|  |  |  |
| --- | --- | --- |
| APTlogogreen3 | ASIA-PACIFIC TELECOMMUNITY |  |
| **SOUTH ASIAN TELECOMMUNICATIONS REGULATOR’S COUNCIL** **(SATRC)** |  |
|  |  |

**SATRC REPORT ON**

**DIGITAL FINANCIAL SERVICES**

**Prepared by**

**SATRC Working Group on Policy, Regulation and Services**

Adopted by

**22nd Meeting of the South Asian Telecommunications Regulator’s Council**

1 – 3 November 2021,Virtual/Online Meeting

**TABLE OF CONTENTS**

[CHAPTER-1: INTRODUCTION 3](#_Toc52452619)

[CHAPTER-2: TYPES OF DIGITAL FINANCIAL SERVICES 5](#_Toc52452620)

[CHAPTER-3: REGULATORY INSTRUMENTS FOR DIGITAL FINANCIAL SERVICES 6](#_Toc52452621)

[CHAPTER-4: STAKEHOLDERS IN DIGITAL FINANCIAL SERVICES 7](#_Toc52452622)

[CHAPTER-5: AUTHENTICATION MECHANISMS 9](#_Toc52452623)

[CHAPTER-6: INTERNATIONAL BEST PRACTICES 11](#_Toc52452624)

[CHAPTER-7: CHALLENGES 14](#_Toc52452625)

[CHAPTER-8: RECOMMENDATIONS 18](#_Toc52452626)

LIST OF ACRYNOMS …………………………………………………………………………………..20

[ANNEXURE – 1 22](#_Toc52452627)

[ANNEXURE – 2 23](#_Toc52452628)

# CHAPTER-1: INTRODUCTION

**1.1 Background and Purpose**

1.1.1. International Telecommunications Union (ITU) defines Digital Financial Services (DFS) as ***“services include methods to electronically store and transfer funds; to make and receive payments; to borrow, save, insure and invest; and to manage a person's or enterprise's finances***”. The broad range of financial services including payments, credit, savings, remittances, insurance etc are accessed and delivered through ‘Digital Channels’.

1.1.2. In this context, the term “digital channels” refers to the Internet, Mobile phones (both smart phones and digital feature phones), ATMs, POS terminals, NFC-enabled devices, chips, electronically enabled cards, biometric devices, tablets, phablets and any other digital system. DFS models also usually employ agents and the networks of other third-party intermediaries to improve accessibility and lower the overall service delivery cost.

1.1.3. The digital financial services (DFS) concept includes mobile financial services (MFS) as many Digital Financial Services (DFS) are provided over the Mobile Network either by the Cellular mobile service providers or in collaboration with the financial institutions like banks. This innovative service has created additional value for the existing cellular mobile networks as the mobile phone is used to access financial services and execute financial transactions. This includes both transactional services, such as transferring funds to make a mobile payment, and non-transactional services, such as viewing financial information. Mobile financial services include mobile banking (M-Banking), mobile payments (m-payments), mobile money, mobile insurance, mobile credit, mobile savings etc.

1.1.4. SATRC countries have many rural villages and remote areas without availability of banking services but still are covered with telecom services like 2G and 3G cellular mobile services. One of the important goals of our governments is to bring these rural population under the umbrella of Financial Inclusion, who are otherwise unbanked by not having access to the banking services. Financial inclusion means, a sustainable provision of affordable financial services that bring the poor into the formal economy. An inclusive system includes a range of financial services that provide opportunities for accessing and transferring funds, growing capital, and reducing risk. Such services may be provided by banks and other traditional financial services organizations, or by non-banking institutions. Financial inclusion contributes to the developmental goals of poverty reduction, economic growth and jobs, greater food security and agricultural production, women’s economic empowerment and health protection.

1.1.5. With the spread of technology, these financial services were envisaged to be made available through digital means, thus giving rise to Digital Financial Services (DFS). Using DFS helps in achieving wider financial inclusion.

1.1.6. The global economy has been affected adversely during the years 2020-21 due to the impact of COVID-19 pandemic. The deepest global recession is sending hundreds of millions into poverty, and recovery appears to be taking longer than expected. However, this pandemic crisis has revived the prospects of digital market and digital transactions due to restrictions in travel and social distancing norms. This has encouraged incentives for economic transformation and adoption of digital business models, including [increased use of digital financial services (DFS)](https://blogs.worldbank.org/voices/expanding-digital-financial-services-can-help-developing-economies-cope-crisis-now-and-boost-growth-later).

1.1.7. Many countries are adopting their renewed digital financial inclusion strategies during this COVID crisis which is giving a glimpse of hope for quicker revival of economic and business activities post COVID pandemic. However this sudden surge of online activities has brought in challenges, but also increasingly, an understanding of how to overcome these obstacles and reduce risk.

1.1.8. Digital Financial Services (DFS) are already existing in SATRC countries and considering the overall policy of financial inclusion and bridging the digital divides followed by all the member countries, these digital financial services should be promoted further which can help the governments to achieve the developmental goals. In this context it is imperative that the existing DFS eco-system exists among SATRC countries should be studied and recommend the possible way forward for further development of such services.

1.1.9. This objective of this study is to prepare policy and regulatory options for Digital Financial Services in SATRC countries and recommend suitable measures.

**1.2 Scope of Study**

1.2.1. To study the Digital Financial Services (DFS) provided over the Mobile Networks in SATRC countries covering the following issues, but not limited to:

Policy and regulatory requirements

Licensing

Security

Consumer protection

Infrastructure

**1.3 Methodology for carrying out study**

1.3.1. The study has been carried out by the Lead Expert in consultation with the other Experts from member countries on the subject. Therefore, in order to conduct the study, a Questionnaire was prepared to obtain inputs (information) on the subject from all SATRC member countries. Based on the inputs, the lead expert has compiled and generated the report based on the best practices for the SATRC regions. The questionnaire along with inputs received from all the countries, is attached as an Annexure to the report. The studies undertaken by the ITU-T Focus Group on Digital Financial Services have also been referred to understand the best practice methods being followed across the world. The Digital Financial Service (DFS) eco-system is an evolving domain; therefore the report is prepared based on the present existing DFS ecosystem including the services and infrastructure.

# CHAPTER-2: TYPES OF DIGITAL FINANCIAL SERVICES

**2.1. Broad Range of Financial Services.**

2.1.1 Digital Financial Services (DFS) include a wide range of financial services which can be accessed and delivered using digital channels which basically includes making payments, issue of credits, savings, deposits, insurance etc. The digital channels include Internet, mobile phones, ATMs, POS terminals etc. As explained above, the Mobile Financial services (MFS) and mobile banking also can be brought under the ambit of DFS. The types of DFS commonly available in SATRC countries are listed below:

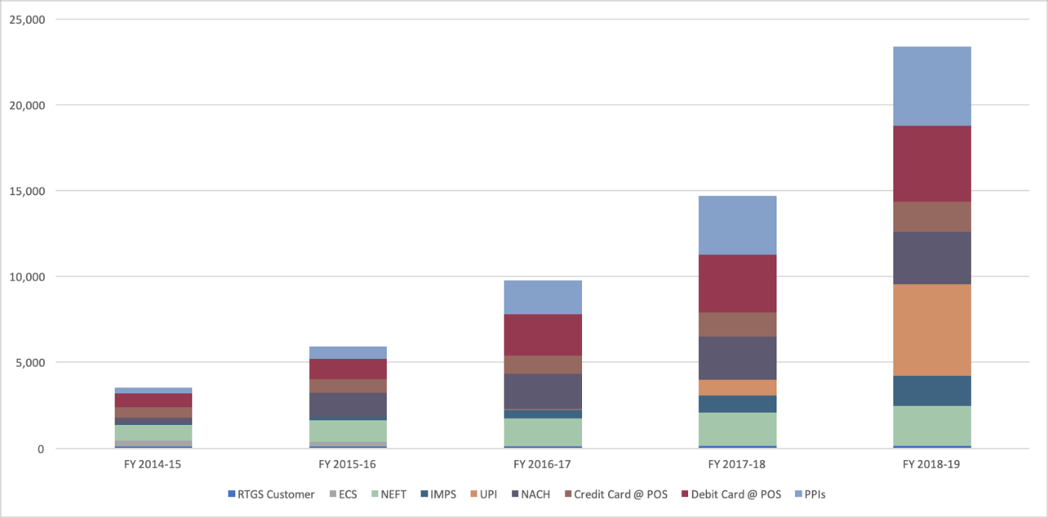
* Payments/deposit services
* Intrabank Money Transfer (P2P)
* Utility payments/Bill payments
* Purchase of goods / Service
* Mobile banking services
* Top-ups
* E-wallet

2.1.2 In countries like India and Pakistan, the DFS sector is a bank led model. MNOs were initially allowed only to offer Pre-paid Payment Instruments (PPIs) which means payment instruments that facilitate purchase of goods and services, including financial services, remittance facilities, etc., against the value stored on such instruments. The MNOs are allowed to offer only the semi-closed type of PPIs for purchase of goods and services, including financial services, remittance facilities, etc., at a group of clearly identified merchant locations / establishments which have a specific contract with the issuer (or contract through a payment aggregator / payment gateway) to accept the PPIs as payment instruments. These instruments do not permit cash withdrawal and can be offered in form of digital wallets, cards etc.

2.1.3. In India the existing PPI license holders were given an option to convert into a Payments Bank. The Payments Bank is an entity, which is allowed to undertake only certain restricted activities viz., (i) acceptance of demand deposits; (ii) issuance of ATM/Debit Cards (not allowed to issue credit cards); (iii) payment and remittance services etc.

2.1.4. The Payments Bank thus allowed the MNOs to continue their PPI business and also expand the scope of their DFS offerings.

2.1.5. The following chart[[1]](#footnote-1) shows digital transaction volumes, and values on a yearly basis over last 5 years as published by Reserve Bank of India (RBI) in India. From this it is clear that the volume of digital transaction has increased phenomenally and has further shot up this year during the COVID-19 pandemic crisis. The actual data of the first half of 2020 will be definitely astonishing. The other countries of SATRC also have similar growth in digital transactions.



# CHAPTER-3: REGULATORY INSTRUMENTS FOR DIGITAL FINANCIAL SERVICES

**3.1. Regulatory Framework and Instruments available in SATRC countries**

3.1.1. It is important to create an enabling regulatory environment that encourages viability for the market participants in a market led approach, while staying focussed on the end objective of financial inclusion for all. This enabling environment should be supported by legislative sanctions such as Act, Regulations etc. There are enough legislative framework in SATRC region and the names of these instruments are mentioned here:

|  |  |
| --- | --- |
| **Afghanistan** | Regulation on Electronic Fund Transfer |
| Electronic Money Regulation |
| **Bangladesh** | Bangladesh Mobile Financial Services (MFS) Regulations, 2018. |
| **Bhutan** | E-Money Issuer Rules and Reulations 2017 |
| **India** | Master Direction issues by the Reserve Bank of India on Issuance and Operation of Pre-paid Instruments (PPIs) |
| Guidelines for Licensing of Payment Banks, 2016 |
| **Maldives** | Maldives Monetary Authority (MMA) issues guidelines |
| **Nepal** | Payment and Settlement Bylaw, 2015 |
| Licensing Policy for Institution/Mechanism Operating Payment Related Activities, 2016 |
| **Pakistan** | Enactment of Payment System and Electronic Fund Transfer Act, 2007 |
| Issuance of Branchless Banking Regulations, 2008 |
| Rules for Payment Service Providers and Payment System Operators, 2014 |
| Regulations for Technical Implementation of Mobile Banking and Interoperability, 2016 |
| **Sri Lanka** | Payment and Settlement Systems Act No.28 of 2005 – license to operate a mobile payment system |
| Mobile Payments Guidelines No.1 of 2011 for the Bank-led Mobile Payment Services |
| Mobile Payments Guidelines No.2 of 2011 for Custodian Account Based Mobile Payment Services |
| Financial Transaction Reporting Act, 2006. |

# CHAPTER-4: STAKEHOLDERS IN DIGITAL FINANCIAL SERVICES

**4.1. Stakeholders in DFS**

4.1.1. Traditionally the financial services are provided by the financial service institutions, which are primarily Banks and non-banking financial institutions. As discussed above these services are not predominantly available in rural and remote areas of many SATRC countries. Moreover the financial inclusion targets of each government goes beyond the urban areas of the country, right into the rural and remote areas. Therefore, the financial inclusion contributes to the developmental goals of poverty reduction, economic growth & jobs, greater food security & agricultural production, women’s economic empowerment and health protection.

4.1.2 With the spread of technology, these financial services are envisaged to be made available through digital means with the collaboration of other stakeholders such as Mobile Network Operators etc. Given the complexity of the Digital Financial Services regulatory environment, it remains imperative that the two sectoral authorities involved broadly in these efforts which are financial services (Banks) and telecommunications (MNOs). In most of the SATRC countries, these are the two main stakeholders handle with DFS policy and regulatory issues.

4.1.3 As the DFS expands and reaches out to many, there are other issues which attract the involvement of other stakeholders. Keeping all this in view, the main stakeholders in the domain of Digital Financial Service are briefly discussed below.

**4.2. Types of Stakeholders in DFS**

4.2.1. **Policy Maker:** The Digital Financial Service policy is made by the concerned ministry/department in the Government. DFS Policy is part of overall financial policy and the government is entrusted with the responsibility of developing a Policy. In many countries the DFS policy is made by the Financial regulator in consultation with concerned ministry in the Government. In few countries the policy is made by the Ministry/Department and the Financial regulator complies with the Policy guidelines.

**4.2.2. Financial Regulators:** In most of the countries, the Financial Regulators play a major role in formulation of DFS policy. The Central Bank is primarily the Financial Regulator and is responsible for not only policy formulation, but also regulation and monitoring. In some countries, there are separate financial authorities to look after issues specific to DFS. Financial regulators are independent in its functioning, but largely depend on the Government (Policy Maker) to formulate policy related to Financial Inclusion.

4.2.3. **Telecommunications Authorities / Regulators:** The Telecommunication authorities/Regulators are playing a prominent role in DFS policy development. The mobile network operators (MNOs) are vital players in the DFS ecosystem as the Digital Financial services are being provided using mobile network and mobile phones. Telecommunication authorities play a significant role in maintaining QoS, data privacy & security, consumer protection, inter-operability, and provision of telecommunications carrier channels such as Unstructured Supplementary Service Data (USSD). The telecom regulator also regulates the tariff and carriage of USSD services which is using telecom network.

4.2.4. **Third Party Service Providers:** In some countries DFS is offered by Third Party Service Providers (TPSP). All TPSPs are required to get a license from the Telecom authority/regulator and authorization by the Central bank to provide interoperable mobile banking services. All TPSPs and operators are required to enter into Service Level Agreements (SLAs) with Central Bank authorized Financial Intuitions (AFIs).

4.2.5. **Competition Authority:** Sectoral regulations may contain competition provisions which apply prior to the occurrence of actions (ex-ante) that may require intervention to ensure a fair and level playing field. Competition law may empower both sectoral regulators and competition authorities. This approach also allows for market investigations and inquiries to determine if an entity has market dominance or is SMP (Significant Market Power) based on its market size and other market factors.There are competition related issues when USSD channels of MNOs are accessed by agent networks to provide services. The issue of competition will come into play when more players get into provisioning of DFS. Therefore the Competition Authority will also play a significant role in regulating the Digital Financial Service.

4.2.6**. Data Privacy and Consumer Protection:** Providing consumers with information and transparency in all digital financial services and products is crucial to develop trust and uptake. Absence of information is likely to result in consumer’s lack of knowledge and awareness on key product features, terms & conditions, which heightens the risk to consumers. Therefore it is vital that the service providers are transparent about their services and products so that consumers have the opportunity to make informed choices and avoid risks such as agent misconduct, overcharging or misleading advertisements and scams. To take care of consumers’ interests, the regulators should have in place a consumer grievance redress mechanism. In case of any disputes, the consumers should have access to Consumer Redressal Forums and appellate authority to safe guard their interest. Securing of personal data of the consumers is also vital. There are departments within the regulatory environment which can take care of privacy related issues. However, the privacy laws are still evolving and legal framework to handle privacy related issues are still developing in SATRC countries.

4.2.7. **Tax Authorities**: Promotion of electronic payments needs to be done with tax incentives. Therefore, Tax authorities will play an important role in development of Digital Financial Services. Digitalisation has huge implications for taxation, impacting tax policy and tax administration at both the domestic and international level, offering new tools and introducing new challenges. As a result, the tax policy implications of digitalisation have been at the centre of the recent global debate over whether or not the international tax rules continue to be ‘fit for purpose’ in an increasingly changing environment at the global level.

4.2.8. **DFS Ecosystem**: The Focus Group constituted by International Telecommunications Union (ITU) has brought out the DFS Ecosystem[[2]](#footnote-2) in the diagram, which is reproduced below, clearly explains the involvement of various stakeholders.



# 

# CHAPTER-5: AUTHENTICATION MECHANISMS

**5.1. Authentication**

5.1.1. It is an accepted practice and norm for a customer to get registered for availing any services from any financial institution including bank. This is the same for availing Digital Financial Services. While opening an account the consumer has to provide some form of identity documentation/proof. In many countries it is required to provide a properly authenticated digital identity, as in the case of ‘Aadhaar’ in India. The information provided by the customer will be matched with the data base of the Authority which maintains the Identity Scheme, by the bank/DFS operator.

5.1.2. Once an account has been opened, any use of service by the customer, whether it is related to account maintenance or to transactions, must be authenticated. How this can be achieved is an important decision. In the case of India it is a requirement that all such touchpoints should be authenticated against the national identity service.

5.2. **Authentication using National Digital Identification system**

5.2.1. [[3]](#footnote-3)Given below is a practical example of how a provider of digital identity services and a mobile money (DFS) operator may collaborate in order to gain mutual benefit, which is depicted in the figure given below. This illustrates a scenario where a consumer has pre-registered with a state issued eID scheme and leverages that identity during the application for a mobile money account.

The process is as follows:

a. Consumer cryptographically signs an application for a mobile money account using their state-issued eID card via a compatible agent owned smartphone.

b. The mobile money operator requests the personal attributes of the consumer from the eID scheme using the signed application.

c. Once the relevant data has been received, the mobile money operator (in this instance also a MNO), uses the data to create and issue a functional identity for the consumer via the mobile connect service. From that point onwards, the consumer is able to authorise mobile money transactions via their mobile connect identity.

5.2.2. The benefits of the model described include reduced friction during customer registration with the mobile money provider, increased convenience for the customer when authorising transactions and access to other services within the mobile connect ecosystem. However whether such a scheme would turn into a success would be dependent on the specifics of the user experience, commercial structure, and functionality of the DFS product.



5.3. **Authentication methods being followed in SATRC countries**

5.3.1 In most of the SATRC countries the process of account opening, and transactions are authenticated by PIN Code. MFS platforms have to ensure that proper protection and security features are maintained in issuing and authenticating the PINs and other securing mechanism. In some countries an OTP (one time password/Pin) is sent to the registered mobile number of the customer and the authentication is established. The national identity number needs to be mentioned while account opening which make KYC verification easier using bio-metric credentials (Examples - India & Pakistan). In Pakistan bio-metric verification is required to open a mobile/branchless banking account. There is Rs.10 charges for biometric and CNIC data verification from NADRA, which is born by the respective bank, there is no upfront charges for customers.

5.3.2. Sri Lanka uses KYC information for authentication and opening of account with daily transaction limits and documentation (Clear NIC Copy/subscriber application form/billing proof if different to the NIC Address). For authentication for transactions, customers have to long in to mobile Cash App/USSD by using the mobile Cash PIN. Also the PIN is required to perform each transaction. Further transaction confirmation is sent to the customer via SMS.

5.3.3. In some countries, the social media data is used for authentication for accessing DFS. For example[[4]](#footnote-4) Sterling bank in Nigeria has partnered with lending platform Social Lender to enable consumers to apply for loans by providing access to their social media data. For example, individuals register on the Social Lender platform via Facebook Connect. Once access to their personal information is authorised, consumers are assigned a credit score based on a proprietary algorithm. This score can be used to apply for loans from the bank.

# CHAPTER-6: INTERNATIONAL BEST PRACTICES

**6.1. India - Creation of Digital Infrastructure (Aadhaar) and provision of Digital Financial Services in India**

6.1.1. Aadhaar identity platform is one of the key pillars of ‘Digital India’, wherein every resident of the country is provided with a unique identity or Aadhaar number. With enrolment of more than 1.25 billion people, this is the largest biometrics-based identification system in the world, Aadhaar is a strategic policy tool for social and financial inclusion, public sector delivery reforms, managing fiscal budgets, increase convenience and promote hassle-free people-centric governance. It is unique and robust enough to eliminate duplicate or fake identities and may be used as a basis/primary identifier to roll out several Government welfare schemes and programmes for effective service delivery thereby promoting transparency and good governance.

6.1.2. With the foundation laid by the Aadhaar authentication ecosystem and properties of Aadhaar, UIDAI established a new payment system for the country by getting into an exclusive partnership with National Payments Corporation of India (NPCI). NPCI then launched following products:

#### 6.1.3 **Aadhaar Payment Bridge (APB):** Aadhaar Payments Bridge is conceived to be a repository of the Aadhaar numbers of residents and their primary bank which they intend to use for receiving all social security and entitlement payments from the government.

#### 6.1.4. **Aadhaar Enabled Payment System (AEPS):** Aadhaar Enabled Payment System (AEPS) enables banks to route the interbank financial transactions through central switching and clearing agency to empower the resident to use Aadhaar as his/her identity to authenticate and subsequently operate his/her respective Aadhaar Enabled Bank Account (AEBA). Through Aadhaar Enabled Payment System the residents of India primarily Rural India get empowered to make basic financial transactions (Credit, Debit, Balance Enquiry, etc) directly through microATMs deployed by Banks in their villages.

6.1.5. **Aadhaar and Unified Payment Interface (UPI)**: UPI is a major innovation in banking that helps solve a lot of the same problems that a debit card was facing earlier. It uses a mobile as a way to authenticate one’s identity, essentially turning the phone into a debit card that can be used anywhere. UPI will allow a customer to have multiple virtual addresses for multiple accounts in various banks. In order to ensure privacy of customer’s data, there is no account number mapper anywhere other than the customer's own bank. This allows the customer to freely share the financial address with others. A customer can also decide to use the mobile number or Aadhaar number as the name instead of the short name for the virtual address.

6.1.6.**The JAM Trinity:** Keeping in view the potential of mobile telephony in improving ‘last mile’ delivery of financial services, the Government of India envisaged the concept **‘JAM Trinity’** - **Jan Dhan - Aadhar - Mobile trinity**. Under the JAM trinity, the Government has linked citizen’s bank account number and mobile number with Aadhar number with an aim to better target and transfer financial resources to the poor. It is to spur the goal of financial inclusion in the country. The Pradhan Mantri Jan Dhan Yojana, aims to ensure access to various financial services like availability of basic savings bank account, access to need based credit, remittances facility, insurance facility, insurance and pension to the excluded sections that is weaker sections and low- income groups. The plan also envisages channeling all government benefits (from Centre/State/Local body) to the beneficiaries account and pushing the Direct Benefits Transfer (DBT) scheme of the Union Government.

**6.2 Pakistan – Progressive Regulations and Successful bank-operator partnerships**

6.2.1. Rapidly developing digital financial technologies via mobile phones provide an opportunity to offer financial services efficiently and at a much lower cost, while providing access to wider segments of society. Over the years, Pakistan Telecommunications Authority (PTA) has successfully partnered with the financial regulator, Fintechs, mobile operators and international development agencies to tap this opportunity to improve lives and strengthen development.

6.2.2. **Supportive Regulations for Bank-Operator Partnership**: The basic regulatory framework for mobile financial services was provided by two policy initiatives by the central bank of Pakistan i.e. State Bank of Pakistan (SBP): (i) Enactment of Payment System and Electronic Fund Transfer Act in 2007, and (ii) Issuance of Branchless Banking Regulations in March 2008. Under these regulations, one-to-one arrangements were allowed for the provision of branchless banking services by authorized branchless banks with joint venture with telecom companies / mobile operators as principle agent. In order to facilitate further development of the sector, SBP updated its Branchless Banking Regulations in 2011, 2016 and 2019.

6.2.3 **Successful one-to-one arrangements**: With the light touch and progressive regulatory framework, the one-to-one arrangements between mobile operators and banks have revolutionized the provision of banking services to the unbanked and poor in Pakistan with over 47 million mobile financial accounts (m-wallets) and a network of above 437,000 mobile banking agents against only 13,000 traditional bank branches. In 2019, there were over 1.3 billion annual mobile banking transactions (3.6 million daily transactions) with an annual volume of over Rs. 4.5 Trillion (Rs. 12.3 billion worth of daily transactions). Mobile operators have played a vital role in this success, which was never foreseen by the traditional banking sector. Two mobile operators-partnered banks, Mobilink Microfinance Bank (Jazz cash) and Telenor Microfinance Bank (Easy paisa), are main players in the mobile banking market with 90% market share in m-wallet accounts and 68% in active agents and have received international recognitions / awards for best mobile money providers.

6.2.4 **Biometric Verification System**: PTA’s initiative for the biometric verification of SIMs in 2014 along with a strong national identity (biometrically verified) database has played a pivotal role in the growth of m-wallets in Pakistan. It allowed the financially excluded population to open m-wallets remotely through USSD channels and Biometric Verification System devices installed at agent locations.

6.2.5**Mobile Banking Interoperability:** To facilitate interoperability for mobile / branchless banking across all mobile operators and banks, PTA and SBP jointly issued “Regulations for Technical Implementation of Mobile Banking, 2016” and “Regulations for Mobile Banking Interoperability, 2016”. Vide these regulations, Third Party Service Providers (TPSPs) have been allowed to provide technical services for interoperable mobile banking. PTA issues licenses to TPSPs whereas SBP issues authorization for the payment system. This regulatory framework provides opportunity for the technical service providers and operators / banks to come forward with their advanced solutions that will make available interoperability on payments and across platforms.

6.2.6 **TPSP Licensing**: Under the above regulations, PTA has started issuing License(s) to grant the successful applicants’ rights with the mandate to establish, maintain and operate telecom system as TPSP for financial and application services across Pakistan. TPSP license permits the licensee to provide technical services for channeling, routing, and switching transactions for branchless/mobile banking among SBP’s Authorized Financial Institutions (AFIs), telecom operator(s) and TPSP(s). TPSP works as a catalyst for interoperability in the mobile banking domain and settling of “any to any” transactions involving multiple financial institutions at the back end and multiple networks at the other end.

6.2.7 **Unified USSD Channel Platform /** **Asaan Mobile Account Scheme:** Government of Pakistan launched National Financial Inclusion Strategy (NFIS) in 2015. Under NFIS, PTA and State Bank of Pakistan (SBP) worked with stakeholders to launch an integrated platform / interoperable solution (Asaan Mobile Account (AMA) scheme). This allows any person with a basic mobile phone to swiftly open a digital transaction account through a USSD code from anywhere, at any time with any bank from any mobile operator’s network. PTA has issued two licenses to Fintechs / TPSPs to play a catalyst role to provide technical services for the interoperability of innovative digital solutions for financial inclusion. Pilot project of AMA scheme has already been completed after required interconnection arrangements among mobile operators, TPSPs and banks and AMA scheme will be launched commercially soon. This will enable all mobile subscribers to remotely open a bank account of any of the currently 14 branchless banks from any of the four mobile networks without the need of internet connectivity.

# CHAPTER-7: CHALLENGES

**7.1 Challenges in provisioning of DFS**

7.1.1. The recent growth of digital financial services has allowed millions of people who are otherwise excluded from the formal financial system to perform financial transactions relatively cheap, secure, and with reliability. The benefits of digital finance extend well beyond conventional financial services. This can also be a powerful tool and an engine for job creation in developing countries.

7.1.2. During the COVID pandemic crisis, there is a rapid increase in the online economic activities including online banking, e-commerce and because of this sudden surge in the economic activities, the challenges in securing the network from cyber criminals have increased. The measures to provide cyber security is very crucial for the success of DFS. At the same time, there are no adequate cyber-crime law in SATRC countries to deal with the situation. Some of the challenges in the DFS eco-system are discussed here.

**7.2. Regulatory challenges**

7.2.1. There are number of regulatory challenges in this new type of services. The existing DFS regulations may become redundant in view of the evolving and innovative new technologies and services. Therefore, the traditional regulatory paradigm of regulating the traditional provider of financial services has to change and the regulators will have to shift from regulating the entities to regulating the activities.

7.2.2. To promote trust and confidence in DFS by the various stakeholders, the regulatory framework must be robust, predictable, non-discriminatory, and transparent. Lack of these attributes can confuse the roles of different participants and create mistrust in the development and operation of DFS. The legal and regulatory framework should provide an adequate balance to promote innovative business models, as well as foster sound risk management practices in the payments industry, including through the supervision/oversight of PSPs and PSOs by regulatory authorities.

7.2.3 Further, to promote transparency and predictability, before implementing new or amending existing laws or regulations in connection with DFS, regulators should carefully evaluate the full costs and benefits of such proposed laws or regulations. Laws/regulations should be drafted carefully to minimize the risk of unintended consequences and should focus on clear, articulated goals or purposes[[5]](#footnote-5).

**7.3. Competition Issues**

7.3.1. The DFS ecosystem transcends across multiple regulatory domains and may involve multiple regulators or authorities. There are regulatory issues which are overlapping in the jurisdiction of Financial Regulator (Central Bank), Telecommunications regulator, Payments regulator, Financial Intelligence wing (Economic offence wing), Competition Regulator etc. In most of the cases for DFS, the Financial services regulator (Central Bank) is the lead regulator. Telecommunications regulators usually act in a supporting role, with their jurisdiction mostly limited to issues related to the telecommunications channel & network.

7.3.2. There are many interpretations on the term ‘competition’ which should be applied to digital economy. In this regard there are multiple theories about how competition-based precepts should be applied to the digital economy, but generally competition-related jurisdiction and power is founded through sectoral regulations and national competition law.

7.3.3. Not all SATRC countries have an exclusive competition law or independent competition regulator. Often, the competition powers are found in sectoral regulation, such that each of the sectoral regulators may have mandates that allow them to intervene in their sector if there is a competition-related concern. For example, in India the competition related issues are being dealt by Competition Commission of India (CCI) and the jurisdiction on competition issues with regard to telecom services are still largely lies with telecom regulator. This may be differently handled by authorities of different SATRC countries.

7.3.4. In some jurisdictions, competition policies or laws are available to guide sector regulators to help them deal with competition-related issues. Because of jurisdictional conflicts, coordination on competition issues has been found to be useful in preventing regulatory arbitrage. This has usually taken the form of a memorandum of understanding (MOU) between the regulators which has outlined who has jurisdiction over a specific issue or sets of issues and the remedies available, if any. Or, the legislature may intervene to specifically carve out competition-related roles.

**7.4. Consumer Interests/Creation of consumer awareness**

7.4.1. Digital financial services are bringing in large number of people in its fold and hence there has to be strong consumer education and protection, including promoting financial literacy and fraud prevention. Systemic approach should be adopted to bring unbanked consumers gradually to make them as digital user. During each process the consumers need to be educated and awareness programme should be conducted to make them aware of the pros and cons of digital banking. The stages of bringing people into digital inclusion are depicted below.

7.4.2. Service providers need to invest more time and money to make digital financial services a viable business including increased marketing and advertisement campaigns to educate the customers on the different types of services.

7.4.3. The availability of affordable smart phones has helped the low income and rural population to have access to the Digital Financial services, which is otherwise expensive for them to access formal banks and financial services. This increased access to formal services by the rural population has seen as an important development goal which helps in economic growth and reduce poverty. The legal and regulatory frameworks which govern DFS play a critical role in creating an enabling environment for low income and unbanked populations to become financially included. One important aspect within regulation is how the rights and interests of consumers are protected and promoted. Consumer trust is the foundation for achieving sustainable uptake and active usage of DFS. This includes protecting consumers from fraud, safeguarding personal data and consumer funds, ensuring transparency, and ensuring recourse mechanisms are available.

7.4.4. Financial consumer protection has gained increased attention during this COVID-19 pandemic when there is a sudden increase in the online activities and business. Therefore, the service providers need to be transparent in their business conduct, disclose key information about their products and services, and treat consumers fairly and ethically

7.4.5. An effective consumer protection framework within DFS can increase consumer confidence thereby increasing adoption and active use of the services. This is even more important for unbanked users who may not have prior experience with formal banking services (World Bank, 2014). While the interests of consumers (and especially low-income consumers to increase financial inclusion) are important it is also imperative that the legal and regulatory framework remains fair and balanced for all stakeholders (World Bank, 2015).

**7.5. Interoperability**

7.5.1. Interoperability in UPI: The open API architecture enables individuals to use a single bank or payment service application to manage their money residing in multiple banks, as well as to execute and receive payments through UPI. As an example, retail customers can conduct transactions on their accounts at Bank A from inside the mobile banking app of Bank B. The greater ease of transferring funds between banks offered by UPI ensures greater competition on bank interest rates and services. Likewise, as long as the interfaces are linked to a UPI member bank, users can use fintech or big tech interfaces that they are familiar with to execute payments. However, the incompatibility issues between handsets and required software to access services needs to be addressed.

7.5.2. Similarly, the Prepaid Payment Instruments (PPIs) should have interoperability for seamless transaction and usage of these instruments. In India, the Reserve Bank of India (RBI) had issued Guidelines to all Bank and Non-Bank Prepaid Payment Instrument Issuers, System Providers and System Participants on 19th May 2021 mandating interoperability of Prepaid Payment Instruments (PPIs). These guidelines require all participating PPI issuers shall be guided by the technical specifications / standards / requirements for achieving interoperability through UPI and card networks as per the requirements of National Payments Corporation of India (NPCI) and the respective card networks. NPCI and card networks shall facilitate participation by PPI issuers in UPI and card networks.

7.5.3. In order to introduce operator level interoperability and facilitate technical implementation of mobile / branchless banking in Pakistan, PTA and the Financial Regulator “State Bank of Pakistan (SBP)” have jointly framed regulations under the title of “Regulations for Technical Implementation of Mobile Banking, 2016” and “Regulations for Mobile Banking Interoperability, 2016” on 16th May, 2016 available at <https://www.pta.gov.pk/assets/media/mbanking1652016-3.pdf> and <https://www.sbp.org.pk/bprd/2016/C3-Annx-A.pdf> respectively. These regulations are applicable on mobile operators, Third Party Service Providers (TPSPs) and financial institutions that offer m-banking services.

**7.6. Security and privacy related issues**

7.6.1 With the increase in number of transactions through digital means and primarily the mobile, considerable investment would need to be made in the security systems. Besides fraud and theft, digital financial services could facilitate financial flows for illegal or illicit purposes.

7.6.2. There are many other emerging security threats within the DFS ecosystem from cyber-enabled attackers to the expansion of the stakeholders into numerous and sometimes competing parties. This document provides an overview of security challenges and threats that face the DFS environment. Multiple stakeholders need to be involved in order to secure the DFS environment. This requires that security be managed at multiple layers, from operational policy to securing associated hardware and software.

**7.6.3 Recommendation ITU-T X.805 Security Management Standard**

The service management approach taken by [ITU-T X.805] is founded upon eight ‘security dimensions’, which are measures designed to address a particular aspect of network security, taken originally from [ITU-T X.800]. The eight dimensions are as follows:

* **Access control:** Protection against unauthorised use of network resources.
* **Authentication:** Methods of confirming the identities of communicating entities.
* **Non-repudiation:** Methods to prevent an individual or entity from denying having performed a particular action.
* **Data confidentiality:** Protection of data from unauthorised disclosure.
* **Communication security:** Assurance that information only flows between authorized endpoints.
* **Data integrity:** Protection of the correctness and accuracy of data.
* **Availability:** Prevention of denial of authorized access to network elements and data.
* **Privacy:** Protection of data information that might be derived from observing network activity.



# 

# CHAPTER-8: RECOMMENDATIONS

**8.1. Recommendations by Working Group of SATRC**

8.1.1. To achieve the Digital Inclusion strategy of each of the SATRC member country, it is important that the digital financial services are delivered as affordable, accessible, secure, transparent, and robust services. The Working Group on Policy, Regulation and Services prepared the SATRC Report on the Digital Financial Services on the basis of the study undertaken. After analyzing the DFS eco-system which exist in member countries of SATRC and on the basis of our consultations and inputs received, the Working Group submits the following recommendations related to pertinent issues in the delivery of Digital Financial Services and the regulatory bottlenecks. In view of the evolving nature of the Digital Financial Service and the regulatory issues, these recommendations address the issues which are existing currently and suggest possible solutions.

**8.2. Collaborative Regulation:** The regulatory issues relating to provision of Digital Financial Services transcends across more than one sector and therefore the regulatory jurisdictions of each of these sectors overlap. Therefore, all the regulators need to have service based approach, so that all the service providers, both bank and non-bank regulated DFS providers are subject to similar regulations and therefore similar rights & obligations as other DFS providers, while recognizing the challenges of managing different channels. To address these issues, the regulators of concerned sectors should collaborate and come up with a broad -based, over-arching regulation.

8.2.1. In this new evolving scenario, both ICT regulators and financial regulators should recognize common interests and the potential areas of cooperation. However, so far there is no consensus on a model for collaboration has been arrived yet. There are many pertinent issues that demand such collaboration, such as e-commerce, mobile money, data security, handling of personal data etc. One sector regulator should trust other regulators to give equal importance to these issues. When such issues transcend from one jurisdiction to other, there may be a probability of unequal regulatory treatment.

8.2.2. Bringing the regulators, particularly the ICT regulator and the Financial Regulator on a same level ground will create an atmosphere to collaborate and discuss. This is possible only through some bi-lateral understanding through signing of Memorandum of Understanding (MoU) with mutually agreed areas of cooperation. The contentious issues can be addressed by a specially set up joint committees having representations from concerned parties. Many countries have started initiatives to bring all the regulators on a common platform and one such initiative in India is the formation of Forum of India Regulators (FOIR) which has 36 regulators as members. Some of the important regulators representing sectors like Telecom & Broadcasting, Energy, Competition etc are members on FOIR. Similar initiatives in other SATRC countries would also be helpful in promoting collaborative regulation.

8.2.3. Financial and Telecom Regulators of SATRC countries may develop a broad based, joint regulatory framework for the promotion of DFS in SATRC countries. For effective working on various issues related to DFS, MoUs and formation of Joint Working Groups having representations from SATRC countries are also suggested.

**8.3. Interoperability:** Interoperability between two operators and devices should be facilitated to promote convenient, seamless financial transaction between one customer to another belonging to two different operator/network. There should not be any restrictions to access telecom infrastructure. It will be desirable to have a transparent policy on the interoperability arrangement and the policy should be made by the lead stakeholders in consultation with all other stakeholders to have unanimity. This lead stakeholder could be the Financial Regulator (Central Bank) who plays an important role in DFS.

8.3.1 The interoperability issues may also be handled by the umbrella organization such as National Payments council for operating retail payments and settlement system in the country. This entity can provide infrastructure to the entire Banking system in the country for physical as well as electronic payment and settlement systems and also to be focused on bringing innovations in the retail payment systems through the use of technology for achieving greater efficiency in operations and widening the reach of payment systems.

**8.4. Level Playing Field:** Proper coordination between financial institutions (Banks) and Mobile Network Operators (MNOs) for carrying out the data traffic over the mobile network without any discrimination. In some countries the MNOs also providing DFS. Therefore, the level playing field should be ensured for all the service providers irrespective of their status while providing Digital Financial Services. Interoperability should be facilitated by the Telecommunications Service Providers (Mobile Service) by providing level playing field for all the types of stakeholders while using telecom infrastructure. There should not be any discrimination between MNOs who are also DFS providers and other DFS providers.

**8.4.1**. To keep the payment market and DFS ecosystem stable, if the national laws permit, all the PSPs and PIPs may be granted license or authorization and the overall regulation should be done by the Central bank. However, these licenses and authorizations should depend on the specific type of services offered and the specific risk associated to those services and to be regulated accordingly. This will bring in a level playing field amongst all the service provides.

**8.5. Network Security & Fraud Elimination:** The MNOs and DFS Providers should ensure that adequate measures have been taken to safeguard the customer as recommended as per ITU standards. With the digitization of payments and banking services, there has been an increase in frauds committed using digital channels especially using mobile phones. Fraud trends include social engineering frauds (banking customer’s confidential details/card details, passwords, OTP etc. are obtained by unknown callers pretending as someone from their banks, financial regulator, armed forces etc.); call spoofing (fraudsters spoofing the official helpline numbers of banks to obtain customer confidential data); unauthorized registration of mobile apps of financial institutions, etc.

8.5.1. Financial and Telecom Regulators may form a joint working group for a comprehensive review of digital frauds and to propose recommendations to tackle these frauds. The specific set of recommendations may be considered for both regulators to be issued to their regulated entities. The Working Group should be an ongoing forum with following objectives: Review trends in social engineering frauds in banking services using telecom/mobile service channels including emerging fraudulent vectors and suggest high-level security governance and possible controls; assess and recommend data security controls for protection of customer’s data including financial data; develop a mechanism for regular coordination between financial regulator, financial institutions, telecom companies, telecom regulator and other agencies for dealing with digital banking frauds. The Working Group should also collaborate with telecom/banking industry to create educational/awareness campaigns for users to protect them from digital frauds.

8.5.2. National level Cyber Security Policies of each of the SATRC country should specifically address issues related to Digital Financial Services, and mandatory security measures to be put in place through legislation.

**8.6 Security on Mobile Devices:** The end-to-end encryption should be ensured to safe-guard the financial transactions between two entities. The new mobile devices are coming up with additional hardware/software to improve data security and DFS providers should be aware of this provision on the device. DFS Providers should recommend the use of mobile devices that support such strong authentication mechanisms.

8.6.1. The authentication methods used by the DFS providers in SATRC countries are largely through mobile phones by the method of creating one time password (OTPs). Therefore, the Device manufacturers and MNOs should ensure that regular security updates are pushed to devices. Because security updates are critical to ensuring that mobile operating systems running on mobile devices are properly functioning and secure against exploits, potentially rendering DFS applications vulnerable, there should be mechanisms in place to ensure that security patches are made easily accessible to user devices.

8.6.2. Device manufacturers and MNOs should ensure that the handset operating system is configured in a way that reduces the size of the trusted computing base and the attack surface. Hardware and software mechanisms within mobile devices, such as secure elements and trusted execution environments can aid in the reduction of the TCB and help to ensure device integrity. Mobile devices that are so equipped should be promoted for use in DFS.

**8.7. Safe-Guarding of Consumer Interests:** The Digital Financial Service providers may create a consumer grievance redressal mechanism for addressing the internal complaints. Consumer should be educated on the available products and services which will enable them to take informed decisions. MNOs and regulators should undertake active customer awareness campaigns to educate consumers about malicious messages, phishing, and spoofing attacks etc.

8.7.1. As already mentioned above, joint regulatory frameworks and joint working of Financial and Telecom Regulators are also important to effectively tackle consumer issues and frauds related to DFS. For consumer protection, Financial and Telecom Regulators have their own consumer protection regulations, however, working groups and collaborations / harmonization with relevant regulators are recommended. A diagnostic study may be carried out to identify the risks and gaps in existing regulatory frameworks related to data privacy and security issues of DFS, and accordingly collaborative actions be framed.

**9. Conclusion:**

9.1 Digital Financial Services (DFS) is an evolving sector, and the eco-system will change as more innovation and technological advancements will enter this sector. The existing regulatory mechanism needs to evolve itself to adapt to the realities of new digital transformation. Therefore, the members of SATRC may continue to engage in multi-level cooperation and collaboration with one another, which will help to formulate the best policy and regulatory parameter to suit their DFS eco-system.

\_\_\_\_\_\_\_\_

**LIST OF ACRONYMS**

AEBA - Aadhaar Enabled Bank Account

AEPS – Aadhaar Enabled Payment System

APB - Aadhaar Payment Bridge

AFI - Authorized Financial Intuitions

CNIC - Computerized National Identity Card

DFS- Digital Financial Services

EMI - Electronic Money Institute

FMI - Financial Market Infrastructure

ICT - Information and Communication Technologies

ITU- International Telecommunications Union

IVRS - Interactive Voice Response System

JAM - Jan Dhan - Aadhar - Mobile

KYC - Know Your Customer / Client.

MFS- Mobile Financial Services

MNO - Mobile Network Operator

MOU - Memorandum of Understanding

NADRA - National Database & Registration Authority

NFIS - National Financial Inclusion Strategy

NIC - National Identity Card

NFC- Near Field Communications

NPCI - National Payments Corporation of India

OTP - One-Time Password

OVD - Officially Valid Document

PIN - Personal Identification Number

PIP Payment Infrastructure Provider

PML - Prevention of Money-laundering

POS – Point of Sale

P2P - Peer to Peer

PPI - Pre-paid Payment Instrument

PSO - Payment System Operators

PSP - Payment Service Provider

SIM – Subscriber Identification Module.

SLA - Service Level Agreement

SMP - Sales Marketing Plan

TPSP - Third Party Service Providers

UIDAI - Unique Identification Authority of India.

UPI - Unified Payment Interface

USSD - Unstructured Supplementary Service Data

VAS – Value Added Services.

# ANNEXURE – 1

**Questionnaire for Work Item on**

**“DIGITAL FINANCIAL SERVICES”**

Q1. How many Mobile Network Operators (MNOs) are there in your country and how many of them are offering Digital Financial Services (DFS)?

Q2. What are the types of DFS existing in your country offered by MNOs?

Q3. Which agencies/departments are responsible for DFS policy, regulation, supervision, and enforcement in your country? Does Telecommunications authorities/regulator play a role in DFS policy formulation? What is the role of each stakeholder (i.e., Telecom Operator, Telecom Regulator, Finance Regulator, etc.)?

Q4. Under whose jurisdiction the issues such as security, data privacy and consumer protection are handled?

Q5. What is the authentication mechanism for account opening as well as transactions? Is there a fee involved for authentication?

Q6. DFS are having regulatory issues which may overlap jurisdictions of more than one regulator (e.g., Financial Regulator, Telecom Regulator, etc.). Is there a joint working group between financial and telecom regulators? How are these turf issues solved in your country?

Q7. Does USSD (Unstructured Supplementary Service Data) based mobile banking payment services regulated in your country by Telecom Regulators? If yes, what kind of regulatory framework is available to manage these services?

Q8. What is the regulatory framework for DFS? Kindly share links of the relevant regulations and describe main features of these regulations in your response.

Q9. Under which legal instrument(s) (e.g., license condition, rules, act, etc.) the MNOs are offering DFS in your country?

Q10. Do you have specific Telecom license(s) / License conditions / Authorizations for the provision of interoperability for Digital Financial Services? If so, is interoperability provided by a single entity or multiple licensees are allowed?

Q11. What are the challenges being currently faced in the provision of DFS?

# ANNEXURE – 2

**Response to Questionnaire by SATRC Working Group Experts**

**Q1. How many Mobile Network Operators (MNOs) are there in your country and how many of them are offering Digital Financial Services (DFS)?**

|  |  |
| --- | --- |
| **Member Countries** | **Responses** |
| **Afghanistan** | There are five telecom operators in Afghanistan and four of them are providing DFS. |
| **Bangladesh** | There are four (4) MNOs in the country now including one Govt owned operator. Out of these, two operators (2) GP and Robi provides DFS services mostly in collaboration with financial institutions |
| **Bhutan** | There are two telecom operators (Bhutan Telecom Limited and Tashi InfoComm Limited) and only Bhutan Telecom Limited is providing DFS. |
| **India** | There are a total of 5 (five) MNOs in India and out of those, as on date, 2 (two) are offering DFS in India through their group companies. |
| **Iran** | There are three MNOs in operation in I.R.Iran and all of them are providing DFS through Banks and Payment Service Providers. |
| **Maldives** | Two. And both offering DFS. |
| **Nepal** | There are three MNOs in operation in Nepal and all of them are providing DFS through Banks and Payment Service Providers (PSPs) and Payment System Operators (PSOs) licensed by Nepal Rastra Bank (The Central Bank of Nepal). |
| **Pakistan** | There are 4 MNOs in Pakistan and all of them are offering DFS. |
| **Si Lanka** | There are 04 MNOs in Sri Lanka and two of them offer DFS. |

**Q2. What are the types of DFS existing in your country offered by MNOs?**

|  |  |
| --- | --- |
| **Member Countries** | **Responses** |
| **Afghanistan** | MNOs are providing the following DFS services in the country.   * Cash in / Deposit. * Cash out / withdraw * Money Transfer / P2P * Top ups * Electricity bill payment * Purchase goods / Service * Salary payment * Loan payments and Re payments |
| **Bangladesh** | By regulation MNOs in Bangladesh are mostly only permitted to act as bearers - usually via USSD - for banks and other DFS SPs. The types of services mostly includes:   * Bill pay services * Agent banking services in collaboration with financial institutions (banks) |
| **Bhutan** | MNO are providing the following DFS services in the country.   * Intra-Bank Money Transfer * Top ups * Utility/bill payment * Online mobile service bill payment |
| **India** | Indian DFS sector is a bank led model. MNOs were initially allowed only to offer Pre-paid Payment Instruments (PPIs) which means payment instruments that facilitate purchase of goods and services, including financial services, remittance facilities, etc., against the value stored on such instruments. The MNOs are allowed to offer only the semi-closed type of PPIs  for purchase of goods and services, including financial services, remittance facilities, etc., at a group of clearly identified merchant locations / establishments which have a specific contract with the issuer (or contract through a payment aggregator / payment gateway) to accept the PPIs as payment instruments. These instruments do not permit cash withdrawal and can be offered in form of digital wallets, cards etc.  Subsequently, the existing PPI license holders were given an option to convert into a Payments Bank. The Payments Bank is allowed to undertake only certain restricted activities viz., (i) acceptance of demand deposits; (ii) issuance of ATM/Debit Cards (not allowed to issue credit cards); (iii) payment and remittance services etc.  The Payments Bank thus allowed the MNOs to continue their PPI business and also expand the scope of their DFS offerings.  Accordingly, as on date, both the MNOs offering DFS in India have converted their PPI licenses into Payments Bank, which is a separate entity and offering services of a Payments Bank including the PPI offerings. |
| **Iran** | Mobile banking & Online mobile service bill payment |
| **Maldives** | Both MNOs offer DFS through an electronic wallet service and mobile pay system which allows cash-ins and cash-out to the wallet through their customer service offices or registered agents. One operator also allows wallet credit through existing online banking services. |
| **Nepal** | Following DFS services are offered:   * E-Banking * Payment Card * E-Money (Wallet) * Mobile Banking |
| **Pakistan** | In Pakistan, mobile financial services (MFS) are provided through bank-led model, under which, bank account resides with the bank. MNOs are working as super-agent for the relevant banks to offer MFS including various transactions, payments etc. |
| **Sri Lanka** | DFS offered by MNOs in Sri Lanka are as follows:   * Cash in (Deposit money to mobile cash account) * Cash Out (Withdraw money from mobile at any mobile cash retail points) * Top ups * Transfer funds * Utility/bill payments * Pay for Goods and Services (pay for Goods & Services purchased at mobile cash merchant points) * Inward Remittance Services (A service to instantly receive foreign remittances directly to your mobile) |

**Q3. Which agencies/departments are responsible for DFS policy, regulation, supervision, and enforcement in your country? Does Telecommunications authorities/regulator play a role in DFS policy formulation? What is the role of each stakeholder (i.e., Telecom Operator, Telecom Regulator, Finance Regulator, etc.)?**

|  |  |
| --- | --- |
| **Member Countries** | **Responses** |
| **Afghanistan** | In Afghanistan, there are two government bodies that make enabling environment for digital financial services. The regulation of telecom network and service is in the domain of Afghanistan Telecom Regulatory Authority (ATRA) and the financial regulation in in the scope of functions of the central bank i.e., De Afghanistan Bank.  De Afghanistan Bank regulating the DFS and have the authority to make policy, regulation, and supervision. Afghanistan Telecom Regulatory Authority just issuing no objection letter to the MNOs and licenses to the VAS service provider that provide DFS in the country through a short code.  MNOs that provide DFS in the country, are having licenses from the Da Afghanistan Bank and have partnership with others private banks. |
| **Bangladesh** | Mainly two (2) departments are involved in DFS policy level decision making in Bangladesh     * Financial Regulator - Bangladesh Bank * Telecom Regulator – Bangladesh Telecommunication Regulatory Commission (BTRC)   Telecom Regulator, BTRC regulates the access of MNOs to DFS services and fixes tariffs and technical procedure for connectivity via USSD for DFS.  Financial Regulator, Bangladesh Bank is the main regulatory authority to issue DFS licenses and permission. They also regulate the financial matters. |
| **Bhutan** | Currently, Financial Regulator or Central Bank – Royal Monetary Authority is responsible for DFS policy, regulation, supervision, and enforcement. |
| **India** | In India, the central bank i.e., the Reserve Bank of India is responsible for DFS policy, regulation etc. Telecommunication authorities/regulator does not play any role in DFS policy, regulation etc. and plays a limited role in policy formulation relating to regulation of services rendered by MNOs as a platform for DFS viz., USSD. |
| **Iran** | Currently, Financial Regulator or Central Bank is responsible for DFS policy, supervision, and enforcement in Iran. Telecommunication does not play a role in DFS. |
| **Maldives** | Maldives Monetary Authority (MMA), which is the central band and financial regulator is the lead stakeholder responsible for policy and regulation of DFS. However, the MMA works in close collaboration with the Telecom regulator CAM in formulating policy and regulations etc.  We have an approach where we have minimalistic regulation. From the telecom side no extra license is required. Whatever rules and regulations that apply in general for the service behind the financial service only will apply. For example, SMS charge. For banking and financial services, regulations from the financial regulator will apply. |
| **Nepal** | Nepal Rastra Bank (NRB) is central bank of Nepal which regulates financial institutions in Nepal. Nepal Telecommunications Authority (NTA) regulates MNOs. NTA provides SMS/IVR/USSD codes to the financial institutions through telecom operators for mobile banking service and Mobile Payment Services. MNOs are providing services to DFS providers under the license terms and condition and regulation from NTA. |
| **Pakistan** | The Central Bank “State Bank of Pakistan (SBP)” is responsible for the DFS regulations, supervision, and enforcement.  Yes, Pakistan Telecommunication Authority (PTA) is playing a role to the extent of formulating regulations for technical implementation of mobile / branchless banking and facilitating SBP in the inter-connect between banks, telecom companies and third party service providers. In this regard, PTA and SBP have jointly framed regulations under the title of “Regulations for Technical Implementation of Mobile Banking, 2016” and “Regulations for Mobile Banking Interoperability, 2016” on 16th May, 2016 available at <https://www.pta.gov.pk/assets/media/mbanking1652016-3.pdf> and  <https://www.sbp.org.pk/bprd/2016/C3-Annx-A.pdf> respectively.  These regulations are applicable on mobile operators, Third Party Service Providers (TPSPs) and financial institutions that offer m-banking services. The regulations provide detailed mechanism for technical implementation of [one-to-one](file:///D:\Documents\Mobile%20Banking\One-to-one%20Model.pptx) and [any-to-any model](file:///D:\Documents\Mobile%20Banking\Any-To-Any%20Model.pptx) of m-banking. All TPSPs are required to get a license from PTA and authorization by SBP to provide interoperable mobile banking services. All TPSPs and operators are required to enter into Service Level Agreements (SLAs) with SBP authorized Financial Intuitions (AFIs). A joint PTA and SBP committee resolve the disputes between the parties and protect consumers’ interest. PTA issues licenses to TPSPs whereas SBP issues authorization for the payment system. This regulatory framework provides opportunity for the technical service providers and operators / banks to come forward with their advanced solutions that will make available interoperability on payments and across platforms. |
| **Sri Lanka** | Central Bank of Sri Lanka (CBSL) is responsible for regulating the Digital Finance Services in Sri Lanka.  CBSL has issued two guidelines in this regard.   1. Mobile Payments Guidelines No. 1 of 2011 for the Bank-led Mobile Payment Services. 2. Mobile Payments Guidelines No. 2 of 2011 for Custodian Account Based Mobile Payment Services   Only the Central Bank of Sri Lanka has the legal mandate to issue license to operate a Mobile Payment System under the Payment and Settlement Systems Act No. 28 of 2005. |

**Q4. Under whose jurisdiction the issues such as security, data privacy and consumer protection are handled?**

|  |  |
| --- | --- |
| **Member Countries** | **Responses** |
| **Afghanistan** | Under the jurisdiction of the Da Afghanistan Bank (Central Bank). |
| **Bangladesh** | Bangladesh Bank. |
| **Bhutan** | Financial institutions and Royal Monetary of Bhutan (Central Bank). |
| **India** | All such issues are primarily handled by the Reserve Bank of India. |
| **Iran** | Security, data privacy and consumer protection are handled in some department of ICT ministry. |
| **Maldives** | Not formally defined yet. Currently shared between the financial and telecom regulator as required. Also, only very small minimum amount transactions are currently allowed through DFS services. |
| **Nepal** | Nepal Rastra Bank (NRB). |
| **Pakistan** | Both SBP and PTA, however, primarily SBP. |
| **Sri Lanka** | * DFS related – Payment and Settlement Systems Dept of the Central Bank of Sri Lanka (under the Payment and Settlement Systems Act No. 28 of 2005) * Telecom companies related – Sri Lanka Telecommunications Act No.25 of 1991 (as amended) including the provisions of the License issued thereunder. * General Consumer Protection – Consumer Affairs Authority Act No.09 of 2003 |

**Q5. What is the authentication mechanism for account opening as well as transactions? Is there a fee involved for authentication?**

|  |  |
| --- | --- |
| **Member Countries** | **Responses** |
| **Afghanistan** | The account opening and transactions are authenticated by PIN Code. In some of the transactions like cash-out and registration National ID and valid photo are part of the authentication mechanism. |
| **Bangladesh** | For account opening customer must fill up a KYC form manually. However, Bangladesh Bank is working on an E-KYC process which is to be introduced soon.  For transaction, all transactions must be authenticated by the account holders using their respective Personal Identification Numbers (PINs) or similar other secured mechanism. MFS platforms must ensure that proper protection and security features are maintained in issuing and authenticating the PINs and other securing mechanisms.  MFS platforms shall also have to follow the ICT Act 2006, and the Guidelines on ICT Security for Scheduled Banks and Financial Institutions 2010 issued by BB, in addressing ICT security issues in mobile financial services.  Currently there are no fees for the customers associated to account opening and transaction authentication. |
| **Bhutan** | An individual needs to provide their valid account number and mobile number for account opening and for the transaction purpose, one has to enter their pin created during the account opening. |
| **India** | The PPI account can be opened by obtaining minimum details of the PPI holder. Such an account is designated as minimum detail PPI. The minimum details shall include mobile number verified with a One Time Pin (OTP) and self-declaration of name and unique identification number of either any of the ‘Officially Valid Document (OVD)’ defined under Rule 2(d) of the Prevention of Money Laundering Rules, 2005, (PML Rules) or any of the mandatory documents, as applicable, under the PML Rules, 2005.  These minimum detail PPIs carry certain restrictions in terms of amount loading, amount outstanding etc. Further, fund transfer from minimum detail PPI to bank accounts or PPIs of same/other issuers are not allowed. Also, a minimum detail PPI can be held for a fixed maximum period only and needs to be converted into KYC (Know Your Customer) Compliant PPI for continued use. The MNOs are following a paperless approach for authenticating account opening as well as transactions.  As regards transactions, the authentication is being done by using the mPINs selected by the PPI account holder.  To the best of information available, no MNO is charging a fee for authentication. |
| **Iran** | It is managed by regulatory of central bank. No. |
| **Maldives** | National Identity Card No. has to be entered for registration. This is cross verified against mobile number and followed by OTP authentication and set up of secure pin. Fee is not required for authentication. |
| **Nepal** | One Time Password (OTP) and Transaction PIN code are used as the authentication mechanism for account opening as well as transactions. Tariff for SMS will be applicable for initiation of transition. |
| **Pakistan** | Biometric verification is required to open a mobile / branchless banking account. There is Rs. 10 charges for biometric and CNIC data verification from NADRA, which is born by the respective bank. There are no upfront charges from customers. |
| **Sri Lanka** | Authentication for account opening:   * Availability of KYC (Basic/Telecom companies KYC for Basic accounts with Rs 10,000 daily limit and Additional KYC for enhanced accounts with Rs 50,000 daily limit) and documentation (Clear NIC copy / Subscriber Application form / Billing proof if different to the NIC address) * No fee involved for the customers for authentication   Authentication for transactions:   * Customers have to log in to mobile Cash App/USSD by using the mobile Cash PIN. Also, the PIN is required to perform each transaction. * Further transaction confirmation is sent to the customer via SMS |

**Q6. DFS are having regulatory issues which may overlap jurisdictions of more than one regulator (e.g., Financial Regulator, Telecom Regulator, etc.). Is there a joint working group between financial and telecom regulators? How are these turf issues solved in your country?**

|  |  |
| --- | --- |
| **Member Countries** | **Responses** |
| **Afghanistan** | There is no joint working group between regulators but there is cooperation between the two regulatory bodies regarding the service. |
| **Bangladesh** | Both BB and BTRC have important regulatory role in DFS. For DFS expansion agenda there are adequate institutional coordination between BB and BTRC with BB taking the lead on financial matters, while BRTC taking the lead on telecom related issues.  The BB and BRTC also periodically hold joint consultation meetings with MFS providers and MNOs to find out industry regulatory concerns and get them resolved on a timely basis. |
| **Bhutan** | There is no joint working group between Financial and Telecom regulators, but we are working towards forming a working group. |
| **India** | To the best of information available, there are no such joint working groups. |
| **Iran** | No. |
| **Maldives** | Yes, there is a joint working group with close cooperation and collaboration between the regulators with the common goal of making digital financial services effective with minimalistic regulations. |
| **Nepal** | NTA and NRB have signed Memorandum of Understanding (MoU) for development and regulation of Mobile Financial Services and Mobile Payment Services in Nepal. This MoU has provisioned a Joint Coordination Committee comprising representatives from both regulators. |
| **Pakistan** | In order to provide enabling environment for DFS, SBP and PTA have signed MoU, under which there is a joint regulatory committee to periodically review the market and discuss and resolve related issues. |
| **Sri Lanka** | There is no joint working group between financial and telecom regulators but there is a close cooperation between the two regulators. |

**Q7. Does USSD (Unstructured Supplementary Service Data) based mobile banking payment services regulated in your country by Telecom Regulators? If yes, what kind of regulatory framework is available to manage these services?**

|  |  |
| --- | --- |
| **Member Countries** | **Responses** |
| **Afghanistan** | Yes, we are regulating USSD based mobile banking payment services and there is VAS procedure and according to that procedure multiple licenses are issued to provide USSD based mobile banking services through a short code. Central bank (Da Afghanistan Bank) is tending to also provide facilities for a central payment switching the connectivity of all networks to be based on mutual agreed mechanism for the services. |
| **Bangladesh** | Telecom Regulator BTRC fixes the tariffs and technical integration procedures of USSD sessions in USSD based MFS solutions.  There a directive issued by BTRC in this regard.  <https://bit.ly/2rBDvcD> |
| **Bhutan** | Yes, USSD based mobile banking payment services follows the National Numbering plan of Bhutan. |
| **India** | Yes, USSD based mobile banking payment services are regulated in India by the Telecom Regulator.  The Department of Telecommunication has allocated a USSD code \*99# for mobile banking services through the USSD gateway and asked the telecom service providers (TSPs) to connect to it as per the requirement of service. Subsequently, the Telecom Regulator mandated that every Telecom Service Provider shall facilitate the banks to use SMS, USSD and IVR to provide banking services to its customers and deliver the message generated by the bank or the customer within a specified time frame.  Further, the Telecom Regulator has prescribed ceiling tariff of Rs. 0.50 per USSD session for USSD-based mobile banking service and established a framework to facilitate the agents of the banks to interface with the access service providers for use of SMS, USSD and IVR channels to provide mobile banking services. |
| **Iran** | No. |
| **Maldives** | No. |
| **Nepal** | There is no USSD based mobile banking payment services in Nepal till date. |
| **Pakistan** | PTA and SBP have joint regulations as mentioned above. Under these regulations, a bank can have an arrangement with a telecom company under one-to-one arrangement. For many-to-many arrangements, there needs to be a TPSP, which is licensed by PTA and authorized by SBP, as discussed above. |
| **Sri Lanka** | No. |

**Q8. What is the regulatory framework for DFS? Kindly share links of the relevant regulations and describe main features of these regulations in your response.**

|  |  |
| --- | --- |
| **Member Countries** | **Responses** |
| **Afghanistan** | In Afghanistan, there are two government bodies that make enabling environment for digital financial services. The regulation of telecom network and service is in the domain of Afghanistan Telecom Regulatory Authority and the financial regulation is in the scope of functions of the central bank.  Following are the links for the regulations for DFS / mobile financial services.  Regulation on Electronic Fund Transfers: <http://dab.gov.af/sites/default/files/2018-12/EFTRegulation21220178464453353325325.pdf>  Electronic Money Institution Regulation: <http://dab.gov.af/sites/default/files/2018-12/EMIsRegulation-201616112016153619417553325325.pdf> |
| **Bangladesh** | <https://www.bb.org.bd/mediaroom/circulars/psd/jul302018psdl04e.pdf> |
| **Bhutan** | e-Money Issuer Rules and Regulations 2017 issued by the Central Bank of Bhutan |
| **India** | The regulatory framework has been discussed in response to aforesaid queries. The links of relevant regulations are as under:  Master Direction Issued by the Reserve Bank of India on Issuance and Operation of Pre-paid Instruments (PPIs) - <https://www.rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=11142>  FAQs on PPIs - <https://m.rbi.org.in/scripts/FS_FAQs.aspx?Id=126&fn=9>  Guidelines for licensing of Payment Banks - <https://www.rbi.org.in/scripts/bs_viewcontent.aspx?Id=2900> |
| **Iran** | <https://www.worldbank.org/en/country/iran> |
| **Maldives** | See Answer A3 above. |
| **Nepal** | Followings are the regulatory framework for DFS in Nepal:  **Payment and Settlement Bylaw, 2015** has been formulated for the development of the secure, healthy and competent payment system. It is further required for the fulfillment of purpose of clause (c)\* of Section 4(1) of the Nepal Rastra Bank Act, 2002 for doing the functions related to regulation, supervision and oversight the services and instruments issued by the institutions/ mechanism which operate payment and settlement services and exercise the powers conferred under part (o) of Section 110(2) of the Act. Detail Bylaw can be found at following link:  https://www.nrb.org.np/  psd/bylaws/P&S\_bylaw\_2072\_ii\_amendment\_in\_english.pdf  **Licensing Policy for Institution/Mechanism Operating Payment Related Activities - 2016** has been formulated pursuant to Bylaws 16(2) of Nepal Rastra Bank’s Payment and Settlement Bylaws, 2015 to issue license for establishment of institution/mechanism operating payment related function and their related instrument and transaction. This provision shall also be applied to the institution/mechanism established in Nepal and operating abroad as well as to those established abroad and operating in Nepal. The detail Licensing Policy can be found at following link:  <https://www.nrb.org.np/psd/policies/Licensing_Policy_in_English-2016.pdf> |
| **Pakistan** | **Regulatory Framework for Mobile Financial Services in Pakistan**  The basic regulatory framework for mobile financial services was provided by two policy initiatives by the central bank of Pakistan i.e. State Bank of Pakistan (SBP): i) enactment of Payment System and Electronic Fund Transfer Act in 2007, and ii) issuance of Branchless Banking Regulations in March 2008 available at <http://www.sbp.org.pk/bprd/2008/C2.htm>. Under these regulations, one-to-one arrangement for mobile / branchless banking was allowed for the provision of branchless banking services by authorized branchless banks with joint venture with telecom companies / mobile operators as principal agent. Subsequently MoIT&T announced the Policy Directive (May 2008) to support the technical implementation of mobile banking in the country by introducing a Third-Party Service Providers (TPSPs) model and Pakistan Telecommunication Authority (PTA) was mandated to prepare Regulations for Technical Implementation of Mobile Banking Services. To this end, a joint regulatory committee was formulated between SBP and PTA to work on the technical framework for mobile banking in Pakistan. SBP and PTA also signed MoU in 2012 to develop a cohesive regulatory framework and to assist each other, in achieving the common objective of providing the low-cost mobile banking services. In order to facilitate further development of the sector, SBP updated its Branchless Banking Regulations in in 2011 and 2016 (<https://www.sbp.org.pk/bprd/2011/C9-Enclosure-2.pdf>; <https://www.sbp.org.pk/bprd/2016/C9-Annx-A.pdf>).  **Rules for Payment Service Providers and Payment system Operators, 2014**  To create an enabling regulatory environment and bring systemic harmony, introduce standardization and setting benchmarks, SBP issued Rules for Payment System Operators (PSOs) and Payment Service Providers (PSPs) in 2014 (<http://www.sbp.org.pk/psd/2014/C3-Annex.pdf>). The purpose of PSOs/ PSPs is to provide an electronic platform for clearing, processing, routing, and switching of electronic transactions. It can make agreements with Banks, Microfinance Banks (MFBs), other PSOs and PSPs, Merchants, e-commerce service providers and any other company for the provision of services mandated to the PSO and PSP under the rules.  PSOs/PSPs are important components of Financial Market Infrastructure (FMI) and they are defined in the Rules as “Authorized Party that is a company registered under Companies Ordinance 1984 and is engaged in operating and/or providing Payment Systems related services like electronic payment gateway, payment scheme, clearing house, ATM Switch, POS Gateway, E-Commerce Gateway etc. acting as an intermediary for multilateral routing, switching and processing of payment transactions”.  PSOs/PSPs authorization is granted in three stages i.e. (i) In –Principle approval (ii) pilot Operation approval and (iii) final stage approval. PSOs/PSPs are required to maintain capital of PKR 200 million (Rupees Two Hundred Million Only) or any other amount as may be prescribed by SBP from time to time capital and for each additional line of business they an additional amount of  25% of the required capital would be maintained. Further, PSOs/PSPs will not act as custodian of consumer’s money or perform any banking function(s). So far SBP has authorized ten PSO/PSPs, out of which three are live. Moreover, 1Link has also been allowed to launch Country first Domestic Payments Scheme “PayPak”.  **Regulations for Technical Implementation of Mobile Banking and Interoperability, 2016**  In order to provide an enabling regulatory framework for the mobile/branchless banking in Pakistan, SBP-PTA joint regulatory committee held several rounds of consultative meetings and drafted regulations for the technical implementation and interoperability of mobile banking, in line with the MoIT&T’s Policy Directive 2008 and SBP’s Branchless banking Regulations issued in 2008. Substantial revisions were made in the draft regulations in order to address concerns of the stakeholders, which include: to bring clarity about the role and scope of TPSPs; restrict TPSPs to be only technical service providers to cellular operators and Financial Institutions (FIs); safe-guard existing mobile banking arrangements between cellular operators and FIs; Operators will be encouraged (not obligatory) for interconnection with TPSPs and FIs; impose no separate license requirements for one-to-one arrangements of mobile banking services for the existing operators.  PTA and SBP jointly issued “Regulations for Technical Implementation of Mobile Banking, 2016” and “Regulations for Mobile Banking Interoperability, 2016” on 16th May 2016 available at <https://www.pta.gov.pk/assets/media/mbanking1652016-3.pdf> and  <https://www.sbp.org.pk/bprd/2016/C3-Annx-A.pdf> respectively.  These regulations are applicable on mobile operators, Third Party Service Providers (TPSPs) and financial institutions that offer m-banking services. The regulations provide detailed mechanism for technical implementation of [one-to-one](file:///D:\Documents\Mobile%20Banking\One-to-one%20Model.pptx) and [any-to-any model](file:///D:\Documents\Mobile%20Banking\Any-To-Any%20Model.pptx) of m-banking. All TPSPs are required to get a license from PTA and authorization by SBP to provide interoperable mobile banking services. All TPSPs and operators are required to enter into Service Level Agreements (SLAs) with SBP authorized Financial Intuitions (AFIs). A joint PTA and SBP committee resolve the disputes between the parties and protect consumers’ interest. |
| **Sri Lanka** | Payment and Settlement Systems Act No. 28 of 2005 – license to operate a mobile payment system  <https://www.cbsl.gov.lk/en/financial-system/financial-infrastructure/payments-and-settlements-systems>  <https://www.cbsl.gov.lk/sites/default/files/cbslweb_documents/laws/acts/en/Payment_setttlement_sys_act.pdf>  Mobile Payments Guidelines No. 1 of 2011for the Bank-led Mobile Payment Services  <https://www.cbsl.gov.lk/sites/default/files/cbslweb_documents/laws/cdg/Mobile_Payments_Guideline_No_1_of_2011_e.pdf>  Mobile Payments Guidelines No. 2 of 2011 for Custodian Account Based Mobile Payment Services  <https://www.cbsl.gov.lk/sites/default/files/cbslweb_documents/laws/cdg/Mobile_Payments_Guideline_No_2_of_2011_e.pdf>  Financial Transaction Reporting Act – prevention of money laundering and anti-terrorist financing reporting  <http://fiusrilanka.gov.lk/>  <http://fiusrilanka.gov.lk/docs/ACTs/FTRA/Financial_Transactions_Reporting_Act_2006-6_(English).pdf> |

**Q9. Under which legal instrument(s) (e.g., license condition, rules, act, etc.) the MNOs are offering DFS in your country?**

|  |  |
| --- | --- |
| **Member Countries** | **Responses** |
| **Afghanistan** | The Central Bank has issued Electronic Money Institute (EMI) licenses to those MNOs who offer mobile money services. |
| **Bangladesh** | Bangladesh follows Bank-led models for MFS services where MNOs are restricted to take part.  By regulation, MNOs in Bangladesh are mostly only permitted to act as bearers - usually via USSD - for banks and other DFS SPs upon permission from BTRC.  However, some of the MNOs are providing some DFS services upon special approval from Bangladesh Bank. |
| **Bhutan** | e-Money Issuer Rules and Regulations 2017 issued by the Central Bank of Bhutan |
| **India** | As stated above, the MNOs are required to obtain PPI license or a Payments Bank license from Reserve Bank of India to offer DFS. |
| **Iran** | The MNOs are advertising DFS conditions in their website. |
| **Maldives** | Mobile license conditions do not prohibit provision of other services and DFS is offered under permit from the financial regulator Maldives Monetary Authority. |
| **Nepal** | As per the provision of Licensing Policy for Institution/Mechanism Operating Payment Related Activities – 2016, if telecommunication service operator wants to operate the business as payment service provider by using own telecommunication network, it can do transaction through establishing a subsidiary company after obtaining the approval of their regulator. Such subsidiary company should also necessarily obtain license from Nepal Rastra Bank. While submitting application by subsidiary company of telecommunication service operator for license to operate as a payment service provider they are required to submit a commitment letter that the telecommunication service operator will provide non-discriminatory access to other institutions/mechanisms operating payment related activities to its own network. If the telecommunication service operator fails to provide non-discriminatory access in its network after providing letter of commitment, the license provided to the subsidiary company of the telecommunication service operator company can be terminated. |
| **Pakistan** | Under their license (provision of value-added service) and PTA’s Regulations for “Technical Implementation of Mobile Banking, 2016”, and as super-agent services under SBP’s Branchless Banking Regulations, 2008 (updated in 2011 and 2016) |
| **Sri Lanka** | Payment and Settlement Systems Act No. 28 of 2005 – License to operate a mobile payment system. |

**Q10. Do you have specific Telecom license(s) / License conditions / Authorizations for the provision of interoperability for Digital Financial Services? If so, is interoperability provided by a single entity or multiple licensees are allowed?**

|  |  |
| --- | --- |
| **Member Countries** | **Responses** |
| **Afghanistan** | There is no specific license for the DFS, and Telecom operators can provide DFS by one of license condition, which is called VAS. |
| **Bangladesh** | MNOs are not allowed to provide DFS/MFS is Bangladesh as per the current regulation. |
| **Bhutan** | No |
| **India** | NIL |
| **Iran** | No. |
| **Maldives** | Interoperability is catered for by multiple licenses – existing banking licences and telecom licenses. |
| **Nepal** | There is no specific Telecom license(s) for DFS. Under the terms and conditions of Telecom License, MNOs are providing services for Digital Financial Services. NTA has issued no objection letter to 2 Telecom Operators to establish subsidiary company to operate DFS as per regulation of NRB. |
| **Pakistan** | A TPSP license as discussed above.  Multiple licenses are allowed for providing interoperability. |
| **Sri Lanka** | No. License to offer DFS is governed by the Central Bank of Sri Lanka. |

**Q11. What are the challenges being currently faced in the provision of DFS?**

|  |  |
| --- | --- |
| **Member Countries** | **Responses** |
| **Afghanistan** | As in all other LDCs and developing countries, the financial inclusion along with digital divide are the common challenges that we also face in our country. Nationalizing the SDGs, our government strategy for a digital economy set multidimensional approaches for achieving relevant targets including reduction of digital gap and the financial inclusion in both urban and rural Afghanistan. |
| **Bangladesh** | Inadequate technological expertise  Cash management hassle by the agents |
| **Bhutan** | Currently, there is weak collaboration among financial institutions, MNOs, central bank and telecom regulator |
| **India** | * As stated above, the Indian DFS sector is led by banks. Thus, the primary challenge in provision of DFS by MNOs is a competitive banking system. * The introduction of United Payments Interface (UPI) which is a system that powers multiple bank accounts into a single mobile application (of any participating bank), merging several banking features, seamless fund routing & merchant payments into one hood. * Limited range of DFS allowed to be offered by the non-banking companies (including MNOs) and even Payment Banks imply the inability to cater to all the banking needs of a customer restricting the attractiveness of opening an account with MNOs. |
| **Iran** | There should be close relationship between Telecom regulator and central bank regulator. |
| **Maldives** | 1. Unable to link to a bank account.  2. Still very novice service, little take up.  3. Services provided by bank is mostly sufficient. (For most people to do their online transactions and banking needs).  4. With nationwide mobile broadband and main traditional banks providing comprehensive online banking service, need is not really seen. |
| **Nepal** | There is no specific/ special regulation from the Telecommunications Regulator (NTA) for Digital Financial Services in Nepal. There is digital divide between rural and urban areas of the country. There is lack of knowledge and trust of DFS for citizen. |
| **Pakistan** | Implementation of interoperable Asaan Mobile Account (AMA) scheme using various platforms e.g., USSD; on-boarding of all the branchless banks and large-scale adoption of digital financial services. Currently, AMA project is under pilot phase.  Average deposit in mobile banking accounts is low i.e., approx Rs. 500. Mobile banking accounts are mostly used for transactions / payments  In Pakistan, there are 47 million mobile banking accounts, out of which, only 19.8 million are active. There is need of more value-added services to offer on these accounts to increase the share of active accounts. |
| **Sri Lanka** | Lack of awareness of  digital services and low levels of financial literacy of the customer as well as difficulty in converting cash-led society to digital-led society due to resistance to change |

1. *https://rbidocs.rbi.org.in/rdocs/PublicationReport/* [↑](#footnote-ref-1)
2. *ITU-T Focus Group on Digital Financial Services* [↑](#footnote-ref-2)
3. ITU-T Focus Group Digital Financial Services: *Identity and Authentication* [↑](#footnote-ref-3)
4. ITU-T Focus Group Digital Financial Services: *Identity and Authentication* [↑](#footnote-ref-4)
5. ITU-T Focus Group Digital Financial Services: *Cooperation frameworks between Authorities, Users and Providers for the development of the National Payments System*  [↑](#footnote-ref-5)