Requirements for a Pro-Poor Mobile Wallet

The Bill & Melinda Gates Foundation

December 10, 2014

Last Modified: June 14, 2016

BILL & MELINDA
GATES *foundation*

Table of Contents

Contents

Suggested citation: Bill & Melinda Gates Foundation. *Requirements for a Pro-Poor Mobile Wallet*. Seattle: Bill & Melinda Gates Foundation; 2014.

1.0 Background

The Bill & Melinda Gates Foundation, through its Financial Services for the Poor (FSP) program, seeks to increase poor people's access to appropriate financial services and tools, accelerating the rate at which they move out of poverty and improving their ability to then hold onto those gains once achieved.

The FSP program believes that impact will occur at three levels:[1]

- Level 1: reducing the resources (in both time and money) that poor people must expend to finance their current activities
- Level 2: increasing poor people's capacity to manage economic shocks and capture income-generating opportunities
- Level 3: generating economy-wide efficiencies by digitally connecting large numbers of poor people to their peers, financial service providers, government services, and other counterparties.

To achieve these impacts, the FSP team created multiple initiatives. One key initiative, the *Level One Project*, seeks to play a catalytic role in expanding access to financial services by enhancing the reach of digital payment services in poor and rural areas and expanding the range of financial services that poor people can access over these platforms.

Rapid advances in digital payment systems, combined with exponential growth in mobile phone penetration in developing countries, enables that FSP program strategic initiative, accelerating the replacement of cash with digital liquidity, including receiving and sending payments electronically.

With the intent of expanding the discussion, the foundation's *Level One Project Guide: Designing a New System for Financial Inclusion* describes a specific reference model for a country-level digital payment system leveraging mobile phone infrastructure. *The Level One Project Guide* outlines how FSP's digital payments system model is designed to meet the needs of the people with very low income, and how that system responds to specific user requirements.

The Gates Foundation also worked with partners to build out a demonstration prototype, providing a working payments switch and emulating core mobile wallet functions through a USSD interface and a smartphone application.

This document extends the prior work of the Gates Foundation, incorporating work from industry groups and other stakeholders to further define a mobile wallet solution that would help drive widespread adoption of digital payments as an alternative to cash in developing countries.

[1] *Financial Services for the Poor Strategy Overview*, 2012, Bill & Melinda Gates Foundation.

2.0 Overview

This document provides the business requirements for the mobile wallet and supporting Digital Financial Services Provider (DFSP) components of the pro-poor mobile payments ecosystem reference model advocated by the Gates Foundation in The Level One Project Guide.

The document identifies the specific capabilities of a mobile wallet intended to meet the core needs of very poor people, enabling them to make or receive payments and access funds through a mobile device (typically a basic mobile phone).

The document includes the needs of both the payer and payee (i.e., consumer and merchant), but is constrained to basic functionality and does not include significant details on the cash management, clearing, or settlement processes that support the payment use cases. Specifically, the document focuses on a specific implementation model that allows users to pay for goods and services, regardless of the recipient type (e.g., person, business, utility, school, government) using a remote payment model that is independent of the payment recipient's systems and infrastructure.

Advanced features requiring a smart mobile device are included for the agent/merchant mobile wallet, as those users benefit significantly from the additional capabilities, and are much more likely to have an advanced mobile device in the target markets.

Value-added services that are prevalent in developed countries (e.g., credit card use, coupons, loyalty programs) are not included, to focus on the primary needs of those with very low incomes.

2.1 HOW TO USE THIS DOCUMENT

This document describes one approach. The requirements herein are not intended to describe the unique scenarios that may be posed in any *specific* environment, but rather to describe an initial target list of expected capabilities that should be included in a delivered solution designed to meet the needs of those with very low incomes. As a starting point, the document could be customized by the user to meet their specific needs. When deciding on what to include, exclude or alter, the user should determine the intended benefit and how environmental factors might require modification to achieve those benefits.

Note: The requirements enumerated in this document follow the wording guidelines defined in the IEEE-SA Standards Board Operations Manual, paragraph 6.4.7. More detail can be found in the "Document Style" section (6.3).

2.1.1 Benefits

Multiple ecosystem stakeholders might use this document with the following benefits:

- **Software Providers**: Provides a jumpstart to development efforts by providing an articulated, core target system for delivery. A majority of user needs have already been discovered and documented, allowing software teams to start prototyping and quickly providing solutions to the marketplace. Development organizations might also incorporate some of these requirements to improve their existing systems.
- **Financial Institutions and Digital Financial Services Providers**: For organizations considering building or buying digital payment capabilities, the document provides a starting set of requirements that can be expanded, or that can be used as a the basis for a request for information (RFI), request for proposal (RFP) and scorecard for evaluating vendors.
- **Financial Regulators and Policy Makers**: This document lays out a clear set of capabilities for the routing and switch components for a pro-poor digital payment infrastructure. Regulators and policy makers interested in expanding financial inclusion to improve the lives of poor people can use these requirements to jumpstart

discussions with government agencies, mobile network operators, financial institutions, advocacy groups and other interested parties.

- **Central Banks**: This document can be the basis for strategic planning and execution of financial solutions for poor people, while stimulating the adoption of efficient and low-cost digital payment solutions.

2.1.2 Potential Modification Drivers

The "right" approach will vary in any particular county's environment, with the ultimate requirements impacted by:

- **Monetary Policy**. Ability to clear and settle funds within the target timeframes for high-volume, low-value payments. May consider how the solution impacts digital payments ubiquity, and subsequently overall price stability and money supply within the economy at a macro level.
- **Regulatory Direction**. Digital money transfers may be regulated under banking rules, a separate digital specific set of rules, or something in between; or, regulation may be silent. In any case, the specific regulation for the target environment may entail adjustments to the system requirements.
- **Business Climate**. Each market is unique, with one or more service providers vying for share of customers. Depending upon the level of cooperation among providers, systems may already operate in *open* or *closed loops*.
- **Cultural Considerations**. In each environment, cultural norms, such as end-user perceptions of and trust in the solution, may impact system requirements. For instance, gender relations in traditionally patriarchal cultures may complicate access to mobile money by women.
- **Infrastructure Capability**. Technical skill sets, connectivity speeds, etc., will play a part in tuning requirements to the target market. For example, power grid reliability may impact service availability and drive additional non-functional resiliency requirements.
- **Product Compatibility**. If organizations have significant investments in legacy systems, simply starting over may not be feasible. Some capabilities may be incompatible without significant rework.

2.2 SCOPE

The scope of the document is bounded by the capabilities specifically defined as in scope, and anything not specifically listed **should** be assumed out of scope.

2.2.1 In-Scope Work

The intent is to fully describe the core mobile wallet capabilities envisioned in *The Level One Project Guide* and further extended by the demonstration prototype system,[2] and that would enable the users to securely and reliably send and receive electronic payments with appropriate participants in the mobile money ecosystem, constrained within national boundaries.

The document includes supporting non-functional requirements, such as performance, availability, confidentiality, security, and usability characteristics necessary for the mobile wallet to meet the demands of its intended user profiles or roles (e.g., consumer, agent, merchant).

The following use cases will be supported by part of the mobile wallet as described in the DFS reference model and expressed in the prototype:

Item	In-Scope Items	Detail
1	Install and set up mobile wallet	User registers and self-activates a mobile wallet
2	Put cash in	Transfer value to mobile wallet by depositing cash at agent
3	Get cash out	Transfer value from mobile wallet to receive cash at agent
4	Make peer-to-peer payment	Send money to another consumer wallet or bank account
5	Purchase goods or services from a merchant using stored value funds	Utilize the mobile wallet stored value account as a payment source to purchase goods or services
6	Purchase goods or services from a merchant using a voucher	Utilize a voucher as a payment source for an authorized purchase

[2] https://prototype.open-dfs.org/index2.html

7	Connect mobile wallet to bank account	Register one or more formal bank account(s) with the mobile wallet to enable funds transfer with financial institution
8	Review pending transactions	List in process activities requiring action by the user to complete the specific business processes
9	Pay bill	Consumer uses mobile wallet to transfer value to biller, satisfying demand for a presented bill
10	Get mini-statement	Display balance and recent transaction
11	Manage account	Update information related to the consumer mobile wallet account
12	Sell goods as merchant	Extensions specific to the merchant
13	Get cash in as agent	Extensions specific to the agent
14	Perform biometric registration	Agent extensions for biometric authentication and authorization
15	Sell using biometrics	Merchant extensions for biometric authentication and authorization

2.2.1.1 Mobile Wallets for Humanitarian Response

Mobile money and mobile wallets have drawn interest and consideration as a delivery mechanism for cash based transfer programs in humanitarian response situations (e.g. earthquake, flood, refugee crisis). However, this context presents unique challenges to mobile wallet systems. Identity verification, new account registration, and the need for rapid deployment are only a few of several challenges that systems may face.

This document identifies the functional and non-functional requirements of a mobile wallet that are more important or relevant in humanitarian response situations to meet the needs of very poor people and the humanitarian response agencies that are deploying cash based transfer programs. These requirements are denoted below with an emergency sign (✚) and have an additional rationale ("Humanitarian Response Rationale") explaining the context for this requirement and why it is more important or relevant.

2.2.2 Out-of-Scope Work

This document is not meant to be an exhaustive description of mobile wallet capabilities and opportunities, but rather a review of the core capabilities needed to serve poor people in developing countries. Focus is on the needs of the wallet holder.

The following items are out of scope and will not be included:

- Legal, regulatory, or stakeholder governance of the system's capabilities
- Functions of the Interoperability Service for Transfers (IST)
- Functions of merchant management
- Functions of mobile money operator agent management
- Capabilities provided entirely within the systems of the mobile network operator (MNO), bank, NGO, government, or other participating entities
- Deployment, distribution or installation of the mobile wallet or supporting infrastructure.
- Communications channels and enabling technology
- Contactless payment transactions
- Extended wallet features (e.g., couponing, loyalty programs)
- Administrative functions for employees of DFSPs, including role-based security, separation of duties, etc.

2.3 METHODOLOGY

This requirements document was developed though analysis of prior works, including: previous Gates Foundation strategy documents, *The Level One Project Guide*, industry research and articles, and the pro-poor demonstration prototype.[3]

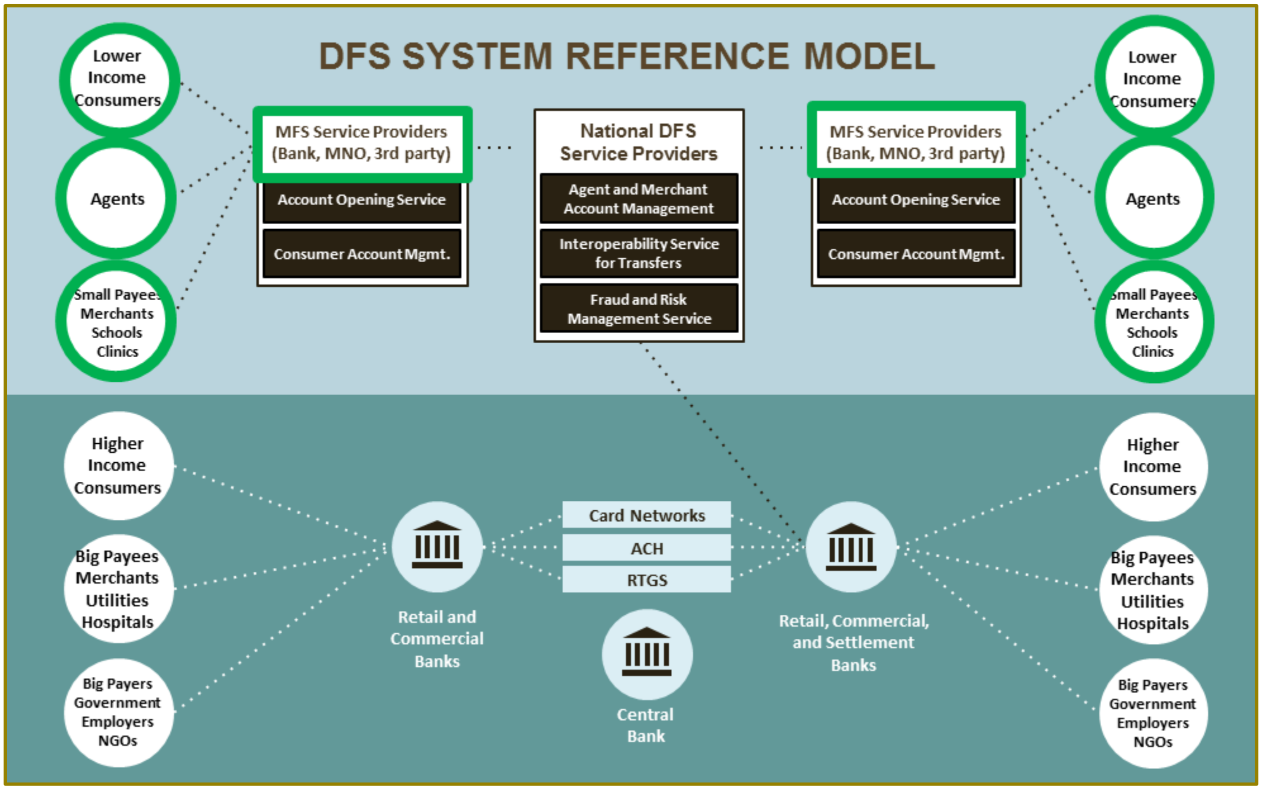
[3] https://prototype.open-dfs.org/index2.html

3.0 DFS System Reference Model

The Gates Foundation has developed a Digital Financial Services (DFS) System reference model for a country-level payment system designed to address the needs of poor people. A physical technical model is specified, along with the system governance necessary to manage such a system, and describes the government and industry support measures required for success. The reference model is only one part of an overall effort by the Gates Foundation to bring financial services to those with very low incomes, and thereby improve their lives. Its purpose is to illustrate what a system designed to meet the needs of ultra-poor users might look like, to outline how it responds to specific user requirements, and to support a robust interactive dialogue among those interested in increasing financial inclusion for poor people.

The reference model can be thought of as an ideal in-country system, designed to meet the needs of all users (consumers and businesses, governments, and other entities with whom they interact) throughout the country. Actual implementations will vary from country to country, but elements of the reference model are apt to be appropriate to every country. In some areas a more regional approach to mobile money payment systems may be appropriate, and some elements of the reference model could be implemented on a regional basis. While no single currently deployed national or payments system incorporates all elements of the reference model, each has been implemented somewhere.

This document specifically focuses on the mobile wallet and supporting DFS System components (highlighted in green in the diagram below):


DFS SYSTEM REFERENCE MODEL
Lower Income Consumers
Agents
Small Payees Merchants Schools Clinics
MFS Service Providers (Bank, MNO, 3rd party)
Account Opening Service
Consumer Account Mgmt.
National DFS Service Providers
Agent and Merchant Account Management
Interoperability Service for Transfers
Fraud and Risk Management Service
MFS Service Providers (Bank, MNO, 3rd party)
Account Opening Service
Consumer Account Mgmt.
Lower Income Consumers
Agents
Small Payees Merchants Schools Clinics
Higher Income Consumers
Big Payees Merchants Utilities Hospitals
Big Payers Government Employers NGOs
Retail and Commercial Banks
Card Networks
ACH
RTGS
Central Bank
Retail, Commercial, and Settlement Banks
Higher Income Consumers
Big Payees Merchants Utilities Hospitals
Big Payers Government Employers NGOs

3.1 ACTORS IN THE REFERENCE MODEL

The following table provides a brief description of the actors that interact with the mobile wallet.

Actor Name	Description

Actor Name	**Description**
Digital Financial Services Provider (DFSP)	An organization providing digital money services to end consumers. This might be a mobile network operator, bank, etc.
Bank	A formally chartered financial institution regulated by a governmental authority
Consumer Account Management System	A service for managing the lifecycle of *consumer* digital money user accounts. This service would typically reside with the Digital Money Service Provider.
Agent Account Management System	A service for managing the lifecycle of *agent* type digital money user accounts. This service would typically reside with the Digital Money Service Provider.
Merchant Account Management System	A service for managing the lifecycle of merchant type mobile money user accounts. This service would typically reside with the Mobile Money Service Provider.
Interoperability Service for Transfers (IST)	A core financial payments switch that securely, reliably and efficiently passes messages from one participant to another.
Fraud and Risk Management Service (FRMS)	A service that analyses participant and transaction records to provide a risk score that can be examined to determine if mitigation action needs to be taken.
Government benefit payer	A governmental organization that provides financial support to large numbers of end consumers
NGO benefit payer	A non-governmental organization (NGO) that provides financial support to large numbers of end consumers
Mobile Network Operator (MNO)	Wireless telecommunications infrastructure provider, providing mobile phone service to end users
Consumer	A person who purchases goods and services in the marketplace.
Agent	A person acting to represent the DFSP, providing physical business services to the consumer (e.g., converting between cash and mobile money).

3.2 HIGH-LEVEL PAYMENT INTERACTIONS

The following matrix shows how the various actors within the payments ecosystem would interact, identifying the specific payment types that might occur. This document is primarily concerned with payments involving the end consumer (highlighted in green)

		Payee		
		Government /NGO	Business	Person
Payer	Government /NGO	G2G [Transfers] Budgetary allocations, funding of programs	G2B [Expenditures] Grants, loans, payments for goods and services, tax refunds	G2P [Expenditures] Welfare programs, salaries, pensions, tax refunds
	Business	B2G [Collections] Taxes, fees for licenses and permits, fines	B2B Payments for goods and services in value chains	B2P Salaries and benefits
	Person	P2G [Collections] Taxes, utilities, fines, fees	P2B Purchases	P2P Remittances, gifts, debt payment

Figure: Participant to Payment Type Matrix

4.0 Core Capabilities

As aptly described by mobile industry group Mobey Forum, the term mobile wallet refers to…

"…the functionality on a mobile device that can interact securely with digitized valuables. It includes the ability to use a mobile device to conduct commercial transactions in the physical world. A mobile wallet may reside on a mobile device or on a remote network/secure server. Alongside the ability to undertake payments, the Mobile Wallet may contain other content, such as identity, commerce and banking services, transport and other tickets, retail vouchers and loyalty programs."4

For the purposes of this document, the **mobile wallet is the application** (whether installed on the phone or hosted by the DFSP); **it provides the secure user access to one or more accounts** (e.g., DFSP) through which electronic value (e.g., float in a stored value account at the DFSP) can be exchanged via a payment process as a stand-in for cash. The application provides for authorization and initiation of payment between the authenticated wallet holder and another party. The actual transfer of value between participants is handled by other components of the mobile payments ecosystem, acting to fulfill the payment instructions initiated from the mobile wallet.

4.1 TOP-LEVEL USER NEEDS

The following key attributes are expected in a successful mobile payments solution:

- **Secure.** People need to trust that the money held in a digital account is secure, and not subject to theft or unauthorized withdrawals. They need assurance that money will go only to the designated recipient, with a record of the transaction that the individual can use to prove that payment has been made or received.
- **Affordable.** Cost to use the system must be very low, both from the standpoint of holding money as well as transacting. To actually replace the use of cash for daily purchases, the cost to the consumer (as well as to the merchants serving lower income consumers) will need to be close to zero, as that is their perceived cost of using cash.
- **Convenient.** The system needs to be easy to sign up for and use to support low literate consumers. Many poor people do not have the identity documents usually required to create financial accounts. This system needs to make some provision to enable these individuals to participate, while managing the related risks. The system has to be understood by prospective users with limited or no mediation. A very important aspect of this is the clarity and transparency of the system's conditions of use, including pricing and service rules.
- **Open.** The system needs to be able to reach many (ideally all) counter parties for both making and receiving payments. It should not require special, costly, or time-delayed accommodations for a counter party using a different service provider. And it should make it easy for an individual to integrate into multiple financial systems of the country—people should not be excluded from the greater economy as a whole, or relegated to a financial system unconnected to that of higher-income earners.
- **Robust.** A digital payment system needs to be available for use as needed, like cash. Users should not have to be concerned about the system being down on payday, for example. As the number of participants (and their usage volume) grows, availability should remain high and be able to handle peak volumes without an interruption in service.

[4] Mobey Forum. *Mobile Financial Terms Explained.* n.d. http://www.mobeyforum.org/whitepaper/mobile-financial-terms-explained-2/ (accessed November 3, 2014).

4.2 DESIGN PRINCIPLES

Based on the core set of user needs, and leveraging lessons learned from both legacy and modern payments systems, the Gates Foundation developed a set of design principles for a pro-poor digital payment system. These principles were used to develop the reference model that meets the needs of the poor:

- **Open loop:** The system should be an open loop, with the objective of encouraging all qualified participants to join. Open-loop systems avoid duplication of efforts by individual participants, which keeps costs down and optimizes services delivered to end users. Ultimately, an open-loop system achieves interoperability through the direct participation of all providers.
- **Immediate funds transfer:** The system should make funds available to the payee in near-real time, providing immediate notification of payment from the payer to the payee. This feature is both demonstrably possible (as many countries have implemented this in various payment systems) and logically necessary to replace cash, which is another form of immediate payment.
- **Push payments:** The system should effect *push* rather than *pull* payments. Push payments, such as an Automated Clearing House (ACH)-type employer direct payroll deposit, work when the payer instructs their account holder to move money to the payee's account holder. This contrasts with pull payments, used in card and direct debit systems, which work when the payee's bank requests money ("pulls") money from the payer's account holder. Existing push payments systems have demonstrated lower fraud rates and lower system costs than pull systems. Note that a push system can incorporate a request message from the payee (for example, a message from a merchant requesting payment), but the transaction doesn't happen until the payer instructs the provider to send the funds.
- **Same-day settlement:** The system should settle funds among participants at least once a day, to ensure the system and its participants have as close to zero exposure from a failing participant as is possible. This controls liquidity risk, and therefore reduces costs. Note that the timing of end-party settlement (when the accounts of the paying party and the receiving party are actually debited and credited) does not have to match the inter-provider settlement timing. This means, for example, that a transaction can be instantaneous between the two users, but their participant institutions are settling with each other later that day.
- **Open, international standards:** The system should adhere to internationally accepted payments standards (such as ISO 20022) rather than implementing system-specific, proprietary standards. This allows for easier and more cost-effective handling of transactions, such as remittances, across different systems.

  Methods of accessing components of the system by participants or other parties should also be enabled through open application program interfaces (APIs). This enables innovation among direct and indirect participants; for example, providers and vendors can more easily embed payment capability in their sector-specific services.
- **Irrevocability:** The system should not specially manage transaction reversal by the originating party nor specify situations in which the liability for a transaction is passed from one participant to another. This eliminates the complexity and services infrastructure required by the system to reverse transactions, thereby eliminating significant system cost. Note that this is only at the system level—direct or indirect participants could still offer value-added services that allow for reversals or other credits. Additionally, this does not mean that there should be no consumer protections: for example, the consumer should be able to make an inquiry into the status of a transaction, or lodge a complaint with their provider about an unauthorized transaction.
- **Shared fraud service:** The system should address how participants may contribute transaction data (either on fraudulent or on all transactions) to a commonly owned fraud management service. Managing some of this functionality at the hub or network level, rather than at individual participant level, is likely to reduce costs of the overall service and improve fraud detection capabilities.
- **Tiered KYC:** The system should enable tiered "know your customer" (KYC) that allows for participation by end users in correlation to level of use. For example, people lacking documentation may open basic accounts, and the risk related to these accounts may be managed by imposing strict maximum account balance and transfer limits. This will help drive volume through participation by the poor, while maintaining proper levels of fraud control.

4.3 ESTABLISH IDENTITY

4.3.1 Description

In operating a risk-managed payment ecosystem, it is necessary to establish the identities of people and organizations. This can be a challenge for those without formal identity documents from an authoritative trusted party. This inability to establish identity can be a primary barrier to financial inclusion.[5]

Globally, varying methods have been used to establish identity in a range of assurance. It is important to note that being able to identify a unique individual in a population does not inherently reduce risk. The identity must be linked to behavior, to establish a risk profile.

Examples of identity assurance include:

- Biometric registration[6]
- National government ID (online verified)
- National government ID (presented and conforming to standard)
- Regional government ID
- Local authority
- Private entity such as an MNO
- Self-representation of identity
- NGO/UN issued program ID

From a technology perspective, it is possible to uniquely identify every individual and provide them with a single, unique electronic identity. Countrywide implementation of such an identification system, however, is quite challenging in practice, and requires a significant resource commitment.

Nigeria[7] and India[8] have initiated nationwide systems to assign biometric-based countrywide unique identifiers. The implementations have met with varying levels of success, and challenges exist with utilizing the available identity for online verification of the presenting user. Regardless of the real-world implementation challenges, a nationwide biometric verification identity verification service, in concept, provides substantial opportunity for financial inclusion.

If a government or trusted private entity has completed KYC activities, then regulations and technology should permit the mobile wallet to access those systems in establishing an individual’s identity.

[5] CIO NOTE: The National Institute of Standards and Technology (NIST) published an “Electronic Authentication Guideline,” providing guidance on mapping the consequence of authentication error to defined technical requirements for assuring identity. The document provides detailed criteria for assurance classification.

[6] Various bodies have identified standards for providing biometric-based identity assurance services.

- ANSI INCITS 442-2010, Biometric Identity Assurance Services (BIAS)
- http://docs.oasis-open.org/bias/soap-profile/v1.0/errata01/os/biasprofile-v1.0-errata01-os-complete.html Biometric Identity Assurance Services (BIAS) SOAP Profile Version 1.0
- http://www.nist.gov/itl/iad/ig/bws.cfm NIST Biometric Web Services, using OASIS standard.
- (under development as of 11/2014) ISO/IEC DIS 30108-1.2 Information technology -- Biometric Identity Assurance Services -- Part 1: BIAS services, http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=53228

[7] www.nimc.gov.ng, National Identity Management Commission [NIMC]. Established by the NIMC Act No. 23 of 2007, the NIMC has the mandate to establish, own, operate, maintain and manage the National Identity Database in Nigeria, register persons covered by the Act, assign a Unique National Identification Number (NIN) and issue General Multi-Purpose Cards (GMPC) to those registered individuals, and to harmonize and integrate existing identification databases in Nigeria. In a few words, our mandate is to provide an assured identity system in Nigeria through the concept of enrol once and be identified for life.

[8] www.uidai.gov.in, Aadhaar is a 12-digit individual identification number issued by the Unique Identification Authority of India on behalf of the Government of India. http://spie.org/x108321.xml The solution for reliable identification of the entire population is to acquire biometric data (iris patterns, see Figure 1, and fingerprints) of every person, stored centrally, linked to a unique 12-digit ‘Aadhaar’ number issued to them that they use to assert their identity in seeking any Government service or benefit. The Aadhaar number ‘travels with the person’ so it can be invoked anywhere, by biometric authentication against the central database. The Aadhaar (meaning ‘platform’ in many of India's 22 languages) is a pointer to many services. For example, it can be used to create a bank account for a person without one.

When a high level of identity assurance cannot be achieved, the permitted activities should be constrained to minimize the impact if an identity is compromised and misused.

4.3.2 Rationale

Understanding that such identity initiatives are underway in developing countries, it is incumbent on emerging payment systems to support such national identification schemes, while supporting inclusion where identity may not be well established.

4.3.3 Requirements

1. The system **shall** uniquely identify individuals at the national or regional (e.g. Southern African Development Community) level if possible, and **always** to the broadest scope supported in the payments ecosystem. For example:

- Global (ICCID, GUID)[9]
- National (e.g., Aadhaar, NIN/NIMC)
- System-wide (e.g., MSIN, Banker's Identification Number)
- Market region (e.g., TMSI)
- Application (e.g., primary key in person object table)

Rationale: It is assumed that the broader the scope of the identification scheme, the easier it will be to perform needed regulatory compliance, reporting, reconciliation, fraud, and other tasks that uniquely identify an individual participant or account owner.

Note: The examples above are not recommendations or even potential solutions, but simply examples or indicators at the described level. For example, while an ICCID is globally unique, it is not useful in this context, as a consumer may not have a SIM.

2. The system **should** utilize national identity scheme services, when available, to establish the identity of an individual.

Rationale: Creating an alternative identification scheme when a unified national scheme already exists would increase the overall cost and add complexity, reducing the durability of the system.

Humanitarian Response Rationale: Importing user registrations from pre-existing lists and identity services may enable rapid deployment and reduce the amount effort of identity verification.✚

4.4 SELF-ISSUE A MOBILE WALLET

4.4.1 Description

In developing countries, banking regulators must balance the needs of Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT) controls with the reality that individuals may lack formal identification documentation. Historically, the process of account opening could be very slow and required significant effort on the applicant's part to provide the required proof of identity.

Mexican regulators recognized that simplifying the account opening process was critical to enabling financial inclusion and pioneered a new approach: tying KYC to the capabilities and limits of the account. This solution permits both anonymous and identified account holders. For example, in the Electronic Interbank Payment System (*Sistema de Pagos Electrónicos Interbancarios*, or SPEI) operated by *Banco de México*, a Level 1 or the lowest level of account with an anonymous owner can have a maximum value of US$280 and be accessed by a mobile phone, but requires no ID and no face-to-face process to open.[10]

In line with that approach, the mobile wallet we propose allows a mobile phone user to self-issue a mobile wallet and primary account, with tiers of limits and capabilities tied to the ability to uniquely identify the account opener. In order to provide the broadest level of access, anonymous registration is supported for a basic account, tying the

[9] http://en.wikipedia.org/wiki/Globally_unique_identifier

[10] Marulanda, Beatriz. *Mexico's engagement with the standard setting bodies and the implications for financial inclusion.* Alliance for Financial Inclusion, 2011.

identity to a specific phone number or SIM, or to a national identity number—but not necessarily with the benefit of confirming that the account holder is the person legally represented by that specific national ID.

Like the lowest level of accounts in the SPEI system, the basic account in the mobile wallet we propose has reduced limits for maximum account value, maximum aggregate transaction value in a given timeframe, etc.

4.4.2 Rationale

Allowing the user to self-issue a mobile wallet and account reduces the barriers to financial inclusion related to proving identity, while still supporting AML/CFT compliance. Further, credit risk is eliminated, as all accounts must be prefunded, reducing the overall systemic exposure to loss by system participants.

4.4.3 Requirements

4.4.3.1 Tiered KYC Limits

1. The system **shall** constrain the activities and properties of any mobile wallet account based on the level of customer risk and in compliance with applicable regulation and law (e.g., KYC, fraud, AML/CFT, tiered account limits).

Rationale: To be durable in the marketplace, the mobile wallet must follow approved risk management controls and guidelines of regulators. Tiered accounts, for example, may have higher limits depending upon how well the account holder can be identified and vetted.

2. The system **shall** provide the ability for a mobile wallet account to be migrated from one KYC tier to another, as warranted by changes in the customer risk profile.

Rationale: It is reasonable to assume that an account holder may start with a basic account, potentially with no documentation, and upon finding value in the mobile wallet, expend the effort to establish their identity, and as a result qualify for a higher account tier.

Humanitarian Response Rationale: A temporary mobile wallet may be deployed (with different KYC requirements and transaction and value limits) during a humanitarian response. There should be a migration path to a standard KYC account once the temporary term of the mobile wallet is complete.✚

3. The system **shall** make the information about the user’s current KYC tier (e.g. transaction and value limits) easily accessible.

Rationale: A user may need to review this information before initiating a transaction.

Humanitarian Response Rationale: KYC levels may temporarily change during a response situation, and users need an easy way to refer to this information.✚

4.4.3.2 Provisioning

1. The system **shall** permit a consumer to register and activate a mobile wallet account, whose capabilities and constraints are in alignment with regulation and law, without secondary approval or manual intervention by a third party.

Rationale: Self-registration/activation reduces barriers to financial inclusion and improves ubiquity of mobile payments capabilities.

2. The system **should** support self-registration via as many channels as supported by the available infrastructure and wallet provider (SMS, USSD, WAP, applet, Internet).

Rationale: More options improve likelihood that the user will complete the sign-up process.

3. The system **should** allow for adjustable and pre-configurable rules for account registration (e.g., custom preset KYC rules).

Rationale: Adjustable registration rules may be needed to accommodate locale specific regulations.

Humanitarian Response Rationale: Speed of response is critical. Designing and pre-configuring emergency rules for account registration (e.g., lowered KYC requirements, delegated account registration process) will enable rapid deployment.✚

4. When the DFSP receives the appropriate self-registration request from a user, the system **shall** respond with the instructions for completing the registration, including any associated fees to complete account registration.

Rationale: The user is unlikely to know the procedure or the syntax of the command depending upon the method of self-registration selected. The response will vary depending upon the implementation. For example, if by USSD, the system would respond with a sample USSD template instruction. The user would then enter the requested information per the template instructions and send it back to the MNO, for routing to the DFSP.

5. The system **shall** enforce minimum data requirements during registration. This should be kept to a minimum. As an example, the minimum required data could be first and last name, date of birth, or national ID/alternate ID.

Rationale: Each operating instance will at some level define the minimum data needed to identify a unique individual within the system. Requiring fewer data elements supports account setup with devices not optimized for text entry, and for users with fewer identity credentials, e.g., address, bank account, driver's license.

Humanitarian Response Rationale: People may have lost identification documents or may have not ever had them. Requiring less information may increase access and enable rapid deployment. Minimal data requirements may also make it easier to register non-resident workers who support response efforts.✚

6. The system **shall** permit a consumer without a phone, SIM, or phone number to self-register and utilize a mobile wallet account from a mobile phone with a registered mobile wallet account.

Rationale: The very poor may not have their own device or SIM.

Humanitarian Response Rationale: Access to mobile phones may decrease from both phone loss/damage and increased financial burden. Supporting workflows for multiple users per phone will increase access.✚

7. The system **should** allow for 3rd party account registration on the consumer's behalf, either via in-person (user is present) or remote (user is not present) methods, with supporting workflows (e.g. remote PIN reset process). See PIN Management.

Rationale: There may be account registration kiosks that help low literacy users.

Humanitarian Response Rationale: 3rd party organizations or entities may use existing identity databases or manually collect identification information in-person (e.g. manual review of identification documents, biometrics) to complete account registration.✚

8. The system **shall** associate a unique account identifier to the submitted user data, ensuring the record can be distinguished from all other mobile wallet accounts in the system.

Rationale: This may be needed to support a mobile wallet for users without a phone number or SIM card.

9. Upon registration completion, the system **shall** associate the phone number (whenever available) to the user data provided.

Rationale: The registration/phone number relationship uniquely maps person to phone for a typical mobile wallet account where the user has their own SIM (which maps to the MSISDN, or phone number).

10. Upon registration completion, the system **shall** send a notification to the account holder providing account details, terms and conditions, including the account ID, transaction limits, and value limits.

Rationale: The user must receive clear indication of the registration success. Further, the user should be made aware of any use limits imposed on the account to improve clarity on how the account may or may not be used.

Humanitarian Response Rationale: This notification may provide an opportunity to provide additional pertinent information (e.g. details of the aid program, timing of the next cash disbursement, where to go for other support).✚

11. The system **shall** log all completed registration activities including the time of registration start, time of registration completion, phone number and the unique account ID.

Rationale: This information may be needed for troubleshooting if there are problems with registration or for general performance management.

12. The system **should** support user groups (e.g. adding, managing, editing), applying properties, and tracking the membership and assign a user to a group at the time of registration.

Rationale: The ability to group and segment users may support reporting and customer service needs.

Humanitarian Response Rationale: Users in a humanitarian response program may need to be treated differently from the rest of the DFSPs users, in terms of user rights or privacy and also reporting.✚

13. At time of registration, the user should be permitted to assign a common-language name, or *alias*, to the newly created account. The alias must be unique (i.e., not reused with another account) in the context of the user's relationship to the DFSP.

Rationale: The solution accommodates multiple accounts, so the user benefits from having an easy-to-remember name assigned to each account they hold.

Humanitarian Response Rationale: Users in a humanitarian response program may opt for using another name due to discrimination or fear of persecution.✚

14. The system **should** enable users to register a SIM/phone pair (i.e., the SIM card's Integrated Circuit Card Identifier (ICCID) and the phone's International Mobile station Equipment Identity (IMEI), in the context of the account. as an authorized transaction device tied to an account holder/PIN.

Rationale: A SIM/phone pairing uniquely identifies both the device and its resident SIM, allowing multiple SIMs to be used on a single authorized device. Also, this ultimately prevents account takeover through the mobile channel. A SIM can easily be cloned and used remotely while the true owner retains access to their SIM. This is made more difficult by tying together the SIM and phone identifiers. Because both SIM and phone would need to be cloned, this likely provides a high enough barrier that the value of the targeted account is not worth the effort.

15. For added account security, the DFSP **may** support registration of one or more pairs of the SIM card's ICCID) and the phone's IMEI in the context of the account.

Rationale: The ICCID is unique to the SIM hardware, while the IMEI is unique to the phone hardware. By registering both pieces, the provider can restrict access to the mobile wallet over the mobile channel to only the authorized IMEI/ICCID pair (or pairs, in the event a customer shares multiple phones/SIMs with others and registers more than one combination).

16. When the user has registered one or more pairs of IMEI/ICCID codes, the system **shall** only permit access to the customer's mobile wallet from the registered device/SIM parings.

Rationale: This ultimately reduces fraud risk, as both SIM and phone would need to be cloned to take over the account via the mobile device channel.

17. The system **should** provide the ability to transition a normal user to an agent user, and also be able to transition a large group of users at once.

Rationale: Streamlining agent registration process will encourage enrollment.

Humanitarian Response Rationale: Existing agents may have been displaced in a crisis (e.g. refugee or IDP situation), and new or existing normal users may be a great source of new agents. Easily and rapidly enabling a normal wallet user to become an agent user may encourage more agent enrollment.✚

4.4.3.3 PIN Management

1. Upon verification of the submitted registration data, the system **shall** require the user to create a PIN (i.e., enter and confirm PIN) to complete registration.

Rationale: The PIN is required for security (i.e., access control and activity authorization) of mobile wallet functions. In conjunction with the legal agreements with the DFSP, the PIN also enables non-repudiation by validating that the wallet holder is authorized to perform subsequent actions.

2. The system **shall** encrypt the PIN during transmission and when stored.

Rationale: The user provides their PIN to authorize controlled activities, thus it must be protected against disclosure to unauthorized parties.

3. The user PIN **shall** never be captured in system logs or displayed on any system user interface in clear text or unencrypted form.

Rationale: To ensure non-repudiation, the PIN should never be visible to anyone after assignment.

4. The system **must** provide a mechanism for the user to reset the PIN without knowledge of the original PIN. Note: This would generally require other user secrets, in-person verification of identity by an authorized representative, or biometric confirmation.

Rationale: People forget or lose PIN numbers, so the system must provide a PIN reset that relies on other information that is available to the legitimate account holder.

Humanitarian Response Rationale: A remote PIN reset workflow is important to support 3rd party account registration process.✚

4.4.3.4 Deprovisioning

1. The system **shall** permit a consumer to unregister and deactivate (close) a zero-balance mobile wallet account without secondary approval or third-party assistance.

Rationale: There should be no barriers to an individual's discontinuing use of the system.

2. When an account is closed, the DFSP **should** retain all records of the account in accordance with law and regulation.

Rationale: Historical records will be required for analysis and reporting even after the account is closed.

3. When an account is closed, the consumer account holder **shall** be prevented from making further changes to the account, or performing any financial transactions. It **may** be desirable to allow users to view the closed account in read-only mode.

Rationale: Closed accounts are historical, and thus the original account holder should be prohibited from further use of the account.

4. The system **should** allow a user to request closure of an account with a positive balance, thus suspending service, but require a zero-balance state before closing the account.

Rationale: Disables use of the account and freezes the value, providing time to move the balance.

5. The system **shall** permit an authorized party to lock an account, prohibiting access by the account holder and suspending all financial transaction capability.

Rationale: There will be situations (e.g., fraud investigations) where the account value must be prevented from movement, or where the user should not be permitted access.

6. The system **shall** prohibit mobile financial transactions to or from the account when the account is suspended, except by an authorized party to transfer out residual value and enable closure.

Rationale: Provides ability to limit use of account except to meet the conditions for closure.

7. The system shall allow a user to reinstate or unlock a suspended or locked account. This process should involve ID verification by the account-holding organization. This same process would be involved for the user to cash out or transfer the funds to another account.

Rationale: At some point in time, the account holder will require access to their funds through the existing account.

4.5 ACCOUNT MANAGEMENT

4.5.1 Description

The *mobile wallet* is a container that may house one or more *accounts* (i.e., value stores that are sources or repositories of funds). In developing countries, the only payment source in a mobile wallet may be a prepaid account backed by funds deposited with the DFSP. However, in more advanced implementations, a digital wallet might include one or more bank accounts, debit cards, or credit cards controlled or owned by the digital wallet holder.

For simplicity, we use the term *account* to refer to a value store associated with the mobile wallet.

4.5.2 Rationale

These are the necessary basic account management features to support the pro-poor use cases visualized in the reference model. In particular, the one-to-many relationship of wallet to accounts is important in developing countries, where multiple users in a household may perform transactions on one handset.

4.5.3 Requirements

4.5.3.1 Manage Account Detail

1. The mobile wallet **shall** enable account holders to update their account details, including linked accounts and payment sources, account aliases, authorized users, contact information, associated rights and privileges, etc. The mobile wallet holder should have the ability to update information associated with both the accounts contained in the mobile wallet and the mobile wallet itself.

Rationale: After a mobile wallet and associated accounts are established, it is likely that some information will change over time. If updates are not supported, data will quickly grow stale and accounts would likely be abandoned, and even reopened with proper information.

2. The system **should** allow all notification messages to be configured on or off depending on user preferences.

Rationale: Added flexibility for the user to customize their mobile wallet.

Humanitarian Response Rationale: A user may feel the need (for safety or security reasons) to keep their enrollment in a cash disbursement program private.✚

3. The system **should** enable the user to select the language and script of their choice from a list in the user interface.

Rationale: Increases usability if the user can select the preferred language and script.

4.5.3.2 Add an Account

1. A mobile wallet **must** have access to one or more accounts for use in payment transactions.

Rationale: Without access to a store of value there is no source of funds to make a payment, or repository of funds to receive a payment.

2. During mobile wallet setup, the system **shall** automatically establish a default account that is uniquely identified in the context of the payment system (typically by assignment of an account ID).

Rationale: Establishing an account at setup ensures the mobile wallet can be used for financial transactions on conclusion of setup.

3. The mobile wallet **should** permit the authorized holder to add sub-accounts under the default account, with each account receiving a unique ID number within the context of the payment system.

Rationale: Mobile wallet holders will benefit from finer control of how funds are segregated for various purposes. For example, they may want to keep funds for paying utilities separate from those to pay school fees.

4. The mobile wallet **shall** provide a default alias (i.e., human-readable name) for each account at the time of creation, unique within the context of the mobile wallet.

Rationale: Enables the user to easily differentiate between multiple accounts that are linked to the mobile wallet.

5. The system **shall** allow the authorized user to change the alias associated with any mobile wallet account they control.

Rationale: The user should have flexibility to alter the alias to reflect the current use, or to provide a clear reminder of its intended use.

6. An authorized account holder **should** be able to delegate authority to additional users on an account-by-account basis within the context of the mobile wallet.

Rationale: The account holder may want to give a spouse access to a mobile wallet account for paying household expenses, but not to other segregated funds in the same wallet.

7. Additional users **must** be registered with the DFSP before they can be associated with a mobile wallet account by the mobile wallet holder.

Rationale: Each individual needs a unique identifier in the scope of the DFSP. Ideally, every individual would only be represented with a single user instance in the payment ecosystem.

8. When authority is delegated on a mobile wallet account, the authorized holder **shall** always retain full control of the account to which additional authorized users are added.

Rationale: The mobile wallet should belong to one individual, with that person having master control over any accounts within the mobile wallet. Added users should not be able to take control away from the original owner of the mobile wallet or the accounts contained therein.

9. Where feasible, the rights and privileges that **may** be assigned to a delegate user **should** be individually grantable and retractable.

Rationale: This provides the most flexibility to meet potential use cases. For example, a delegate user may only be able to see available balance, be able to make a payment for a specified bill, accept payments for retail sales on my behalf, etc.

10. The mobile wallet **should** allow the holder to delegate bill payment to a delegate user for individual or recurring bills.

Rationale: The wallet holder can limit where funds can be spent, even if a delegate is authorized to spend funds within a mobile wallet account. Thus, the wallet holder has detailed control of not only what activities the delegate can do (e.g., pay someone), but with whom those activities are permitted (e.g., Vendor A but not Vendor B) in the context of a particular shared account.

11. The capabilities and limits of any account within the mobile wallet **should** be based on the KYC levels associated with the mobile wallet account holder, and not those of any delegate users.

Rationale: Delegate users are effectively separate authorization sub-domains within the mobile wallet. Because the mobile wallet holder has full control of any account in the mobile wallet, that individual's limitations should take precedence.

4.5.3.3 Switch Accounts

1. The mobile wallet **shall** allow the user to designate the active account when multiple accounts are registered with the mobile wallet.

Rationale: The mobile wallet activities are generally applicable at an account level. Thus, the user either needs to designate the account context as a default, or select the account when each activity is performed.

2. When the *switch account* action is initiated, the user **shall** be presented with a list of accounts registered with the mobile wallet.

Rationale: Presenting choices improves usability.

3. The currently active account **should** be indicated when the account list is displayed. For example, the active account may be preceded with an asterisk (*), bolded, or otherwise highlighted depending upon the capabilities of the display.

Rationale: Highlighting the active account assists the user in identifying other choices.

4. The mobile wallet **shall** indicate the current account by displaying the account name on the main screen.

Rationale: Displaying the active account improves usability.

5. The mobile wallet action context **shall** conform to the type of account selected when the active account context is changed.

Rationale: A wallet may have different types of accounts registered (e.g., a consumer and a merchant account), thus the wallet should update the available actions to provide the proper capabilities associated with the various account types.

4.5.3.4 Access a Mini-Statement

The *mini-statement* allows the wallet holder to view the details of their account(s), including both the current status and historical activity.

1. The mobile wallet **shall** provide a mini-statement function, displaying details for the selected account, including current status and historical activity.

Rationale: Mobile wallet holders may not have access to paper histories of their accounts. Providing visualization of the account history aids in issue resolution, supports enquiry of past activity, and facilitates tracking of transactions and understanding of fees.

2. The mini-statement **shall** require the user to enter their PIN prior to viewing

Rationale: The account balance is private information.

3. The mini-statement **should** be free for the user to view.

Rationale: Encourages trust in the system.

4. If there is a fee for the mini-statement it **shall** be presented, and the user **must** agree before the fee is charged.

Rationale: Encourages trust in the system. However, a fee to access the mini-statement should be avoided if possible.

5. The mini-statement **shall** display the current balance of the selected account.

Rationale: The user will likely want to see this data frequently. It is recommended that the balance be displayed at the top of the history.

6. The mini-statement **shall** display historical transactions in reverse chronological order (i.e., newest to oldest).

Rationale: It is reasonable to assume the user will enquire regarding more recent transactions.

7. The mini-statement **shall** display the historical transactions in groups appropriate to device (i.e., page the list of transactions).

Rationale: Limiting the display to a useful number of records reduces unnecessary data transmission and improves the user experience.

8. The mini-statement **shall** provide the ability for the user to move serially through the available set of historical transactions in either direction, as the data permits (i.e., next/previous page).

Rationale: Users will need to be able to navigate the paged data set since all records are not displayed at one time.

9. The UI **shall** provide the ability to scroll the display if all returned data is not viewable within the screen area.

Rationale: Some screens will not have the ability to display all of the paged transaction data, thus requiring some method to visualize the obscured off-screen data.

10. At a minimum, each mini-statement historical transaction record **should** indicate the following:

a. The name of the transacting third party (payee or payer, as appropriate)

b. The transaction amount

c. The transaction date

d. Any fee amount the user paid to execute the described transaction

Rationale: These are the minimum values needed to reasonably describe the transaction. However, the list is not exhaustive.

11. The mini-statement shall include headings for each data element presented.

Rationale: The data may not be intuitive. Providing headings reduces user learning curve and confusion.

12. The mini-statement **shall** follow a consistent presentation convention to clearly delineate each data value. For instance, a semicolon (;) may be used as a delimiter between each data element value in a displayed transaction record resulting in "Name;Amount;Date;Fee" for a header, with corresponding sample values of "Hassan Jat;-150.25;11Nov2014,-2.00".

Rationale: Delineating values improves readability.

13. The mobile wallet **shall** display the mini-statement for the active account context.

Rationale: The mobile wallet may contain multiple accounts, so clarity is needed.

14. The mobile wallet **should** include the account ID in the mini-statement display.

Rationale: Reduces confusion if multiple accounts are available.

4.6 SET UP A MOBILE WALLET

4.6.1 Description

There are many aspects to configuring the mobile wallet for use. This section describes the required component configurations to enable the mobile wallet for use in several potential deployment environments.

4.6.2 Rationale

Preconditions for use of the mobile wallet must be designated to provide clarity.

4.6.3 Requirements

4.6.3.1 Provision an Account (Payment Services)

Mobile Financial Services Providers (DFSPs) operate *payment services*, enabling individuals to send and receive payments with other subscribers to that or other partnering DFSPs' payment services.

In a *closed* system, the mobile wallet subscribers are typically only able to send and receive payments within the customer base of that specific DFSP. The foundation advocates for an open, integrated model, where subscribers of one DFSP can make payments to subscribers on a different DFSP. The preferred architecture identifies a central switch (the IST) to route payment messages between DFSPs.

Thus, this section provides requirements to enable support of multiple accounts from a single DFSP. A *horizontal* wallet approach is included for information only, and does not reflect the *vertical* wallet implemented in the prototype, where the mobile wallet connects only to accounts of a single DFSP.

See *6.1.1, Mobile Wallet Approaches* for more details.

Vertical Wallet Implementation

1. The mobile wallet **shall** utilize the account of the registering DFSP by default.

Rationale: In scenarios where the registering DFSP is the only account, it must be utilized.

Horizontal Wallet Implementation Only

2. The mobile wallet **shall** allow the user to provision at least one account for transaction handling.

Rationale: The mobile wallet cannot be used for payments if no account is provisioned. This is implied in the prototype, as the wallet functionality is hosted at the DFSP.

3. If more than one payment source is configured in the selected service, the mobile wallet **shall** allow the user to select one as preferred payment source.

Rationale: Storing the user preference reduces effort to use the mobile wallet for payments.

4. When only one account is provisioned, the mobile wallet **shall** default to the configured payment source.

Rationale: Fewer steps are required to set up the mobile wallet if a default is selected when only one account is available. The user still has full control to select no default.

5. The mobile wallet **shall** allow the user to activate and deactivate provisioned payment services on demand.

Rationale: Fee structures or other considerations might incent the wallet holder to selectively enable or disable payment services.

6. The mobile wallet **shall** allow the user to view a list of payment services registered for use with the mobile wallet.

Rationale: When more than one account may be registered, the information must be accessible to the user so that they might make informed decisions on adding, dropping, or managing payment services.

7. The mobile wallet **shall** allow the user to designate a primary account when more than one account is configured.

Rationale: Storing the user's preference reduces effort required to use the mobile wallet for payments.

8. The mobile wallet **shall** ask the user to select an account *at the time of use* if no provisioned account is set as default.

Rationale: Users may prefer to have no default payment service, and instead select the service each time one is needed.

9. The mobile wallet **may** allow the user to assign a primary account and source for each payment situation.

Rationale: The user may want to use one account and payment source pair to purchase goods at a merchant, and another to pay taxes or receive a remittance. This could potentially include saving defaults for each recipient, for example, store different sets of preferences for Merchant A and Merchant B.

4.6.3.2 Payment Transaction Modes

Mobile payments are generally performed in one of two modes:

- Remote: Parties use a mobile device to send and receive payments or transfer funds purely over the mobile channel, irrespective of their physical locations. In reality, the parties may be standing in the same store, but the payer does not use the merchant's point of sale (POS) infrastructure to initiate payment. Initiating a payment through a USSD session on a basic GSM phone is an example of a remote payment.
- Proximity: The mobile device is used primarily to authorize a payment at the point of sale and relies on the infrastructure for the payment recipient to process the transaction. Using a biometric fingerprint scanner tied to a POS terminal to authorize a purchase in a store is an example of proximity payment.

The mobile wallet described herein supports both payment modes. However, the *emphasis is on remote payments*, as the model can be supported with ubiquitous GSM phones and does not require sophisticated biometric scanners or POS systems. Similarly, remote payment models have greater utility because the buyer doesn't need to physically travel to a merchant to authorize payment.

1. The mobile wallet **shall** allow the end user to make remote payments (i.e., perform the payment without interacting with the payee's proximate payment system).

Rationale: This is the primary operating mode, where the payer does not interact with the payee's infrastructure or POS system directly, but performs all payment actions on their mobile device through the mobile channel.

2. The mobile wallet **shall** enable the user to make proximity payments when compatible systems are available (i.e., interact directly with the merchant payment system).

Rationale: This alternate payment mode allows the payer to use their mobile wallet outside of the mobile channel, potentially leveraging the payer's equipment and infrastructure (e.g., POS system).

4.6.3.3 Associate a Bank Account

In bank-led mobile payment systems, a formal bank account often serves as the value store for mobile payment. In the mobile operator–led model described herein, value is stored in the DFSP system, with the DFSP commingling the funds in common accounts held at one or more banks.

1. The mobile wallet **should** allow the user to register a formal bank account as a recipient of payments.

Rationale: Bank accounts offer additional features (e.g., ability to earn interest, access to bank branch system) that may not be available with e-money. Further, e-money does not yet have the same ubiquity as cash. Thus, a mobile wallet holder may wish to regularly send excess value to a bank account, and access cash through their bank instead of paying fees at a mobile money agent.

2. The mobile wallet **shall** allow the user to unregister a previously registered formal bank account.

Rationale: A user might choose to unlink their mobile wallet from their bank account for many reasons (e.g., discontinuing use of the mobile wallet, closing the bank account).

4.6.3.4 Registered Bank Account Capabilities

The proposed model only permits push payments. Thus, an external bank account typically serves as a value "sink," allowing the mobile wallet holder to disburse funds from a stored value account held at the DFSP to their formal bank account. Inbound transfers from a formal bank account would need to be authorized from the banking system, since the mobile wallet has no pull payment capability.

1. The mobile wallet **shall** enable the account holder to transfer funds from the mobile wallet account to a registered formal bank account.

Rationale: A user may have excess value in their e-money account and want to move it to an interest-bearing savings account held at his bank.

2. The mobile wallet **should** allow a registered bank account to be designated as the default bank account.

Rationale: Allows more automation. If no default exists, the user would have to elect a specific registered bank account whenever such an account was needed.

3. If regulation allows and the holder elects to do so, the DFSP **should** automatically transfer value over the maximum account limit to an associated bank account when an inbound payment would violate the permitted e-money account maximum value limit.

Rationale: The situation would occur where a user's e-money account does not have enough headroom to receive the total value of an inbound payment. Thus, it is helpful to have an automatic solution to enable the full inbound payment amount to be received.

4. The mobile wallet holder **must** provide the bank ID, the target bank account number, and the bank account owner name to register the bank account.

Rationale: This is the information required to reasonably confirm account ownership. Note: As this is a push account, there is little risk to the bank account holder.

5. The DFSP **should** employ an account verification to confirm the account exists, can receive funds, and that the mobile wallet holder has access to the account.

Rationale: Verifying the account reduces the potential for misdirected transfers.

6. The DFSP **should** automatically transfer a nominal random amount to the target bank account to verify it can make the deposit.

Rationale: A successful micro-deposit confirms that the account exists and subsequently enables verification that the mobile wallet holder has access to the account.

7. The mobile wallet **should** require that the mobile wallet holder confirms the deposit before the account is permitted to receive funds.

Rationale: Requiring confirmation dramatically reduces the chances that an invalid or incorrect account was configured, and thus increases trust in the system. For example, if the DFSP deposited 3 units of local currency into the account, the mobile wallet holder must respond "3" when challenged by the account activation process.

4.7 MAKE A PAYMENT

4.7.1 Description

A key value driver of the mobile money ecosystem is the ability to transfer value electronically between parties, regardless of proximity. In the proposed model, payment authorization is always initiated by the payee (i.e., *push payment*), though recipients would be able to request a payment, thereby simplifying activity on the payee side and potentially improving the process flow at the point of sale.

The mechanics of a payment require the payer provide the necessary information (i.e., payee, amount) to create a payment instruction that can be executed by the payment ecosystem components. The payee would then authorize the payment after review and acceptance of any fees.

The model primarily relies on the payer pre-funding an account tied to the mobile wallet and held by the DFSP. Thus if the payer and payee are on the same DFSP, the payment is considered "on-us" from the DFSP's perspective, and may be completed entirely within the mutual DFSP's system. If payer and payee are on separate DFSPs, the payment is considered "off-us," and must be routed through the network for final processing.

Typical use cases include sending money to another person, buying goods, or paying for services. Payments may either be solicited (e.g., a biller sends a request for payment) or unsolicited (e.g., the wallet holder initiates the payment process).

- Bill payment may be differentiated in that the payment instruction might be stored and automatically authorized for subsequent use or on a pre-determined schedule.
- Person-to-person (P2P), remittance, and person-to-small-merchant payments are operationally the same (identify the recipient, provide the amount, and approve the payment).
- Person-to-business (P2B) is specialized when the business presents a bill, but is otherwise the same as P2P (except that the recipient is not an individual).
- Person-to-government and person-to-large-business may be specialized, in that additional information may be needed to ensure proper credit for a specific debt.

4.7.2 Rationale

Sending and receiving payments are the two primary uses of a mobile wallet.

4.7.3 Requirements

1. The system **shall** enable a mobile wallet holder to pay a third party by instructing the DFSP to transfer value from an account registered with the mobile wallet.

Rationale: This is a core function of the mobile wallet.

2. The user **shall** lose access and control of funds paid out from their account immediately upon execution of that payment.

Rationale: Needed to ensure validity of the payment system.

3. The mobile wallet **should** allow the user to make a payment using any available payment channel (e.g., USSD, WAP, SMS, phone-based apps, SIM-based apps).

Rationale: Improves ability to perform the transaction.

4. The system **shall** allow the user to designate the intended payee by entering the phone number, alternate ID, specific account number.

Rationale: Providing alternatives allows for better flexibility where privacy or cultural concerns might otherwise impede sharing of the phone number of the payee.

5. The system **may** allow the user to designate the intended payee by selecting the intended payee through the phone's contact list.

Rationale: Using a contact list provides better usability for low-literacy users and prevents key-stroke errors.

6. The system **shall** enable the payer to select the payee from a list of the 5 most frequent payees, or to designate a different payee.

Rationale: Providing a most-used payee list improves usability, and potentially reduces data entry errors when designating a payee.

7. The system **may** allow the user to include a short message or note as part of the payment instruction.

Rationale: Larger payees may need detail on why the payment is being sent or to which bill it should be applied. For example, if a person has several children at a school, but wishes to pay tuition for only one at a specific time.

8. The system **shall** display the common name of the payee in response to submission of the payee identifier (i.e., phone number, alternate ID, account number) provided prior to completion of the payment.

Rationale: Provides feedback to allow sender to confirm the entered information matches the expected recipient.

9. The system **shall** enable the payer to abort a payment process up until the user actively confirms the payment, enabling execution.

Rationale: Provides an opportunity to correct errors before committing the payment.

10. The system **shall** display the transaction details (e.g. recipient, total amount with any added fees) and require the user to confirm the transaction by entering in their PIN.

Rationale: Provides an opportunity to see a summary of the transaction and any fees before confirming the payment.

Humanitarian Response Rationale: Transaction fees may be temporarily dropped in a response situation. The fee must be separated out so the user is clear on the fee they are paying, or lack thereof.✚

11. When a payment is sent, the system **shall** log all details of the transaction (e.g., amount, date and time, payer, payee)

Rationale: Logging enables historical review for issue resolution or later display.

12. The system **may** allow for transaction to be geo-tagged based on the location of the user when a transaction is completed using GPS technology, if available and with user consent.

Rationale: The DFSP could use this geo-tagged transaction data to provide additional support services or for fraud prevention assessments/analysis.

Humanitarian Response Rationale: A humanitarian response agency may use this information to understand people migration in a crisis situation, especially in the case of internally displaced people (IDP) or refugees.✚

13. The system **should** support multifactor authentication for transaction authorization in high-risk scenarios (e.g., funds transfer).

Rationale: Phones can be stolen, SIM cards can be cloned, PINs can be observed. By adding a second factor, it is more difficult to perpetrate fraud.

14. The system **should** be capable of utilizing time-limited, one-time-use passcodes for transaction authorization.

Rationale: Providing a one-time-use code with a limited lifespan enables financial transactions with merchants, businesses, or individuals when no lasting relationship is required. It also facilitates fraud prevention in the event a static PIN is compromised.

15. The mobile wallet may enable the user to transfer value in response to a request for payment. (See *4.8, Pay a Bill*)

Rationale: Allows payer to respond directly to a bill, invoice, or other request for payment without having to enter all of the payee details.

16. The system **may** allow the user to schedule a payment to be executed at a future date and time.

Rationale: Providing future payment scheduling improves usability.

17. The system **shall** allow the user to cancel any payment schedule for a future date/time.

Rationale: Planned payments can change for a variety of reasons.

18. The system **shall** notify the user when funds have been transferred from the mobile wallet account.

Rationale: Closes the loop on the user action and provides awareness in the event of misuse.

19. The notification of funds transfer **should** include payee name, payee ID, amount transferred, any fees paid, and the time and date of transaction completion.

Rationale: This is the minimum information needed to distinguish the payment.

20. The system **should** provide a notification if the transaction request times out and does not complete. The notification should include: recipient name, amount, date and time of failure, and suggested next step (e.g. "Please try again in a few minutes"). This notification message may also include a phone number for users to follow-up with question.

Rationale: Let a user know when a payment submission failed so they can try to send again.

4.8 PAY A BILL

4.8.1 Description

A bill payment is a special case, as the payer is first presented with a request for payment by the ultimate payee. Given the proposed model is based on push payments (i.e., payers authorize payment at the time of sending), billers cannot initiate a direct debit (or pull) payment. Thus, an efficient alternative is to allow a biller to request payment for goods or services. This is advantageous as the payer does not need to enter the recipient details or amount, but rather confirms the payment request details, reducing potential misdirected payments.

In an example scenario, the mobile wallet holder has a variety of goods they wish to purchase at a store. The merchant's POS system has the ability to request payment from a mobile payer, and thus totals the goods, enters the payee's mobile phone number, and sends a payment request. The payer receives a notification of a pending bill that includes the requested amount and identifies the payee. The payer reviews the payment request and authorizes payment. The system processes the payment, notifying the merchant, who then releases the goods to the buyer, completing the purchase. After the transaction is completed, both the payer and the merchant receive a confirmation message with the transaction details (e-receipt). A physical receipt may be issued by the POS device.

This model is particularly effective in that the payee is expecting the request for payment, and can easily confirm the requested amount and then authorize payment.

Fraud Note: Care needs to be taken to protect the mobile wallet holder from fraudulent, unfounded payment requests. *High-volume* bogus requests or spam would likely be controlled at the switch or DFSP level, as improper activity could be reported or identified centrally, the sending account blocked, and related transactions voided. However, *individual* spam requests are likely if only a phone number is needed.

4.8.2 Rationale

The proposed bill-paying process reduces the opportunity for misdirected payment or errors in the payment details when initiated by the payer. Paying an invoice is a common practice in commerce, whether the biller is a utility, school, merchant, or someone owed a debt.

4.8.3 Requirements

1. The mobile wallet **shall** support payment requests (i.e., bill pay).

Rationale: This enables large sophisticated billers (e.g., utilities, schools, large merchants, governments) to invoice large populations of payers efficiently, while also supporting the needs of small sellers or other consumers to *request payment. As discussed in The Level One Project Guide, adoption of the system by government is a key condition of success for DFS System deployments. Government acceptance not only drives initial transaction volume (thus immediately lowering costs), but it is also a visible endorsement of the payment system.*

2. The mobile wallet **should** allow the user to activate or deactivate acceptance of payment requests.

Rationale: Allowing the user to enable or disable the capability reduces fraudulent requests (spam) or nuisance, if the requests became problematic for the mobile wallet holder.

3. The mobile wallet **shall** queue pending payment requests for review by the mobile wallet holder.

Rationale: The user may not be available to address a request as it is delivered, thus a queue is needed to collect the payment requests.

4. The mobile wallet **should** notify the user when a request for payment is received.

Rationale: Notification provides maximum time for review and action by the recipient.

5. The mobile wallet payment request **shall** display the total amount requested, inclusive of any added fees or charges.

Rationale: Fee transparency is key to maintaining user confidence in the system.

6. The mobile wallet payment request **shall** clearly and separately display **each** added fee or charge in the context of the payment request.

Rationale: Granular fee details provide clarity and help to maintain user confidence in the scheme.

7. For each payment request, the mobile wallet **shall** allow the user to authorize payment, delete it, or re-queue the request.

Rationale: The wallet holder needs full control over payment requests.

8. The mobile wallet **should** allow the holder to dial the biller directly from the request if supported by the mobile device.

Rationale: This makes it easier for a payer to discuss the invoice/bill with the sender.

9. If the mobile wallet holder elects to authorize payment for a payment request, the mobile wallet **shall** require the payer to enter a valid PIN, or verified biometric measurements (if supported by the device).

Rationale: Requiring confirmation protects against unintended payment while viewing that request for payment record.

10. The mobile wallet **should** allow the holder to add billers to an Approved Senders list, explicitly enabling receipt of payment requests from the designated senders.

Rationale: Enables selective receipt of payment requests to only approved, known senders. This is a common technique in firewalls where all inbound requests are rejected unless from specifically pre-approved senders. The use of whitelists could significantly reduce the exposure to fraud scenarios using payment requests to trick people into payment approvals.

11. The mobile wallet **should** allow the holder to add billers to a Blocked Senders list, explicitly rejecting all payment requests from the designated senders.

Rationale: Enables selective blocking of nuisance billers or bad actors. Another common firewall technique is to allow general acceptance of messages, with the ability to automatically reject messages from known bad actors.

12. The mobile wallet **should** allow the holder to report fraudulent payment requests to the DFSP for review and follow-up action.

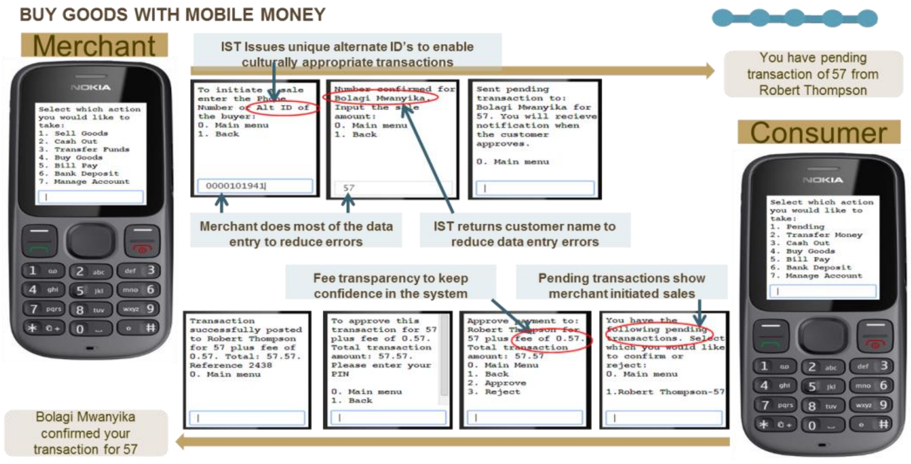
Rationale: Improves awareness at a higher level of the ecosystem, and makes the information available to improve fraud detection and prevention tools of the ecosystem partners.

4.9 REQUEST A PAYMENT

4.9.1 Description

In commerce, businesses and individuals routinely request payment for services rendered, goods sold, or outstanding debt. Thus, it is reasonable to support this function in the mobile wallet.

Section 4.8, Pay a Bill, describes how the system should enable payment when presented with a demand. This section provides details on originating the demand. The following diagram highlights the prototype's implementation.



BUY GOODS WITH MOBILE MONEY

Merchant

```
Select which action
you would like to
take:
1. Sell Goods
2. Cash Out
3. Transfer Funds
4. Buy Goods
5. Bill Pay
6. Bank Deposit
7. Manage Account
```

IST Issues unique alternate ID's to enable culturally appropriate transactions

```
To initiate a sale
enter the Phone
Number or Alt ID of
the buyer:
0. Main menu
1. Back
0000101941
```

```
Number confirmed for
Bolagi Mwanyika.
Input the sale
amount:
0. Main menu
1. Back
57
```

```
Sent pending
transaction to:
Bolagi Mwanyika for
57. You will recieve
notification when
the customer
approves.

0. Main menu
```

Merchant does most of the data entry to reduce errors

IST returns customer name to reduce data entry errors

You have pending transaction of 57 from Robert Thompson

Consumer

```
Select which action
you would like to
take:
1. Pending
2. Transfer Money
3. Cash Out
4. Buy Goods
5. Bill Pay
6. Bank Deposit
7. Manage Account
```

Fee transparency to keep confidence in the system

Pending transactions show merchant initiated sales

```
Transaction
successfully posted
to Robert Thompson
for 57 plus fee of
0.57. Total: 57.57.
Reference 2438
0. Main menu
```

```
To approve this
transaction for 57
plus fee of 0.57.
Total transaction
amount: 57.57.
Please enter your
PIN

0. Main menu
1. Back
```

```
Approve payment to:
Robert Thompson for
57 plus fee of 0.57.
Total transaction
amount: 57.57
0. Main Menu
1. Back
2. Approve
3. Reject
```

```
You have the
following pending
transactions. Select
which you would like
to confirm or
reject:
0. Main menu

1.Robert Thompson-57
```

Bolagi Mwanyika confirmed your transaction for 57

4.9.2 Rationale

There are multiple scenarios where mobile wallet holders may need to request payment. For example, a merchant may facilitate a request for payment from a consumer wishing to pay with mobile money, or another consumer may need to request funds for a debt.

4.9.3 Requirements

1. The mobile wallet **shall** enable an authorized holder to request payment from (i.e., invoice) a third party.

Rationale: This enables large sophisticated billers (e.g., utilities, schools, large merchants, governments) to invoice large populations of payers efficiently, while also supporting the needs of small sellers or other consumers to request payment.

2. The user **must** provide the amount requested and the phone number or alternate ID of the payment request recipient.

Rationale: This information is needed to route the request and specify the demand.

3. The system **may** allow the sender to include an expiration date for the payment request.

Rationale: Some payment requests may not be valid until completed, but rather only until some deadline.

4. The system **shall** notify the requester when a payment request has expired before payment is received.

Rationale: Notification provides a reminder that further action may be needed.

5. The system **may** allow the sender to include a text note with the payment request.

Rationale: A text note could include a reminder of why the request is being sent, or an invoice/tracking number, etc.

6. The system **should** respond with name of the recipient associated with the phone number or alternate ID prior to requesting approval to send the request.

Rationale: Providing the corresponding recipient allows the sender to confirm the phone/ID match the expected recipient, and correct the target address prior to sending the request.

7. The mobile wallet **shall** indicate to the wallet holder that the request was sent.

Rationale: Provides assurance that the request has been made.

8. The system **should** allow the requestor to rescind a payment request that has not been paid by the recipient.

Rationale: Allows for correction of requests sent in error, cancellation, or other retraction.

9. The system **should** remove rescinded or expired payment requests from the recipients pending payment requests queue.

Rationale: Rescinded or expired payment requests should be cleaned up and removed from the payer's mobile wallet, to avoid accidental or improper payment.

10. The mobile wallet **shall** display a list of outstanding payment requests (i.e., pending transactions).

Rationale: Allows the requester to track and follow up on payment requests that have not been fulfilled.

4.10 VOUCHER PAYMENT

4.10.1 Description

Governments and NGOs that provide aid to individuals in need often find high levels of leakage when delivering targeted aid. A 2010 study calculated that Egypt could save up to 73 percent of the cost of food subsidies if leakage could be eliminated and the subsidy program's beneficiary population and geography better targeted.[11] In an effort to reduce leakage and improve access to aid, some developing countries are leveraging digital payments technology to deliver subsidies directly to the beneficiary, cutting out intermediaries and reducing fraud.[12]

Both bulk digital payments and vouchers rely on the mobile channel for distribution, avoiding issues related to cash distribution. Bulk payments are decomposed into individual beneficiary payments and can be subsequently converted to cash at the discretion of the recipient. Thus, the desired goal of keeping money digital is stunted.

Alternatively, vouchers cannot be converted to cash, but must be expended through the digital payment channel at a pre-approved set of vendors. This constraint helps drive acceptance of digital payments, as merchants must accept digital payments or miss the sales opportunity. The voucher digital payment provides additional benefits over bulk payment and cash, as the voucher provides voucher issuers with mechanisms to be assured aid is used as intended:

- Voucher use can be limited to only vetted, approved and trusted merchants
- Voucher value can be limited to a percentage of the total purchase, thus assuring the recipient is personally invested in the goods purchased
- Voucher usage details can be collected showing timing and location details of aid distribution
- The voucher issuer may retain control of the money until the voucher is redeemed, though regulation could drive escrow of the funds at the time the voucher is created.

The demonstration prototype includes a method for distributing and redeeming subsidy vouchers through the mobile channel. The solution relies on various parts of the mobile payments ecosystem to fully implement the desired distribution and usage control, including the IST, DFSP, and mobile wallet.

As demonstrated in the prototype, the voucher issuer defines constraints on the voucher's use, including:

- Maximum value
- Percentage value of the total sale that the voucher will cover
- Merchant locations where the voucher may be used
- Expiration date

[11] Sherine Al-Shawarby, Heba El-Laithy, Ahmad Iman Youssef, and Iman Sadek, "Egypt's food subsidies: benefit incidence and leakages," Social and Economic Development Group, Middle East and North Africa Region, The World Bank, September 16, 2010.

[12] http://www.fmard.gov.ng/news_inside/135

In the primary usage model, recipients receive notification when the vouchers are distributed by the benefactor, describing the terms of use (i.e., constraints) and the potential value. The mobile wallet tracks vouchers for quick reference, but the value is not transferred to the mobile wallet.

The recipient is responsible for redeeming the voucher on eligible purchases. It is only the point of the purchase transaction where the voucher is converted into payment instructions for the benefit of the selling merchant and the actual value is transferred by the voucher issuer directly to the merchant.

4.10.2 Rationale

Vouchers can play a critical role in increasing the access to aid by the targeted beneficiary while providing improved assurance that the aid was used for the purpose intended by the provider.

4.10.3 Requirements

4.10.3.1 Voucher Notification and Logging

1. The DFSP **shall** send a notification (e.g., SMS message) to the designated beneficiary when a voucher has been delivered for the benefit of the mobile wallet holder.

Rationale: The IST distributes voucher notifications to the DFSP, who is responsible for distribution to the mobile wallet holder. SMS is a typical out-of-band notification method in the expected environment.

2. The DFSP **shall** send a notification (e.g., SMS message) to the designated beneficiary when a voucher retraction message has been delivered.

Rationale: Proactive notification ensures the beneficiary is aware if a voucher is no longer available.

3. If the voucher's effective value reaches zero (e.g., expired, retracted or its value exhausted), the voucher **shall** not be displayed in the available voucher list in the mobile wallet.

Rationale: Housekeeping—the voucher has no value, so there is no reason to clutter the user interface or give the impression that there may be some residual use for the voucher.

4. The system **shall** log all voucher usage, including but not limited to voucher IDs, participant IDs, amounts transacted, date/time of use, and the mode of use (merchant- or purchaser-initiated).

Rationale: Logging is required to support stakeholders' analysis of use.

4.10.3.2 Voucher Constraints

1. The system **shall** identify eligible vouchers at the time of payment.

Rationale: Vouchers are intended to be used only under specific conditions. Therefore, the system must evaluate the details of the payment transaction to determine if it meets the constraints defined by voucher issuer.

2. The system **shall** consider a voucher eligible for use in a payment transaction when **all** of the following are true:

- The voucher is registered in the mobile wallet.
- The voucher has reached the activation date. (A voucher issuer may provide a voucher in advance of the date it is intended to become active and valid.)
- The voucher has not reached the expiration date.
- The voucher has not been retracted by the issuer.
- The voucher has a positive, non-zero value.
- The payee is identified as a permissible merchant under the terms of the voucher usage constraints.

Note: An additional constraint is that the voucher may only be used to purchase permissible goods. This constraint is primarily enforced by the merchant, as the mobile wallet and DFSP do not know the specific goods being purchased. In a sophisticated infrastructure, the merchant's POS might share the SKUs of items being purchased, so the system can validate their eligibility (similar to coupon enforcement in a modern grocery store). However, the expectation is that such capabilities are not broadly available in the target deployment environment.

Rationale: These are standard constraints to ensure the voucher is valid for use.

Humanitarian Response Rationale: Agencies may constrain voucher use in order to adhere to donor restrictions and other regulations or be motivated by a programmatic objective by selecting the merchants (and goods) for which the voucher is eligible.✚

3. The system **shall** allow only one voucher per payment transaction.

Rationale: Using multiple vouchers (i.e., chaining) would diminish the ability of the voucher issuer to require personal investment by the payee.

4. The system **shall** allow partial use of its value.

Rationale: Allowing for multiple transactions provides more flexibility to the user and promotes more frequent usage of digital payment services.

5. The system **must** subtract the expended value from the total defined voucher benefit to provide the remaining available value to the beneficiary.

Rationale: Vouchers have a starting value that must be reduced with each expenditure to ensure the financial integrity of the voucher system.

4.10.3.3 Merchant-Initiated Voucher Use

In this mode, the merchant (i.e., payee) may use a POS system, mobile app, or mobile device using USSD. Regardless of the endpoint, the consumer (i.e., purchaser) must provide their phone number or alternate ID for the merchant to access the voucher and request payment from both the voucher issuer and purchaser (i.e., copayer).

1. The system **shall** automatically determine if the purchaser's mobile wallet has a voucher that is eligible for use when the merchant initiates the sale and provides either the purchaser phone number or alternate ID.

Rationale: Improves usability for the merchant, increases likelihood of voucher use, and thus maximizes value to the purchaser.

2. The system **shall** notify the merchant that the purchaser has one or more eligible vouchers available for use.

Rationale: Notification to the merchant provides clear awareness of the voucher availability and improves potential for utilization of the benefit available to the purchaser.

3. The system **shall** allow the merchant to request payment via either voucher or mobile money.

Rationale: The goods being purchased may or may not be covered by the voucher. Merchants should be aware of such issues and support the intent of the voucher's issuer.

4. The system **shall** notify the purchaser that the merchant has requested payment using a voucher, displaying the total purchase amount, voucher value, and any added fees.

Rationale: Purchaser awareness and subsequent approval are key to control of voucher use. Also, fees must be transparent.

5. The system **shall** automatically calculate the amount not covered by the voucher and present the purchaser with the option to pay the remaining amount with another payment source (e.g., e-money, cash).

Rationale: Improves usability by performing the basic math calculation for the participants.

6. The purchaser **shall** have the option to approve or cancel the voucher's usage.

Rationale: The payer must retain control of authorizing any transaction. This is a key ground rule.

7. The purchaser **must** enter their PIN to approve the transaction.

Rationale: Provides positive confirmation of intent and control of funds.

8. If the purchaser does not approve the voucher's use, the payment request **shall** be canceled and no funds will be transferred.

Rationale: Value must be preserved if a transaction is not performed.

9. If the payer approves the voucher's use, the payment **shall** complete and the designated value will be deducted from the participating funding sources (i.e., voucher provider account and purchaser stored value account).

Rationale: Required to ensure the integrity of the payments ecosystem.

10. The system **shall** notify the merchant and the payer, indicating the status (complete or canceled) of the payment transaction, and display the total amount of the transaction and the amounts provided by each participating account. For example, "Total charge 50: 30 paid by voucher and 20 paid by e-money."

Rationale: Notification confirms payment, completing the process and assuring the merchant that goods can be released to the purchaser.

4.10.3.4 Purchaser-Initiated Voucher Use

1. When payment is initiated, the system **should** automatically determine if the purchaser's mobile wallet has a voucher that is eligible for use at the specified merchant.

Rationale: Automatic detection improves likelihood of use.

2. If an eligible voucher is identified, the mobile wallet **should** present the user with the option to select a voucher for use in the transaction.

Rationale: Access is needed for expenditure.

3. The system **should** include the voucher as the first payment source option (i.e., before stored value or cash) when a voucher is deemed eligible in the context of the initiated payment transaction.

Rationale: Putting the voucher payment first improves the likelihood of use, and thus maximizes the benefit to the purchaser.

4. At time of use, the system **shall** display the effective value of the voucher and the amount remaining to be paid by the purchaser through other means (e.g., stored value account or cash) to meet the total purchase amount.

Rationale: Improves usability by performing the basic calculation for the purchaser, and protects against overpayment.

5. The system **should** link the voucher use and copayment in a single confirmation.

Rationale: Improves usability and reduces total notifications easing housekeeping.

6. When the voucher payment is confirmed by the purchaser, the system **shall** request approval from the merchant to approve use of the voucher as a payment source for the transaction.

Rationale: Informs the merchant that a voucher is being used. Merchant can accept or refuse for any reason. Merchant should ensure the voucher is being used for eligible goods.

7. If the merchant does not approve the voucher's use, the payment request **shall** be canceled and no funds will be transferred.

Rationale: No value is lost if the voucher is not used. However, it may be better to require acceptance if the merchant is an authorized recipient. This would be based on agreements between the merchant and voucher issuer, or driven by regulation.

8. If the merchant approves the voucher's use, the payment **shall** complete and the designated value will be deducted from the accounts (i.e., voucher and stored value account).

Rationale: Necessary to ensure the integrity of the payments ecosystem.

9. The system **shall** notify the participants (e.g., merchant, purchaser and voucher issuer), indicating the status (complete or canceled) of the payment transaction, and indicate the total amount of the transaction and the amounts provided by each participating account. For example, "Total charge 50: 30 paid by voucher and 20 paid by e-money."

Rationale: Notification confirms payment, concluding the process and assuring the merchant that goods can be released to the purchaser.

4.10.3.5 Voucher Payment (Issuer to Merchant)

1. When the purchaser copayment in processed, the system **shall** generate a request to the voucher issuer for payment to the identified merchant on behalf of the voucher recipient.

Rationale: The voucher has no actual value. The model uses push payments only, so the system must request payment from the voucher issuer when the voucher is redeemed in a purchase transaction.

2. The request for payment **shall** provide the voucher identifier, purchaser identifier, merchant identifier, reimbursement amount requested, total amount of purchase, copayment amount by purchaser, copayment type (e.g., e-money, cash), merchant location identifier (may be combined with merchant identifier, depending upon implementation), and date and time (and potentially geo-tagged location) of the transaction.

Rationale: This information is needed to accurately track and validate usage of the voucher.

3. The expectation is that the voucher management system **will** confirm eligibility in the context of the purchase transaction and automatically approve the payment request, causing payment funds to be transferred.

Rationale: Manual intervention would be slower, but effective. In either case, the merchant requires confirmation of voucher payment before goods will be released. Automation ensures expediency of the redemption process.

Note: Care must be taken on implementation to prevent fraudulent redemption messages being created or injected into the system, directing payment to an unauthorized third party. The voucher management function authorizes the actual voucher redemption payment, so the expectation is that it will include the necessary validation controls to prevent payment for non-compliant or fraudulent transactions.

4.10.3.6 Voucher Statement

1. The mobile wallet **shall** provide a listing of available vouchers, including their value and expiration date (if applicable) on request of the mobile wallet holder.

Rationale: The listing provides the recipient with a means to track vouchers and plan how the value might be utilized.

2. The mobile wallet **shall** require the user to enter a valid PIN before displaying the voucher list.

Rationale: The PIN provides an additional level of confidentiality, allowing the payee to reduce awareness of the available value.

3. A voucher **shall** be considered available if the following conditions are met:

a. The voucher has a positive, non-zero value.

b. The voucher has not reached the defined expiration date.

c. If the voucher is part of a batch, the batch available value is positive. For clarity, vouchers may be oversubscribed with the value available on a first come first served basis.

d. The voucher has not been canceled by the issuer.

Rationale: This is a definition of availability.

4. If no vouchers are available, the mobile wallet **shall** positively state that case.

Rationale: This helps avoid confusion on the part of the user. For example, "Sorry, no vouchers are available."

4.11 DEPOSIT CASH (CASH IN)

4.11.1 Description

Value must be associated with the mobile wallet before a payment can be made. Common methods of converting cash to e-money include:

- Deposit cash with an agent of the DFSP.
- Deposit cash at an ATM for credit to the mobile wallet. This is essentially the same as an agent transaction; the registered agent is an ATM instead of a human.
- Purchase a scratch card at a retail location and register the card with the mobile wallet.
- Transfer funds from another value source (e.g., bank account or card).
- Receive a payment from a third party.

In our pro-poor model, the system is primarily designed for push value transfer. As a result, the mobile device cannot initiate (pull) an inbound transfer, but either accepts funds transfer automatically or responds to a transfer when some acceptance action is required. Thus, any inbound transfer is essentially a payment ***to*** the wallet holder. In either case, the value of the wallet account receiving the funds is increased and the user is notified of the transfer.

In the developed world, pull payments are more common, and would provide for initiating the transfer ***from*** the mobile wallet by a third party. This use case is outside the scope of this document.

4.11.2 Rationale

The pro-poor model is designed to reduce costs by reducing risk. Push payments are inherently less risky than pull payments, as the control of funds resides with the sender. By focusing on push transfer, the complex mechanisms, processes, and ultimate risk transfer can largely be eliminated.

4.11.3 Requirements

4.11.3.1 Enabling Receipt of Funds

There may be situations where it is a benefit to the mobile wallet holder to limit the *inflow* of funds from various sources or channels (e.g., a scheme in which a fraudster deposits a small amount of money, claiming it's mistake and then "helping" the recipient return the money by using social engineering tricks to inflate the amount returned). Thus, providing control to the mobile wallet holder allows them to work within their risk concerns.

1. The mobile wallet **should** allow the user to selectively enable methods for receiving funds from the funds receipt methods available through the DFSP.

Rationale: The user may choose to limit available options to those they intend to use, reducing training requirements and simplifying use while also reducing opportunities for error.

2. By default, all available funds receipt methods **should** be enabled.

Rationale: Automatically enabling the transfer mechanisms improves ease of use and reduces training requirements for the end user.

4.11.3.2 Notification

1. The user **shall** be notified when funds have been transferred to the mobile wallet.

Rationale: Notification improves awareness.

2. The notification of funds transfer **should** include sender name, sender ID, amount transferred, and time and date of transaction completion.

Rationale: This data is needed to clearly identify the transfer.

3. The system **should** provide a mechanism that would allow the recipient to message the sender to respond to notification messages.

Rationale: Nice to have convenience.

4. The system **should** allow the user delete notification messages with or without review.

Rationale: Enables easier housekeeping if volume of messages is high.

4.12 WITHDRAW CASH (CASH OUT)

4.12.1 Description

The ubiquity and universal acceptance of cash necessitates that a successful mobile money solution minimizes barriers to moving value between digital money and cash, though the long-term goal is to keep money digital once converted from cash.

In developing countries, mobile money providers typically utilize agents to facilitate the conversion. The agent not only verifies that the recipient is authorized, but also confirms cash acceptance by the account holder. Alternatively, some ATM networks have been integrated into the local mobile money systems, allowing consumers that have a mobile money account but no bank account to use the ATM to convert from digital money to cash.

The following sections provide the requirements defining support for transferring value from a mobile wallet in the form of a *cash-out* transaction.

4.12.2 Rationale

Consumers may need cash to complete payment transactions where mobile money is not accepted, or they may simply desire to have the cash in hand. Regardless of the motivation, the mobile money solution must provide the ability to convert stored value to cash, or risk not being accepted in the marketplace.

Further, ATMs and agents might both achieve the same goal of dispensing cash, but each has unique benefits. For example, ATMs are potentially available 24 hours a day, every day of the year, but they require significant capital investment and are generally only deployed where the expected demand justifies the expense. By comparison, agents require little hardware or infrastructure, and can thus be deployed where ATMs are not feasible (e.g., remote locations without supporting required infrastructure).

4.12.3 Requirements

4.12.3.1 Withdraw Cash Using an Agent

The DFSP's agent provides the consumer account cash interface services needed to convert between cash and e-money (i.e., *cash in, cash out* or *CICO*).

The agent cash-out transaction can follow multiple scenarios:

- Customer-initiated: The customer initiates a mobile payment designating the registered agent ID as the payee. This is effectively the same as the basic person-to-person payment process, though the agent requires additional steps to verify the transfer of cash to the payee (e.g., the agent must enter their PIN to confirm the withdrawal, and require the consumer to sign a log book confirming cash was delivered).
- Agent-initiated, with consumer's mobile device: In an agent-initiated cash-out transaction, the consumer would express the details of the cash-out request to an authorized agent of the DFSP, providing their phone number or alternate ID and the amount requested. The agent would enforce any procedural rules (e.g., require the consumer to sign a log book) and then initiate the cash out request process using either a mobile device or the business's POS system. In turn, the system would send a pending request to the consumer for approval of the withdrawal. This is effectively the same as the standard request for payment process.
- Agent-initiated, with biometric authorization: The agent initiates the cash-out process, and the consumer authorizes payment through biometric authentication at the point of sale, without the use of their own mobile device.

General

1. The system **shall** allow an authorized recipient to withdraw cash through a DFSP's authorized agent.

Rationale: This is a primary capability of the agent role. As agents are portable and don't require significant hardware or technology investment, they are likely to be more available in remote locations, or where there is demand for their services.

2. The system **shall** allow the consumer account holder to initiate the cash-out transaction from the consumer mobile wallet.

Rationale: This is a core function of the mobile wallet. Initiation by the account holder is in alignment with the push-payment design principle, keeping control with the account holder.

3. The system **shall** allow the authorized agent to initiate the cash-out transaction from the agent mobile wallet, mobile app, Web interface, or other available purpose-built system.

Rationale: Consumer account holders may not have a phone, their phone may be inoperable, or it may simply be unavailable. Allowing the agent to act on behalf of the account holder allows them to provide a valuable service.

4. The agent and consumer account holder **may** perform their required activities for the cash-out transaction on independent devices or entirely on the agent system or device.

Rationale: The account holder may not always have a phone, so agent's system must be able to complete cash-out transactions.

5. The system **shall** require the account holder to either present verified biometric measurements linked to the account or enter their PIN on an authorized endpoint device (e.g., consumer phone, agent's phone, agent's POS system) to authorize the cash-out transaction.

Rationale: These two methods are acceptable to confirm authority for the transaction. Ensures positive approval by the payer and supports non-repudiation.

6. The system **shall** permit the account holder to cash out the lesser of available account funds or other limits as defined by system rules or regulation (e.g., tiered KYC).

Rationale: Ensures the cash-out transaction doesn't create the potential for financial loss to the system, and that the transaction is compliant with regulation/law.

7. The system **shall** notify the account holder when a cash-out transaction is performed.

Rationale: Notification provides confirmation of the transaction success and awareness in the event the transaction was not initiated by the account holder.

8. The cash-out notification to the account holder **shall** include the agent ID, date/time, amount, authorization method, and any fee amount.

Rationale: This is the minimum data needed to understand the transaction from a historical perspective.

9. The system **shall** track the amount withdrawn separately from the fee charged by the agent as a consumer protection measure.

Rationale: This helps the DFSP monitor the agent network.

Biometric-related

10. If the consumer has linked a biometric profile to their mobile wallet, biometric verification **shall** be accepted for authorization of account transactions, in lieu of the wallet holder's mobile device.

Rationale: Biometric verification provides out-of-band authorization for the transaction, and ensures that the authenticating individual is the same person that performed the biometric enrollment. This method is at least as valid as physical control of a mobile device. Further, some wallet holders may not have a phone to use for authorization, so biometric methods are necessary.

11. Biometric authorization **may** be limited to proximity-based payments.

Rationale: The ecosystem infrastructure or participants may not have the equipment or messaging support to leverage biometric authorization for initiation of the payment.

Third-Party Cash Disbursement

12. The system **shall** enable the account holder to initiate a remote agent cash-out transaction enabling a third party to physically receive the cash upon presentation of an authorization from the account holder.

Rationale: This is a hybrid capability, similar to a P2P transaction followed by the recipient performing a cash-out transaction. The difference is that the recipient does not need to be a mobile money user, but only to provide the authorization and to meet the identification demands of law, regulation, or business rules.

Humanitarian Rationale: Humanitarian assistance is sometimes directed to beneficiaries that need assistance to access their funds. Third-party disbursements therefore offer flexibility and allow recipients to access cash even though they face obstacles in performing the transaction on their own.

13. The system should provide the ability for the account holder to generate a release authorization code that substitutes for authorization of a cash-out transaction.

Rationale: Enables a remote third party to present the code and receive the funds. This may be prohibited by regulation, or undesirable from the perspective of the DFSP, depending upon fee structure.

4.12.3.2 Withdraw Cash at an ATM

This use case is similar to an agent-assisted withdrawal, as the ATM would have a unique virtual agent identifier within the payment ecosystem. It is slightly different as there is no physical person to confirm the recipient's identity, or to verify and log the authorization.

In a typical scenario, the payer would generate a cash-out authorization code from their mobile wallet account using their mobile device. This code could be enabled for a single, predetermined ATM, or any participating ATM in the ecosystem, but it effectively authorizes a payment of a specified amount to the ATM's virtual agent account, inclusive of any fees. After generating the cash-out authorization code, the payer would enter the code and their associated phone or alternate ID at the authorized ATM, which would then dispense the predetermined amount of cash.

Alternatively, the payer could request a cash-out at the ATM by entering the phone number and amount to withdraw.

The details are the same as the generic merchant purchase solicited payment use case.

1. The system **shall** enable account holders to withdraw cash at a participating ATM.

Rationale: Where available, ATMs are potentially accessible 24x7x365, providing around-the-clock access to cash.

2. ATMs **must** be registered with the system to participate in the mobile money ecosystem and provide services to the mobile wallet holder.

Rationale: An ATM is effectively a virtual agent of the DFSP, providing services, such as cash-out, that can be facilitated without a physical person.

3. The system **should** support ATM cash-out transactions initiated at the mobile device **or** at the ATM.

Rationale: Provides greatest opportunity to leverage ATMs to support remote or proximate cash-out.

4. If ATM-initiated cash-out transactions are supported, the system **shall** permit the mobile wallet account holder to enable or disable ATM initiated withdrawals.

Rationale: Fraudsters may send unwanted payment requests from an ATM. Allowing the user to disable this capability allows the wallet holder to avoid fraudulent messages through this channel.

5. If ATM initiated cash-out transactions are supported, the system **shall** disable ATM-initiated withdrawals by default, requiring the mobile wallet holder to opt-in to activate the capability.

Rationale: An ATM-initiated cash-out transaction is vulnerable to fraud, as it does not require the mobile wallet holder to initiate the transaction. Thus, the person whose funds are at risk should have control over whether to accept or reject the risk.

6. **If** the ATM cash-out transaction is ATM-initiated:

> a. The user **shall** provide the payer's mobile wallet account identifier and the amount requested.
>
> *Rationale: This is the minimum data required to send a payment request. The account identifier might be a phone number, mobile wallet account ID, or some alternate ID, depending on the mobile wallet implementation.*

b. The system **shall** send a payment request to the mobile wallet, indicating the amount requested, the ATM address, and the ATM identifier.

Rationale: A request must be sent to notify the payer of a need for action, though the assumption is that, for a legitimate transaction, the payer is aware of the cash-out process and prepared to take action.

c. The system **shall** require that the payer approves the payment request by entering their account PIN at the mobile wallet user interface.

Rationale: Ensures positive approval by the payer, and supports non-repudiation.

d. The system **shall** escrow the amount requested upon payment authorization.

Rationale: The funds need to be sequestered from the time of authorization until the transaction completes to avoid cash losses due to processing timing or reliability issues.

e. The ATM **shall** attempt to dispense the authorized amount of cash and respond to the payer, indicating full success, partial success, or failure of the cash-out, as well as the amount dispensed.

Rationale: Status is needed to finalize the transaction, and ensure funds are not tied up unnecessarily due to ATM issues.

f. The system **shall** cancel an incomplete ATM cash-out transaction if not completed within a participant-agreed timeframe from initial payment request. (60 seconds is recommended)

Rationale: The payer needs time to authorize the transaction, but the intent is to keep the timeframe short to avoid tying up the ATM. The timing must be from the time of request to ensure a transaction does not sit waiting for payer approval.

g. The system **must** immediately return any undisbursed escrowed funds to the source mobile wallet account if the transaction completes without disbursing the entire amount. (This might include notification by the ATM of or no partial disbursement, notification by the ATM of failure, or cancellation of the transaction due to time-out prior to distribution.)

Rationale: If it can be determined that money was not dispensed, the mobile wallet holder should not be unreasonably denied use of their funds.

h. If the payer rejects the payment request, the transaction **will** be canceled.

Rationale: This is a natural end state for the transaction.

7. **If** the ATM cash-out transaction is initiated from the mobile wallet:

a. To dispense cash, the ATM **shall** require the user to provide a valid cash-out authorization code and either the payer's associated mobile phone number, alternate ID, or biometric ID.

*Rationale: The ATM withdrawal is slightly different from a physical agent cash-out, as there is no person to request identification or log disbursement of the money. The technology of the ATM provides the disbursement logging, but the actual money may be received by the account holder, or any third party with authorization information and knowledge of the payer's account. Requiring both a unique code for the transaction and account information reduces the likelihood of unauthorized use. Note, however, that **there is no specific authentication of the recipient**.*

b. The system **shall** enable the account holder or registered agent to generate a unique, single-use cash-out authorization code from a permitted endpoint device (e.g., mobile device, agent's POS system).

Rationale: The cash-out authorization code is critical to enabling remote cash disbursement at an ATM, but to reduce the risk of fraud, it should only be created from a controlled endpoint.

c. The system **should** allow the cash-out authorization code to be designated as valid at either a single pre-identified ATM **or** any participating ATM.

Rationale: Allowing the authorization code to be tied to a specific ATM gives tighter control to the payer, helping prevent fraud. Permitting any participating ATM provides greater flexibility to the user.

d. The cash-out authentication code **shall** be valid until use, retraction, or expiration.

Rationale: These are the appropriate end states for the authorization.

e. The system **shall** escrow the authorized cash-out amount upon generation of the cash-out authorization code.

Rationale: The funds need to be sequestered from the time of authorization until the transaction completes, to avoid cash losses due to processing timing or reliability issues.

f. The system **should** allow the user to define the time at which the cash-out authorization code becomes active for use and the duration of its validity (i.e., set the start date/time and number of minutes from start time that the code will expire).

Rationale: Provides flexibility to schedule remote pickup of the funds, enabling greater utility if the payer is willing to have the funds tied up for an extended period of time.

g. The system **should** limit the duration of validity. 10 minutes is recommended.

Rationale: The longer the code is usable, the greater the risk of use by an unintended party. Also, ensuring expiration prevents a large number of unused authorization codes from building up in the system with associated funds in escrow.

h. By default, the authorization code **should** be active for use for a fixed duration (10 minutes is recommended) from the time of creation.

Rationale: Setting a default ensures expiration without the action of the payer.

i. The system **shall** limit the future activation date and time. (Recommendation is 48 hours from time of creation.)

Rationale: Some maximum delay to activation is needed to ensure funds are not tied up for a long period of time and that pending codes do not unnecessarily build up in the system.

j. The system **shall** not permit a cash-out authorization code to be generated for an amount exceeding the funds available in the source account.

Rationale: System integrity requires only good funds can be authorized for withdrawal, as there is no recovery mechanism once funds are disbursed.

k. The user **shall** be able to cancel any cash-out authorization code prior to its use or expiration.

Rationale: Cancelation allows the payer to have full control, and potentially retract an authorization made in error.

4.13 ENFORCE ACCOUNT LIMITS

Note: This section is replicated from the IST requirements document with modification to support implementation at the DFSP.

4.13.1 Description

The regulatory climate and risk tolerance of system participants can vary widely by country or region. However, all stakeholders want to ensure that losses and fraud are minimized, and that the payment system does not provide a vehicle for money laundering, terrorist financing, or other criminal behavior.

To achieve these goals across the financial infrastructure, regulators and operators have defined k*now your customer (KYC)* rules that providers **must** follow to assure the identity of a potential or current account holder, and subsequently enforce appropriate controls on the value and capability of the account.

The ability to identify the account holder, a key component of KYC, poses significant challenges in developing countries where many people lack formal identification, and must rely on other means to establish their identity (e.g., someone who is known, such as a village leader, must vouch for their identity). This can be a barrier to joining formal financial systems, resulting in large numbers of unbanked individuals.

Several countries have enabled *tiered KYC* to encourage participation by the unbanked. With tiered KYC, providers tie account parameters to the evaluated risk level of the account owner, designating controls needed for each risk level. In general, the lower the evaluated risk, the greater the potential value or the broader the capabilities of the account.

Common controls include limiting the maximum account balance, or the value and quantity of transactions that an account holder may perform over varying timeframes (e.g., daily, weekly, single transaction). In practice, account balance limits would likely be imposed at the DFSP or bank level, with the switch potentially routing threshold violation or warning messages from the DFSP or bank.

To ensure flexibility to manage risk in the many transaction scenarios, the controls limits may vary depending upon:

- Type of activity being performed (retail purchase, funds transfer, account opening, etc.)
- Type of participants involved (government-to-person, person-to-person, agent-to-person, etc.)
- Level of validation of the participant’s identity (minimal, vouched for by trusted person, validated with national ID, etc.)

In providing financial services to poor people, *micro-tiers* are an attractive option for the undocumented to open basic accounts for electronic payments. Because these micro-tier accounts have very low maximum balances and transfer limits, the risk to the system and its participants is controlled. Tiered KYC systems (and the regulatory policies that enable them) are more inclusive and thus pro-poor.

4.13.2 Rationale

The regulatory and risk management rules are likely to be complex and are sure to change over time. The system will not scale unless rules can be created and uniformly applied to address common scenarios.

4.13.3 Requirements

1. The IST **shall** provide a capability to enforce account and transaction limits, referred to as *transaction and account control rule*s (TACRs) herein, to support fraud and risk management strategies. For example, accounts may have varying limits depending upon KYC rules.

Rationale: For the system to scale and provide consistent results, regulators and good business practice require the tools to mitigate risk.

2. The DFSP **shall** provide the ability to limit the **maximum value** (i.e., dollar amount) of **any transaction instance by transaction type**.

Rationale: The impact of a specific risk is limited based on the amount of money involved.

3. The DFSP **shall** provide the ability to limit the **frequency** (i.e., count per timeframe—hourly, daily, weekly, monthly, etc.) at which **any transaction type** (e.g., cash withdrawal) may be performed.

Rationale: Risk factors include how often certain activities or behaviors occur.

4. The DFSP **shall** provide the ability to limit the **aggregate maximum value** of transactions over a specified timeframe (frequency) **grouped by transaction type.**

Rationale: Risk varies by transaction type and thus the need for the ability to limit how much may be transacted within a certain grouping. For example, it is much less risky to transfer $10,000 between accounts than to send $10,000 in payments to a third party.

5. The DFSP **shall** provide the ability to limit the **maximum value** of **any account** (i.e., account balance).

Rationale: Specific financial accounts may be limited in value based on numerous risk criteria.

6. The DFSP **shall** provide the ability to create and manage groups of TACRs.

Rationale: When TACRs are grouped to enforce regulatory requirements for KYC by level, the configuration effectively provides tiers.

Humanitarian Response Rationale: Speed is critical in a crisis. A DFSP may pre-arrange acceptable TACRs with a local regulator based on relaxed KYC regulations and pre-configure them to be rapidly deployed.✚

7. The DFSP **shall** enable groups of TACRs to be enforced on individual accounts.

Rationale: Individuals may have many accounts with different control structures. Grouping is needed to efficiently apply sets of rules to a type of account. ***Supports the concept of KYC tiers****.*

8. The DFSP should either:

a. Reject any transaction that violates an enforced TACR and notify stakeholders (originator, receiver, system administrator and potentially regulators and law enforcement) of the specific reason the transaction was rejected, **or**

Rationale: Rejecting the transaction keeps the overall system simple, as opposed to creating some resolution process. Notification gives the stakeholders the opportunity to coordinate and address the issue.

b. Complete the transaction as normal, but suspend the account after processing and notify stakeholders (originator, receiver, system administrator and—potentially—regulators and law enforcement) of the specific reason the transaction triggered account suspension.

Rationale: Some risk or fraud reviews might require more time to perform. Thus, allowing the transaction to complete avoids overall transaction processing impacts while preventing future violation. This acknowledges that the transactions are generally low in value and do not pose a systemic risk to the payments system, and thus some level of loss may be acceptable.

Note: Regulation would likely drive the decision between the above processing models.

9. The DFSP **shall** provide the ability to apply TACRs based on the **roles or accounts** participating in a transaction.

Rationale: Different rules will be needed for the same type of transaction depending upon who is participating. This would potentially enable a government payment to be accepted, even if the account maximum balance is exceeded.

10. The DFSP **shall** provide the ability to apply TACRs based on the **direction** of funds transfer (if any).

Rationale: Different rules will be needed depending upon the characteristics of the sender and recipient.

11. The DFSP **shall** allow individual TACRs to be assigned a processing priority.

Rationale: Enables hierarchical rules processing.

12. When two rules are in conflict, the TACR with the higher priority **shall** apply, and the TACR with lower priority **will** be ignored.

Rationale: A mechanism is needed to address situations where the rules are in conflict.

13. The system **should** notify the users when the TACRs have been changed.

Rationale: Users should be notified when new account limits are deployed.

Humanitarian Response Rationale: New, temporary account limits (e.g. daily maximum in number of transactions) may be deployed in a crisis. Users should be notified in order to build awareness and trust.✚

4.14 REPORTING AND DASHBOARDS

4.14.1 Description

Any complex system needs to provide data describing the activities of the system so that analysis can be performed. Reporting capabilities can vary in complexity from interactive, drillable reporting interfaces to a simple text based message. Reporting capabilities can be embedded in the system, or (for more sophisticated needs) provided by an integrated third-party solution. Regardless of the implementation, the system must be capable of exposing the data necessary to meet the reporting expectations of users, regulators and law enforcement agencies while ensuring consumer data privacy standards are met. With financial systems, that level of data access is expected to be very detailed to enable evaluation of system health, dispute resolution, user activity monitoring, liquidity and cash position, etc.

4.14.2 Rationale

Without some reporting capability, the system's stakeholders would lack information to support business processes that rely on the IST, including but not limited to performing risk management, evaluating system health, evaluating expenses of the system, and investigating disputes.

4.14.3 Requirements

Centralized Reporting

1. The DFSP **should** have robust information systems that provide accurate current and historical data. Data should be provided in a timely manner and in a format that permits it to be easily analyzed.[13]

Rationale: This is a basic capability needed to support business processes.

2. The DFSP **shall** expose transaction detail for reporting to authorized users.

Rationale: This is a basic capability needed to support business processes.

3. The DFSP **should** provide a reporting interface for authorized internal users.

Rationale: The prototype includes some basic reporting capability.

4. The DFSP **should** provide pre-configured ("canned") reports for common business process needs, including:

a. Transaction type reports

b. Revenue reports

c. Cash and float demand reports

Rationale: Provides efficiency by building once and using many times.

5. The DFSP **shall** provide a search interface enabling authorized users to view historical data.

Rationale: This is a common mechanism to provide efficient selection of desired historical info.

6. The DFSP **shall** provide the ability to limit the search scope by date/time, transaction type, involved accounts, specific users, amount and location.

Rationale: Simple filters are required to selectively retrieve data.

7. For basic reporting, the DFSP **should** provide a paged view of the response data from a report request.

Rationale: Provides more control of data handling for presentation or load control.

8. For basic reporting, the DFSP **should** allow the user to export the data in XML, CSV, PDF and Excel formats.

Rationale: Users will want to consume the data in a variety of formats.

9. The DFSP **should** provide access control to the lowest unit of data stored (i.e., the field).

Rationale: Common reporting mechanisms access the storage layer. However, not every field within a data store has the same level of sensitivity or access requirement. Thus, providing access control at the lowest level provides the greatest flexibility.

10. The DFSP **shall** be able to report the user-level data in a de-identified way.

Rationale: Helps protect the identities of the users.

11. The DFSP **may** provide a configurable reporting interface allowing an administrator to customize the reports to fit their specific reporting requirements.

[13] (International Settlements and International Organization of Securities Commissions, 2012)

Rationale: Enables more useful reporting than pre-canned reports.

Mobile Wallet Reporting

12. The mobile wallet **should** enable the wallet holder to designate a historical transaction as a favorite.

Rationale: Allowing the account holder to recall designated prior transactions enables easy reauthorization without the need for rekeying.

13. The mobile wallet **should** retain a list of up to 10 favorite transactions for recall by the account holder.

Rationale: Allowing the account holder to recall designated prior transactions enables easy reauthorization without the need for rekeying.

14. The mobile wallet **should** allow the account holder to automatically repeat a favorite transaction.

Rationale: Reduces likelihood of user keying error by automatically populating the payment detail.

15. The mobile wallet **shall** require the user to enter their PIN in order to repeat a favorite transaction.

Rationale: The user must always provide authorization at the time a payment is executed.

5.0 Non-Functional Requirements (NFR)

This section contains non-functional requirements not included in previous sections.[14]

5.1 PERFORMANCE

The performance constraints specify the timing characteristics of the software. Certain tasks or features are more time-sensitive than others; the non-functional requirements **should** identify those software functions that have constraints on their performance.

- Response times: application loading, screen open and refresh times, etc.
- Processing times: functions, calculations, imports, exports
- Query and reporting times: initial loads and subsequent loads

1. At a minimum, the system **must** be able to complete 1,000 message transactions per second.

Rationale: This number may adjust based on the demand for processing services in a specific region, but as stated provides for robust transaction processing throughput, based on field observation of mobile money systems in Africa.

2. The system **must** sustain an average message processing time of no more than 1 second over any 60-minute period.

Rationale: One second for processing is reasonably attainable and should allow for the entire payment transaction process to complete in a timeframe (e.g., 6 seconds) that does not unnecessarily slow the transaction at the point of interaction between the parties.

3. The maximum processing time for any message **should not** exceed 200% of the average processing time.

Rationale: A threshold needs to be established for overall evaluation of processing health. This value was provided as a percentage of the average processing time instead of a fixed maximum, to indicate that, if processing takes twice as long as normal, impact on the overall system and end user should be reviewed.

4. Server response time for rendering the user interface **should** be no more than 1 second.

Rationale: Good design practice to ensure server-side work does not consume too much of the overall response time perceived by the end user, making sure that time is available for transmission to and presentation of the end-user web interface.

5. For IP access:

- Average user interface load time **should** be no more than 3 seconds.
- Maximum user interface load time **should** be no more than 6 seconds.

Rationale: Sets a reasonable response time from a user perspective. Anything longer would be considered poor performance from the end-user's perspective, and would likely reduce adoption.

6. The mobile wallet **shall** support continuation of transaction processes in the event that the transaction is interrupted by a connection loss (e.g., USSD gateway session time-out).

For USSD access on the local carrier network:

- From the mobile device, the average delay from calling a service to displaying the first page of the application **shall** take no more than 6 seconds.

[14] Descriptions of the non-functional requirements categories are adapted from *Applied Software Project Management*, Andrew Stellman and Jennifer Greene, O'Reilly Media, 2006

- From the mobile device, subsequent pages **shall** have an average delay of no more than 1.5 seconds.

Rationale: Sets a reasonable response time from a user perspective.

7. The system **shall** be able to configure the length of time for session time out.

Rationale: Provides system flexibility on local network constraints.

Humanitarian Response Rationale: The session time out may need to be adjusted upward because there is likely to be increased system load in a crisis.✚

8. If, for any reason, performance is compromised, the system **must not** allow improper transactions. Depending upon the level of performance degradation, a "system unavailable" message or transaction queuing/prioritization scheme must be in place, to either reduce the volume of transactions to be processed (by stopping the inflow) or manage transactions as gracefully as possible given the volume or state of the system.

Rationale: Individual user performance is not a higher priority than overall system performance. Good design practice requires a fallback process in times of unexpected system load.

5.2 SECURITY

Confidentiality and integrity requirements define the security attributes of the system, restricting access to features or data to certain users and protecting the privacy of data entered into the software. Items to consider include:

- Fault trapping (I/O): how to handle electronic interface failures, etc.
- Bad data trapping: data imports, flag-and-continue or stop the import policies, etc.
- Data integrity: referential integrity in database tables and interfaces
- Image compression and decompression standards
- Login requirements: access levels, CRUD levels
- Password requirements: length, special characters, expiry, recycling policies
- Inactivity time-outs: durations, actions
- Encryption of data, at rest and in transit
- Physical security: hardware, internal network nodes, and employee terminals should be secured in accordance with banking/financial services industry standards

5.2.1 Network Integrity

1. The MNO **should** provide network integrity security, monitoring for duplicate SIMs and proactively block access when a duplicate SIM can be confirmed. Activity/usage patterns may provide mechanism for identification.

2. The MNO **should** fingerprint the mobile device to enable cloning detection.

3. The DFSP **should** reject or block abnormal payment origination (i.e., behavior is inconsistent with prior use).

4. The DFSP **should** support escalation of cloned SIM fraud to the MNO.

5.2.2 Data Integrity

1. The system **must** meet PA-DSS security standards.

Rationale: Industry standard.

2. The system **must** ensure only authorized users can create/read/update/delete protected data.

Rationale: Data integrity cannot be achieved if anyone can alter the information.

3. The system **shall** validate all user inputs to fields within forms.

Rationale: Prevents "garbage in," and controls the potential for system compromise through methods like SQL injection.

4. The system **must** ensure minimum required data elements are provided before creating a record.

Rationale: If a specific amount of information is needed to uniquely identify, correlate, or utilize a record, creating a record without that data simply takes up space and adds to system load and maintenance without benefit.

5. The system **should** enforce referential integrity constraints on dependent data elements where the data has no relevance out of context of the reference.

Rationale: If the data has no value out of context then the context must be associated.

6. If compression is used to reduce the size of data in motion or at rest, the system **must** only use lossless compression mechanisms.

Rationale: Prevents data loss.

7. The system **must** provide the ability to track changes to any stored value.

Rationale: If the change cannot be tracked there is no ability to detect the change after the fact or determine potential impact.

5.2.3 Authentication

This section describes authentication requirements for system level users.

1. The system **must** allow every individual user to have a unique user account with independent authentication credentials.

Rationale: Separate accounts enable accountability for use of the account and limit exposure of assigned privileges to the intended party.

2. The system **may** support complex passwords consisting of at least 20 printable characters, including combinations of numbers, letters, symbols, and punctuation.

Rationale: Brute force password cracking capabilities are driving the need for longer passwords.

3. When a new account is created, the system **shall** automatically generate a random, unique password that meets administrator-defined complexity requirements

Rationale: It is poor security practice to use a standard initial password when new accounts are set up. Better to auto-generate and communicate a random password to avoid unauthorized use of new accounts.

4. The system **shall** require that the user change the password on first login after authenticating with the automatically generated initial password.

Rationale: Ensures only the user knows their daily use password, as they would set it at the time they take control of the account.

5. The system **shall** support federation with external authentication providers.

Rationale: Reduces the number of individual passwords users would need to know and remember in an enterprise.

6. The system **shall** automatically lock out an account after an administrator-defined number of consecutive failed login attempts over a given period of time. Consider a maximum of 5 attempts over 10 minutes.

Rationale: Prevents brute-force password cracking through the login interface.

7. The system **shall** support multifactor user authentication mechanisms.

Rationale: As computing power increases, passwords must become increasingly longer and more complex to avoid brute-force cracking. Adding a second factor of authentication can increase the time and processing needed to circumvent account authentication controls.

8. The system **should** require the multifactor authentication for any account with administrator privileges.

Rationale: Administrators and other privileged users have significant authority that can cause significant loss or outage is misused. Requiring multifactor authentication greatly improves the control over privileged accounts and can significantly increase the effort required to gain unauthorized access.

9. The system **shall** provide the ability to log all login attempts such that forensic analysis can identify the originating endpoint IP address, user ID, date and time, browser model and version utilized, and machine operating system and version utilized.

Rationale: This information is necessary to determine how and by whom a system was accessed.

10. All internal and external communications between systems, partners, and user endpoints **shall** be encrypted.

Rationale: Good security practice to prevent exposure of confidential information during transmission.

11. Mobile device users **must** authenticate to access the service.

- Mobile device users **must** provide a PIN to access the service via USSD.
- At a minimum, mobile application users **must** provide username/password or similar key/value pair authentication tokens.
- Digital certificate–based authentication (i.e., PKI) **should** be utilized when possible, to authenticate to the service from an appropriately provisioned mobile device.

Rationale: Good security practice to prevent account misuse in a variety of deployments.

5.3 USABILITY

Usability relates to how easily users can learn to use a system and how efficiently they use it. Highly usable systems reduce the effort required to read or input data and prevent users errors, in turn in increasing operational efficiency. Items to consider include:

- Look and feel standards: screen element density, layout and flow, colors, UI metaphors, keyboard shortcuts
- Internationalization/localization requirements: languages, spellings, keyboards, paper sizes, etc.
- Understandability
- Learnability
- Operability
- Attractiveness
- Usability compliance

1. The user interface **must** be provided in the predominant language of the target market.

Rationale: Using the predominant language reduces training required, and makes the system available to a larger user population.

2. The user interface **should** support language localization, to advance adoption by reducing language barriers in the target market.

Rationale: Localization enables broader adoption with less redesign, and allows better scalability and faster deployment in new markets.

3. The user interface **should** maintain a consistent look and feel within the context of any role.

Rationale: Consistency reduces training requirements and increases adoption.

4. The system **may** support simultaneous use of multiple currencies within a single system instance.

Rationale: Improves portability to other environments without redesign.

Humanitarian Response Rationale: The need to handle multiple currencies may result in a crisis from increased cross-border migration (from refugees or IDPs) as well as a surge in international remittances as aid.✚

5. The system **must** support the primary national currency of the target market.

Rationale: Users would expect to use the local currency and not be expected to convert to an alternate currency. Failure to support the local currency would reduce acceptance of the solution in the marketplace.

6. The user **must** be able to return to the home screen directly from any primary (i.e., not pop-up) system screen/window.

Rationale: Generally accepted good design practice.

7. The system **should** provide a spell-checking function for text entry fields where feasible.

Rationale: Improves data quality.

8. The system **may** allow users to assign keyboard shortcuts to initiate common functions or activities.

Rationale: Improves efficiency of administrative interfaces.

9. The system **should** provide context-sensitive help on each user screen where feasible.

Rationale: Reduces training with improved usability. Enables effective self-service user training.

10. The system **should** minimize full screen redraw when updating information on the user interface.

Rationale: Reduces data transmission load.

11. The system **should** utilize icons and graphics in the user interface where appropriate and possible.

Rationale: Supports low-literacy users.

USSD Interface

12. The USSD session should automatically terminate when a predetermined time has elapsed without user response (i.e., time-out).

Rationale: Frees up network resources and controls expense of communications.

13. Menu selection/predefined answers: When the user selects menu items or predefined answers, the USSD user interface **should** provide implicit feedback in the menu title or in the following step.

Rationale: Reduces user confusion with system interactions requiring multiple steps.

14. Critical transactions: The USSD user interface **should** provide explicit confirmation when performing a critical task (e.g., the user needs absolute certainty that the amount of money to be transferred or other critical data is correct).[15]

Rationale: Builds trust in the system.

15. Accumulation Confirmation: If sequential steps are necessary to complete one transaction, all collected data **may** be presented at the end of the sequence for confirmation. To be efficient, however, all data should fit onto one page.[16]

Rationale: Improves overall usability and builds trust in the system, as the user can see full context collected over multiple steps.

16. Global commands: Besides the start page, any menu **should** contain a link to start over (e.g., provide *Home* option)

Rationale: General good design practice related to usability.

17. Standard navigation: The interface **shall** provide the option to return to the previous menu (e.g., provide a *Back* option)

Rationale: Allows a user that selects the wrong path to back up, without requiring them to disconnect from the service and start over.

[15] Usability & Best Practice Guide for the Text Channel, Voice Objects, October 2007, http://developers.voiceobjects.com/files/WP-Best-Practice-Guide-Text-Channel.pdf

[16] ibid.

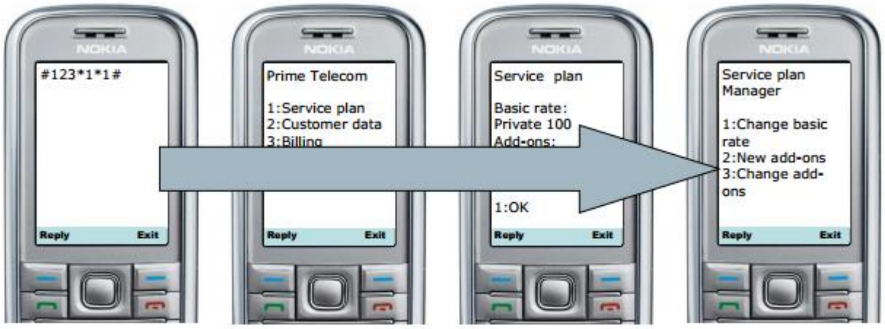
18. USSD list items **should** be numbered to indicate selection choice.

Rationale: Improves usability.

19. USSD lists **should** include navigation options (e.g., *Previous*, *Next*) to move backward and forward through the list, where appropriate (i.e., don't include *Previous* option at start of list, or *Next* at the end of a list).

Rationale: Provides common structure for list presentation.

20. The USSD interface **shall** support keyboard shortcuts for common tasks as an alternative to menu navigation. In the example below, dialing *#123*1*1#* would directly activate the corresponding service on the second menu level.



Short-cut dialing

Rationale: Improves usability, especially on older devices.

5.4 RELIABILITY

A set of attributes that bear on the capability of software to maintain its level of performance under stated conditions for a stated period of time. Items to consider include:

- Mean time between failures (MTBF): What is the acceptable threshold for downtime (e.g., one a year, 4,000 hours)?
- Mean time to recovery (MTTR): If broken, how much time is available to get the system back up again?
- Maturity
- Fault tolerance
- Recoverability
- Reliability compliance

1. The DFSP **must** have a minimum 99.95% availability (5.04 minutes of downtime per week), excluding appropriate scheduled and communicated maintenance windows.

Rationale: Anything less would reduce trust to a point that user acceptance may suffer as cash would become a required backup.

2. The DFSP interface **must** be have a maximum recovery time of 30 minutes.

Rationale: Payment networks must be readily accessible, and any sustained outage could cause substantial disruption to users and potential decline in acceptance of the system for regular use.

3. The DFSP supporting infrastructure **must** have no single point of failure.

Rationale: Improves system resiliency, leading to higher availability.

4. When a failure occurs, the DFSP **must** be able to isolate the failure to the offending component.

Rationale: Effective problem isolation improves recoverability.

5. Faulted transactions **must** not be propagated to other partners.

Rationale: Isolating failures reduces downstream impacts and improves the overall system usability.

6. DFSP transaction processes **must** *fail safe* without impacting the processing of other transactions (i.e., a faulting transaction would not consume all system resources with runaway processing).

Rationale: Isolating a transaction process minimizes the overall impact to the system as a whole.

7. The DFSP implementation **should** utilize path and switch diverse redundant telecommunications components.[17]

Rationale: Common expectation for critical systems, to reduce connectivity loss due to a single piece of equipment or line cut.

8. The system **shall** support message retry for non-financial transaction messages when an intermittent error condition is identified.

Rationale: Automated retry improves system recovery times and overall message throughput.

9. The system **shall not** retry delivery of a financial transaction message if duplicate message detection cannot be performed.

Rationale: Without a check for duplicate messages, automatic retry attempts could endanger system performance.

10. The system **should** exhibit ACID (atomicity, consistency, isolation, durability) properties to guarantee that database transactions are processed reliably.[18] Note: In the context of databases, a single logical operation on the data is called a *transaction*.

Rationale: Good design practice.

11. The system **shall** be able to operate using 2G mobile network technologies (e.g. USSD, SMS).

Rationale: 2G network technology is reliable and prevalent.

Humanitarian Response Rationale: Telecommunications infrastructure may be damaged in a crisis. 2G networks will be the most widely available and more affordable option for data transmission, so mobile wallets should be able to operate with 2G technologies such as SMS and USSD.✚

12. The system **should** support geographically diverse primary and secondary failover sites (e.g. hot/warm/cool) for disaster recovery and business continuity of the system.

Rationale: Best practice for system disaster recovery and business continuity.

Humanitarian Response Rationale: In a rapid-onset crisis (e.g. earthquake), there needs to be geographically diverse sites to maintain reliability of the service.✚

5.5 MAINTAINABILITY

The ease with which the system can be changed, whether for bug fixes or to add new functionality. This is important because a large chunk of the IT budget is spent on maintenance and each change carries inherent risk. The more maintainable a system is, the lower the inherent risk and total cost of ownership.

A set of attributes that bear on the effort needed to make specified modifications include:

1. The IST **must** conform to agreed-upon architecture standards (e.g., the architecture should be "restful")

Rationale: Standards improve ability to maintain the system over time by ensuring conformity to known good practices.

2. The IST **must** conform to agreed-upon design standards. (e.g., modular design/Separation of Concern, Third Normal Form (3NF) for database design, Object Oriented – Polymorphism, Inheritance, Encapsulation)

[17] *BITS Guide to Business-Critical Telecommunications Services*, Financial Services Roundtable/BITS, 2004

[18] http://en.wikipedia.org/wiki/ACID

Rationale: Standards improve ability to maintain the system over time by ensuring conformity to known good practices.

3. The IST **must** conform to agreed-upon coding standards/conventions (e.g., good/best industry practices)

Rationale: Coding standards reduce variation in programming and reduce long-term operational and maintenance risk.

5.6 PORTABILITY

The ease with which software can be installed on all necessary platforms, and the platforms on which it is expected to run, and the ability of software to be transferred from one environment to another. Items to consider include:

- Adaptability
- Installability
- Co-existence
- Replaceability
- Portability compliance

1. The mobile wallet USSD implementation **should** be endpoint independent.

Rationale: Ease of implementation

2. The mobile wallet application implementation **should** support the top two operating systems (e.g., Apple iOS, Android) deployed in the target market, or the operating systems required to meet 80% of potential customers.

Rationale: Necessary to encourage adoption.

5.7 SCALABILITY

This section provides the desired ability of the system to support expansion or growth as load or demand is increased. Items to consider include:

- Ways in which the system may be expected to scale up
- Throughput: how many transactions per hour does the system need to handle?
- Storage: how much data does the system need to store?
- Year-on-year growth requirements

1. The system **should** scale out, increasing capacity through addition of more hardware or server instances.

Rationale: Scaling out allows additional hardware to be added as warranted and needed, to spread system load.

Humanitarian Response Rationale: There can be increased system load in a crisis and being able to scale out to support this expected surge is important.✚

2. The system **should** support online access to transaction history for the current and prior operational time frames (e.g., quarter, year) to ensure billing disputes or support issues can be investigated and resolved.

Rationale: Timely access improves customer service and reduces time to resolution of inquiries.

3. The system **must** support an archival strategy allowing records to be retrieved and reviewed in a timeframe no less than the records retention period required by law.

Rationale: Regulation and law often require retention periods of many years. Designing the system to support efficient archiving and retrieval can improve system scalability by removing data that does not need to be accessed from online systems, in turn freeing up resources for current and near-term activities.

4. The system **should** have enough storage capacity to support expected online data growth over 24 months, in conjunction with the archival strategy.

Rationale: The system needs headroom for operation and growth, or a dynamic mechanism to scale capacity on demand. This ensures operations under period of sustained growth without the risks associated with frequent system updates and replacement.

5. The mobile wallet implementation **should** seek to minimize storage at the endpoint device.

Rationale: Encourages adoption and use in developing nations, where older handsets may be in use.

5.8 FLEXIBILITY

If the organization intends to increase or extend the functionality of the software after it is deployed, that **should** be planned from the beginning in as much as possible; it influences choices made during the design, development, testing, and deployment of the system. Flexibility is the ease with which the system can be reused, deployed, and tested.

1. The system **must** be constructed in a modular fashion, such that major components or functions can be independently updated or replaced.

Rationale: Reduces risk when performing changes or maintenance. Potentially allows for rapid upgrade of functional components.

2. The system **should** be constructed using object-oriented design, such that components interact via method calls and do not directly access the attributes of other components.

Rationale: Industry best practice.

5.9 AUDITABILITY

When something goes wrong, there is need to understand the root cause so it can be corrected and/or avoided in the future. The instrumentation required for proper auditing of critical functions, including system process checkpoints, exception logging, etc. can be resource intensive and care should be exercised to ensure that subsystems do not interfere with application performance. Items to consider include:

- Audited elements: What business elements will be audited?
- Audited fields: Which data fields should be audited?
- Audit file characteristics: before image, after image, user and time stamp, etc.

1. The system **must** provide the ability to audit the details of every financial transaction.

Rationale: Auditability is a core need in any regulated industry to demonstrate compliance with regulation and law.

2. The system **must** track creation, update, and deletion of every system permission, role and right such that prior and new states are documented.

Rationale: System permissions enable users to perform processes or access data. The ability to track and monitor any changes to permissions is critical to determining potential risks for specific user accounts and evaluating potential issues during forensic review.

3. The system **must** track all changes to system configuration settings accessible through the user interface.

Rationale: Changes to system configuration can impact system integrity, stability, etc., and must be tracked to enable review of issues.

4. The system **must** track the creation of any business entity (e.g., partner, user, interface)

Rationale: Necessary for forensic auditing, training review, etc.

5. The system **shall** provide unique error codes for each class of data quality, processing or delivery error.

Rationale: Unique error codes are required to quickly identify and resolve issues or route problems for support.

5.10 INTEROPERABILITY

This section discusses the building of coherent services for users when the individual components are technically diverse and managed by different organizations. Items to consider include:

- Compatibility with shared applications: What other systems does it need to talk to?
- Compatibility with third-party applications: What other systems does it have to live with amicably?
- Compatibility on different operating systems: What does it have to be able to run on?
- Compatibility on different platforms: What are the hardware platforms it needs to work on?

1. The system **must** support open standards for authentication, authorization, etc.

Rationale: Open standards support broad acceptance and enable innovation by lowering the barrier to integration.

2. The system **must** support the ISO 8583 for all messages agreed to be necessary by participants.

Rationale: This is the legacy standard for financial transactions support by the majority of industry participants, particularly financial institutions.

3. The system **must** support the ISO 20022 standard for messages between transaction participants.

Rationale: This is the industry standard for financial transactions, with built-in support for mobile payments.

4. The mobile wallet **shall** support USSD standards for the man-machine interface (MMI) at the mobile device.

Rationale: The USSD protocol is a primary technology of secure interaction between the mobile money user/handset and the DFSP gateway.

5.11 DOCUMENTATION

Documentation provides the historical *what/why/how/when/who* system details, for future analysis or as the basis for change or support.

1. The system documentation **should** follow a consistent style and structure.

Rationale: Consistency reduces the learning curve and overall maintenance overhead.

2. The system administrative functions and related interfaces **must** be documented such that an administrator with appropriate experience but limited knowledge of the system can perform needed maintenance and administrative tasks.

Rationale: Detailed administrative documentation reduces training requirements and provides work instructions that potentially reduce variation, errors and overall operations costs.

3. Any published API **must** be fully documented such that a third party with reasonable technical skills and software API experience could implement a working interface.

Rationale: Good documentation is needed to bolster adoption and use of the API, which is to be consumed by external partners that will not have access to internal company knowledge.

4. The system architecture **should** be formally documented showing the individual system components and interfaces, server names, network subnets, protocols used, etc.

Rationale: High-level architecture documentation is very helpful when system issues occur or change planning is performed.

5. The software documentation **should** include references to any standard design patterns and include both the methods and attributes of each object, with descriptive text of its function. The intent is to provide software design documentation of sufficient detail that a developer of reasonable skill could understand the software components and perform maintenance as needed.

Rationale: Good software design documents will reduce maintenance and training costs over time.

6.0 References/Related Documentation

6.1 BACKGROUND DETAILS

6.1.1 Mobile Wallet Approaches

Mobile wallet approaches can be broadly categorized as *vertical* or *horizontal*.[19]

- Vertical wallet: The service provider acts as a wallet provider. It designs, controls and manages the mobile wallet to provide its services for the wallet. For example, a mobile network operator hosts a basic wallet tied to a stored value account backed by funds at the MNO's bank. Phone users on its network are able to send and receive payments through a USSD interface.
- Horizontal wallet: The mobile wallet provider offers a wallet capable of integrating services from other service providers. The wallet provider aggregates services and drives mass-market adoption. It often also offers design and management services for other service providers. Horizontal wallet models are common in developed countries.

The approach advocated in *The Level One Project Guide* is agnostic of wallet approach, integrating Digital Financial Services Providers (DFSPs) utilizing either wallet approach through a financial transaction routing utility (i.e., Interoperability Service for Transfers, or IST).

The wallet described herein closely adheres to the vertical wallet approach, as that model was implemented in our demonstration prototype. Also, the vertical wallet approach is more prevalent in developing economies, and can be deployed directly by an MNO that provides mobile money services.

6.1.2 Payment Transaction Modes

Mobile payments are generally performed in one of two modes:

- Remote: Parties use a mobile device to send and receive payments or transfer funds purely over the mobile channel, irrespective of their physical locations. In reality, the parties may be standing in the same store, but the payer does not use the merchant's point of sale (POS) infrastructure to initiate payment. Initiating a payment through a USSD session on a basic GSM phone is an example of a remote payment.
- Proximity: The mobile device is used primarily to authorize a payment at the point of sale and relies on the infrastructure the payment recipient to process the transaction. Using a biometric fingerprint scanner tied to a POS terminal to authorize a purchase in a store is an example of proximity payment.

The mobile wallet described herein supports both payment modes. However, the *emphasis is on remote payments*, as the model can be supported with ubiquitous GSM phones and does not require sophisticated biometric scanners or POS systems. Similarly, remote payment models have greater utility because the buyer doesn't need to physically travel to a merchant to authorize payment.

6.1.3 Where does the mobile wallet reside?

It is important to recognize that the mobile wallet capabilities may either be *resident* on the mobile device, or *hosted* on a remote server. The mobile device provides the man-machine interface (MMI) in all cases, but may or may not provide the business functions of the mobile wallet.

For example, the data supporting an Unstructured Supplementary Service Data (USSD) session mobile wallet described herein is housed on the remote servers of the DFSP. The mobile device displays only transmitted menus and the instruction screen, and collects the user input from the keypad, and then forwards the commands to the DFSP, where they are interpreted to create a payment instruction that is subsequently routed to the payment ecosystem.

Alternatively, a SIM-based mobile wallet application might store the account value on the SIM, and provide the application for authorizing payment, viewing the balance, and adding or removing value.

[19] Mobey Forum, Business Workgroup. *Structures and Approaches: The Changing Face of the Mobile Wallet*. Mobey Forum, 2013.

The mobile wallet described herein is hosted, as that model depends the least on the mobile device and SIM.

6.1.4 The Secure Element

Typically, a *device-resident* mobile wallet requires a tamper-resistant platform (typically a one-chip secure microcontroller) capable of securely hosting applications and their confidential and cryptographic data (e.g., key management) in accordance with the rules and security requirements set forth by a set of well-identified trusted authorities, known as a *secure element (SE)*. The secure element form factor may be a Universal Integrated Circuit Card (UICC), microSD, or embedded SE. The microSD and UICC form factors are both removable, while the embedded SE is permanently installed within the hardware.[20]

The demonstration prototype's client application for agents did not utilize a secure element. However, a production solution would most likely leverage the secure element or equivalent emulation to ensure a secure operating environment.

The prototype hosted mobile wallet utilizes USSD and does not require a secure element.

6.1.5 GSM

Global System for Mobile Communications (GSM) is one of the two fundamental mobile telecommunications network technologies, along with Code Division Multiple Access (CDMA). Originally known as *Groupe Speciale Mobile*, this technology is used by mobile networks around the world—those in Europe do so exclusively. The technology is driven by several bodies, a major one being European Telecommunications Standards Institute (ETSI). The strategic interests of GSM mobile network operators are represented by the GSMA, an association of more than 1,000 mobile operators and related companies devoted to supporting the standardizing, deployment, and promotion of the GSM mobile telephone system.[21]

6.1.6 The SIM

GSM is the primary cellular network technology deployed in the developing world. The *Subscriber Identity Module* or *SIM* card is a GSM-compatible implementation of the Universal Integrated Circuit Card (UICC) defined by ETSI TR 102 216 and subsequent standards.

The mobile network operator provides and controls the SIM, which is identified on the individual operator network by the i*nternational mobile subscriber identity* (IMSI) stored therein. Mobile network operators connect mobile phone calls and communicate with their market SIM cards using their IMSIs.

A SIM card contains its unique *Integrated Circuit Card Identifier* (ICCID), international mobile subscriber identity (IMSI), security authentication and ciphering information, temporary information related to the local network, a list of the services the user has access to and two passwords: a *personal identification number* (PIN) for ordinary use and a *personal unblocking code* (PUC) for PIN unlocking. (Wikipedia)

6.1.7 Deployment

A device resident mobile wallet may be pre-installed by the MNO on the SIM, pushed by the DFSP on first access, pre-installed on the phone, or installed on demand by the end user (e.g., on a smart phone).

The hosted mobile wallet demonstrated in the prototype is USSD session–based and does not require specific deployment on the device, as the USSD menus are delivered at the time of use.

6.1.8 Context for Users and Providers of Payment Services

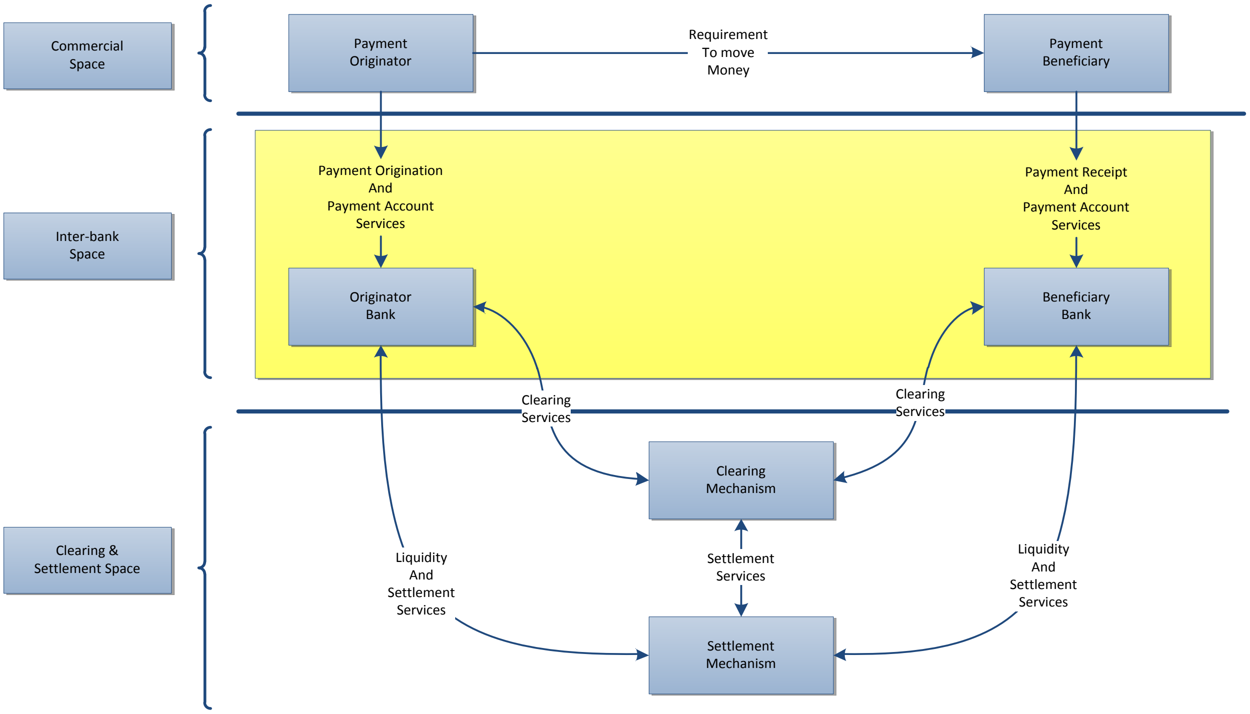
Implementation of communications and interfacing standards supports efforts to reach a state of ubiquitous, low cost mobile payment capabilities on a national scale. Legacy financial transaction systems predominantly supported ISO 8583. However, that standard does not directly support messages for mobile payments. A newer standard, the ISO

[20] Global Platform. *lPlatform made simple guide: Secure Element.* n.d. http://globalplatform.org/mediaguideSE.asp (accessed November 3, 2014).

[21] Mobey Forum. *Mobile Financial Terms Explained.* n.d. http://www.mobeyforum.org/whitepaper/mobile-financial-terms-explained-2/ (accessed November 3, 2014).

20022 universal financial industry message scheme, does provide support for the unique messaging needs of mobile payment, and is recommended as the current standard for interoperable mobile payment systems.

The European Payments Council developed a scheme for ISO 20022 compliant credit transfers that aligns conceptually with the push payment model proposed in the special report. The following diagram from the EPC documentation generically describes the push payment system needs and actors.


Commercial Space
Inter-bank Space
Clearing & Settlement Space
Payment Originator
Requirement To move Money
Payment Beneficiary
Payment Origination And Payment Account Services
Payment Receipt And Payment Account Services
Originator Bank
Beneficiary Bank
Clearing Services
Clearing Services
Clearing Mechanism
Liquidity And Settlement Services
Settlement Services
Liquidity And Settlement Services
Settlement Mechanism

From the *SEPA Credit Transfer Scheme Rulebook, Version 7.1*:[22]

- *The demand for payment services using a customer credit transfer arises from an Originator, who wishes to transfer Funds for whatever reason to a Beneficiary. Whilst the account is provided by a bank, the underlying demand and its nature are outside the control and responsibility of the banking industry or any individual bank.*
- *For this requirement to transfer Funds to be satisfied, the bank holding the account of the Originator must have the means necessary to remit the Funds to the bank holding the account of the Beneficiary and in the process be provided with the necessary information to accomplish the transfer.*
- *Provided that the Originator has sufficient funds or sufficient credit with which to execute the credit transfer, provided that the Originator is acting within its authority and provided that the credit transfer does not break any applicable legal, regulatory, or other requirements, including requirements established by the Originator Bank, then the Originator Bank will make the payment and advise the originator accordingly.*
- *The means for making the transfer will exist if the bank holding the account of the Beneficiary, the Beneficiary Bank, has agreed both the method and the rules of receiving the payment information as well as the method and the rules for receiving the payment value.*
- *Based on these means of transfer, the Beneficiary Bank will use the information received to credit the account of the Beneficiary, make the Funds available for its use once value has be received, and inform the Beneficiary about what has been applied to its account.*

[22] European Payments Council. *SEAP Credit Transfer Scheme Rulebook, Version 7.1.* Brussels: European Payments Council (EPC), 2012.

- *The purpose of interbank Clearing and Settlement is to correctly exchange information and to safely exchange value. The demand for Clearing and Settlement services stems from the need to transfer money between banks.*

For the mobile payments model, and depending on local regulation and law, a DFSP may stand in for an originating or beneficiary bank to transfer e-money and clear payment, though settlement of funds ultimately occurs within the formal banking system.

6.2 INDUSTRY GROUPS

The mobile wallet is a key component of the overall mobile payments ecosystem. As such, there are many stakeholders involved in the development and use of the mobile wallet to enable payments and other value-added capabilities from a mobile device.

The following is a partial list of stakeholders, including their representative areas of concern.

GSMA www.gsm.org	The GSMA represents the interests of mobile operators worldwide. Spanning more than 220 countries, the GSMA unites nearly 800 of the world's mobile operators with 250 companies in the broader mobile ecosystem, including handset and device makers, software companies, equipment providers and Internet companies, as well as organizations in industry sectors such as financial services, healthcare, media, transport and utilities. The GSMA also produces industry-leading events such as Mobile World Congress and Mobile Asia Expo.
Global Platform www.globalplatform.org	GlobalPlatform works across industries to identify develop and publish specifications which facilitate the secure and interoperable deployment and management of multiple embedded applications on secure chip technology. GlobalPlatform Specifications enable trusted end-to-end solutions which serve multiple actors and support several business models.
European Payment Council www.europeanpaymentscouncil.eu	The EPC is the decision-making and coordination body of the European banking industry in relation to payments. The EPC develops the payment schemes and frameworks which help to realize SEPA. SEPA is a European Union (EU) integration initiative in the area of payments. SEPA is the logical next step in the completion of the EU internal market and monetary union.
Mobey Forum www.mobeyforum.org	Mobey Forum is the global industry association empowering banks and other financial institutions to lead in the future of mobile financial services. Mobey Forum connects industry thought leaders to identify commercial drivers for the development of better mobile commerce. Mobey Forum's members collaborate to analyze business strategies and technologies to create innovative, interoperable and competitive financial services. Mobey Forums Workgroups and Task Forces get together to discuss specific topics in the mobile financial services industry, such as mobile wallets, MPOS and security. Each group has a knowledgeable chair with long-standing experience and expertise on the topic. Group participants are Mobey members—from banks and other organizations within the industry. The Workgroups and Task Forces produce Mobey Forum's whitepapers.
European Telecommunications Standards Institute (ETSI) www.etsi.org	ETSI, the European Telecommunications Standards Institute, produces globally-applicable standards for Information and Communications Technologies (ICT), including fixed, mobile, radio, converged, broadcast and internet technologies. Original standards developer of GSM.
3GPP www.3gpp.org	The third Generation Partnership Project (3GPP) unites [Six] telecommunications standard development organizations (ARIB, ATIS, CCSA, ETSI, TTA, TTC), known as "Organizational Partners" and provides their members with a stable environment to produce the Reports and Specifications that define 3GPP technologies. The project covers cellular telecommunications network technologies,

	including radio access, the core transport network, and service capabilities—including work on codecs, security, quality of service—and thus provides complete system specifications. The specifications also provide hooks for non-radio access to the core network, and for interworking with Wi-Fi networks.

6.3 DOCUMENT STYLE

The requirements enumerated in this document follow the wording guidelines defined in the IEEE-SA Standards Board Operations Manual, paragraph 6.4.7. Those guidelines follow:

The word ***shall*** indicates mandatory requirements strictly to be followed in order to conform to the standard and from which no deviation is permitted (**shall** equals is required to).

The word ***should*** indicates that among several possibilities, one is recommended as particularly suitable without mentioning or excluding others; or that a certain course of action is preferred but not necessarily required (**should** equals is recommended that).

The word ***may*** is used to indicate a course of action permissible within the limits of the standard (may equals "is permitted to").

The word ***can*** is used for statements of possibility and capability, whether material, physical, or causal (can equals "is able to").

Note: The use of the word **must** is deprecated and **shall not** be used when stating mandatory requirements; **must** is used only to describe unavoidable situations.

Note: The use of the word **will** is deprecated and **shall not** be used when stating mandatory requirements; **will** is only used in statements of fact.

6.4 ACRONYMS, ABBREVIATIONS, KEY TERMS AND DEFINITIONS

This subsection provides the definitions of all terms, acronyms, and abbreviations required to properly interpret this document.

Abbreviation/Acronym/Term	**Definition**
AML/CFT	Anti-Money Laundering and Combating the Financing of Terrorism
ARPU	Average Revenue Per User
BIP	Bearer Independent Protocol
C2C	Consumer to Consumer
CAT	Card Application Toolkit
CICO	Cash In, Cash Out
DFS	Digital Financial Services
DFSP	Digital Financial Services Platform
DFSP	Digital Financial Services Provider
ECS	Electronic crediting system
FDI	Foreign Direct Investment
FATF	Financial Action Task Force
FSP	Financial Services for the Poor
FSP	Financial Services Provider
FRMS	Fraud and Risk Management Service
GSM	Global System for Mobile Communications, originally *Groupe Spécial Mobile*
ICTs	Information and communication technologies
IDRBT	Institute for Development and Research in Banking Technology
IMPS	Immediate Mobile payments services
IMSI	International Mobile Subscriber Identity
IST	Interoperability Service for Transfers

Abbreviation/Acronym/Term	Definition
ISV	Integrated Solution Vendor
IVR	Interactive Voice Response
KYC	Know Your Customer
MASP	Mobile payment application service provider
MDM	Mobile Device Manufacturer
MDPS	Merchant Digital Payment Service
MFS	Mobile Financial services
MM EDP	Mobile Money Ecosystem Demonstration Platform
MMSP	Mobile Money Service Provider
MMU	Mobile Money for the Unbanked
MNO	Mobile Network Operator
MPFI	Mobile Payments Forum India
MSISDN	Mobile Station International Subscriber Directory Number
MSME	Micro, Small and Medium Enterprises
MTAN	Mobile Transaction Authentication Number
MTO	Money Transfer Organization (MTO)
MVNO	Mobile Virtual Network Operator
NEFT	National Electronic Funds Transfer
NFC	Near Field Communication
NGO	Non-Governmental Organization
NPCI	National Payment Corporation of India
PCI	Payment Card Industry
PIN	Personal Identification Number
POS	Point of Sale
RBI	Reserve Bank of India
REST	Representational State Transfer
RTGS	Real Time Gross Settlement
SIM	Subscriber Identity Module
SMP	Significant Market Player
SMS	Short Message Service
STK	SIM Application Toolkit
UI	User Interface
USAT	USIM Application Toolkit
USSD	Unstructured Supplementary Service Data
WAP	Wireless Application Protocol