

- Every TSP shall be responsible to report any, fraud, cyber-attack or suspicious transaction immediately to NPCI Fraud Risk team at fraudrisk_bbps@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.

12. 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 quarterly with reference to TOR System Audit framework. TSP must submit external assessment reports annually to BBPCU.
- External Audits must be conducted only by CERT-IN empanelled audit firms. As mentioned in BBPS circulars, BBPCU may nominate, any other agency appointed by them to conduct audit with prior notice.
- 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.
- TSP must submit a status report to BBPS on the internal audits carried out by them for BBPOU during a financial year, within 45 days from the start of the next quarter. The status report may 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.

13. List of Abbreviations

API	Application Program Interface
BBPCU	Bharat Bill Payment Central Unit
BBPOU	Bharat Bill Payment Operating Unit
BOU	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	NPCI 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
TLS	Transport Layer Security
TPS	Transactions Per Second
URL	Uniform Resource Locator
XML	Extensible Mark-up Language
XSD	XML Schema Definition