Requirements for a Pro-Poor Interoperability Service for Transfers

The Bill & Melinda Gates Foundation

January 5, 2015

BILL & MELINDA
GATES foundation

Table of Contents

Contents

Suggested citation: Bill & Melinda Gates Foundation*. Requirements for a Pro-Poor Interoperability Service for Transfers*. 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 model outlined in *The Level One Project Guide* defines two core operating components that would be operated by the Digital Payments System Organization, a not-for-profit entity: the Interoperability Service for Transfers (IST) and the Fraud and Risk Management Service (FRMS).

The operating model also includes components that would interact with the IST and FRMS, but be operated by participating Digital Financial Services Providers (DFSPs): account opening services (AOS), consumer and agent management services, and merchant account management

This document extends the prior efforts of the Gates Foundation, incorporating work from industry groups and other stakeholders to flesh out detailed requirements for the IST solution envisioned in *The Level One Project Guide* 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

The purpose of this requirements document is to describe the behavior of the Interoperability Service for Transfers (IST) defined in* The Level One Project Guide. *This document provides requirements, design constraints and other factors necessary to describe the demonstrated capabilities of the prototype IST.

The IST requirements herein are not intended to be comprehensive, but rather to highlight one approach that meets the criteria of a pro-poor digital payments switch described in the reference model. The IST described herein is a *thick* switch, containing services and features that extend capability beyond the core financial and non-financial transaction routing capability of a *thin* switch. Also, these requirements include capabilities implemented in the DFS System IST prototype, created to spur discussion among ecosystem partners.

The requirements document is intended as an example for describing and documenting solution requirements for components of a pro-poor financial services eco-system leveraging mobile and digital infrastructures. It represents a specific model, though the “right” approach will vary depending upon the situation in any particular counrty’s environment, including but not limited to vision, monetary policy, regulation, power and telecommunications infrastructure, and banking and telecom technologies.

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 the poor.

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.

The IST requirements herein are not intended to be comprehensive, but rather to highlight one approach that meets the criteria of a pro-poor digital payments switch described in the reference model. The IST described herein is a *thick* switch, containing services and features that extend capability beyond the core financial and non-financial transaction routing capability of a *thin* switch. Also, these requirements include capabilities implemented in the DFS System IST prototype, created to spur discussion among ecosystem partners.

The requirements document is intended as an example for describing and documenting solution requirements for components of a pro-poor financial services eco-system leveraging mobile and digital infrastructures. It represents a specific model, though the “right” approach will vary depending upon the situation in any particular country’s environment, including but not limited to vision, monetary policy, regulation, power and telecommunications infrastructure, and banking and telecom technologies.

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 IST envisioned in *The Level One Project Guide* and further extended by the demonstration prototype system.[2] If built, the envisioned national system would operate as an *open loop* transaction routing utility, available to all qualified parties participating in payment processes. **The IST's primary function is to securely and reliably transmit financial transactions between the appropriate participants in the digital money ecosystem.**

The document includes supporting requirements, such as performance, availability, confidentiality, security, and usability characteristics, necessary to ensure the switch can meet the demands of its intended constituents.

To provide the intended services, the IST must interface with:

- Regulated financial institutions
- Governmental and non-governmental organizations (NGOs) that provide financial support to consumer beneficiaries, or receive payments such as utilities, fines, or school fees
- Mobile network operators
- Digital financial services providers (i.e., mobile wallet operators)
- Account lifecycle management systems
- Fraud and risk management systems

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

- Agent and merchant management systems

Also included are the capabilities of the *actors* responsible for managing the system components, setting up system partners and interface, monitoring system operations, and interacting with supported partners.

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

Item	Switch Model	In-Scope Items	Detail
1	Thin	On-board transaction partners	Set up new participants, provide test environment
2	Thin	Route transactions	Transfer messages between participants
3	Thick	Provide directory services	Identify details of target accounts, including home network or DFSP.
4	Thick	Enforce account limits	Determine if transactions conform to risk-mitigation limits
5	Thick	Perform fraud and risk check	Identify potentially fraudulent activity and assess risk participants
6	Thick	Enable transaction commissions	Track transaction fees execution and ensure that payers are aware they are incurring a fee prior to performing a transaction
7	Thick	Process bulk payments	Decompose into individual transactions or groups, tracking status of component transactions and the parent bulk file
8	Thick	Manage vouchers	Distribute notification to beneficiaries and route subsequent payments at the time of use
9	Thin	Provide settlement instructions	Determine amounts owed between participants and ensure funds are transferred
10	Thin	Provide reports	Enable users to view and analyze system activity and historical transaction data
11	Thick	Provide biometric repository and verification service	Register and associate biometric profiles with accounts

2.2.2 Out-of-Scope Work

The following items are out of scope and are not included in this document:

- Cross-border financial transactions or communications
- Legal, regulatory, or stakeholder governance of the system's capabilities (this activity would be the responsibility of the IST implementers, operators and participants)[3]
- Functions of the mobile wallet
- Functions of merchant management other than those required to support vouchers
- Functions of digital money operator agent management
- Capabilities provided entirely within the systems of the mobile network operator (MNO), bank, NGO, government or other participating entities
- In general, *push* transactions are not revocable or reversible when the transaction completes normally, and thus reversal of properly executed transactions (i.e., transactions initiated by the payer) is out of scope. For clarity, correction of transactions resulting from system error **should** be addressed.
- Transaction liability or risk transfer between participants

[3] The Gates Foundation is preparing a rulebook to inform the governance structure.

2.3 CURRENT STATE

Providing access to formal financial services is fundamental to improving the lives of poor people, and digital payment systems are clearly a means to this end. Yet previous Gates Foundation research has determined that the economic models of traditional providers in formal payment systems simply do not work when applied to the ultra-poor. Banks, the traditional providers of financial services, typically make money on payments in four ways: from account services—the value of the "money in the bank;" from fees on cash-in, cash-out (CICO) transactions; from other charges for payments transactions; and from related activities (or, *adjacencies*) such as lending.

Extending to poor people these business models predicated on wealthy customers is challenging, because balances are low, transaction values are small, and fees for transactions are often considered unacceptable—particularly for daily payments currently made in cash. Research has concluded that payment systems designed to serve poor people will need to work primarily on a *usage-driven* model, rather than one driven by account balance. In a usage-driven system, a high number of low-value transactions can generate enough revenue to attract commercially viable providers of financial services and related financial institutions—if transaction and operational costs to these providers can be minimized. Fortunately, modern technology, better systems design, the achievement of minimum scale, and operational efficiencies can together produce dramatic improvements in the costs of payment systems. In turn—with appropriate policies in place—this can enable the low fees and prices necessary to drive adoption and continuous usage of these systems.

To date, more than 225 digital financial services have been launched in the world. Many of these are in developing countries, and have goals of financial inclusion or support of poor people. These have been met with varying degrees of enthusiasm by consumers, merchants, banks, mobile money operators, and regulators. Although some are regarded as successes, none have broken through the "cash ceiling" by replacing cash as it is used for commercial and personal transactions today. Because of this, current digital financial service implementations are supported by extensive, expensive, and risk-prone agent networks handling CICO functions.

Many emerging payments systems are private *closed-loop* systems, where payments are only possible if both payer and the payee have direct relationships with the provider. Examples of closed-loop systems, include remittance providers such as MoneyGram or Western Union, online wallets such as PayPal, and mobile money systems such as M-PESA. While closed-loop systems may be easier to establish, providers appear incented to keep their systems closed in order to establish a dominant market share and defend against competitors. These systems are less useful a pro-poor operating environment than open-loop systems, due to costly duplication of infrastructure. Because a closed loop requires end-to-end functionality, not all services will be optimized, and they almost always have practices that make withdrawal of funds by non-members of the system more expensive or slower.[4]

Challenges identified in existing digital payments solutions include:

- Burdensome and costly account opening
- Digital financial services platforms have limited functionality and are slow to innovate
- Complicated user experience—too many numbers to remember and too much typing
- Frequent network downtime disrupts accessibility and usability
- Lack of interoperability between MFS providers
- Low merchant acceptance
- CICO transactions are dominant
- Agent liquidity challenges deter usage
- Lack of system-wide fraud and risk management tools
- High percentage of over-the-counter transactions

2.4 FUTURE STATE

The desired future state is to deploy a pro-poor digital payment ecosystem, facilitated by an interoperability switch capability that provides a standardized, highly scalable architecture, ensuring efficient routing of transactional and

[4] *The Level One Project Guide*, Bill & Melinda Gates Foundation, 2014

supporting information to connected partners in near-real time. Thus, overall ecosystem friction is minimized and per-transaction costs are reduced. The ultimate cost of operation is directly related to many factors, including transaction volume, cost of development, and depreciation schedule of the build-out investment.

The target IST implementation would support an open-loop model, enabling partners to develop to interface standards (e.g., ISO 20022 and ISO 8583, the prevailing legacy and current standards) to create a high-functioning messaging interface for connection to similarly integrated partners and services. This standardized and scalable messaging hub, along with a broad membership of diverse partners representing a wide breadth of services and capabilities, would provide opportunities for rapid innovation, as the standards would be extensible with common message structures.

2.5 METHODOLOGY

This requirements document was developed though analysis of prior works, including Gates Foundation strategy documents, *The Level One Project Guide*, industry research and articles, and the pro-poor IST demonstration prototype[5].

A major focus of this project was to place careful attention on the functional view of user and system requirements and to explicitly avoid computer jargon and discussions of actual software and hardware solutions. In this way, this project focused on the "What" and "Why" descriptions of the IST, not on the "How" or physical information technologies that may be used to implement the requirements.

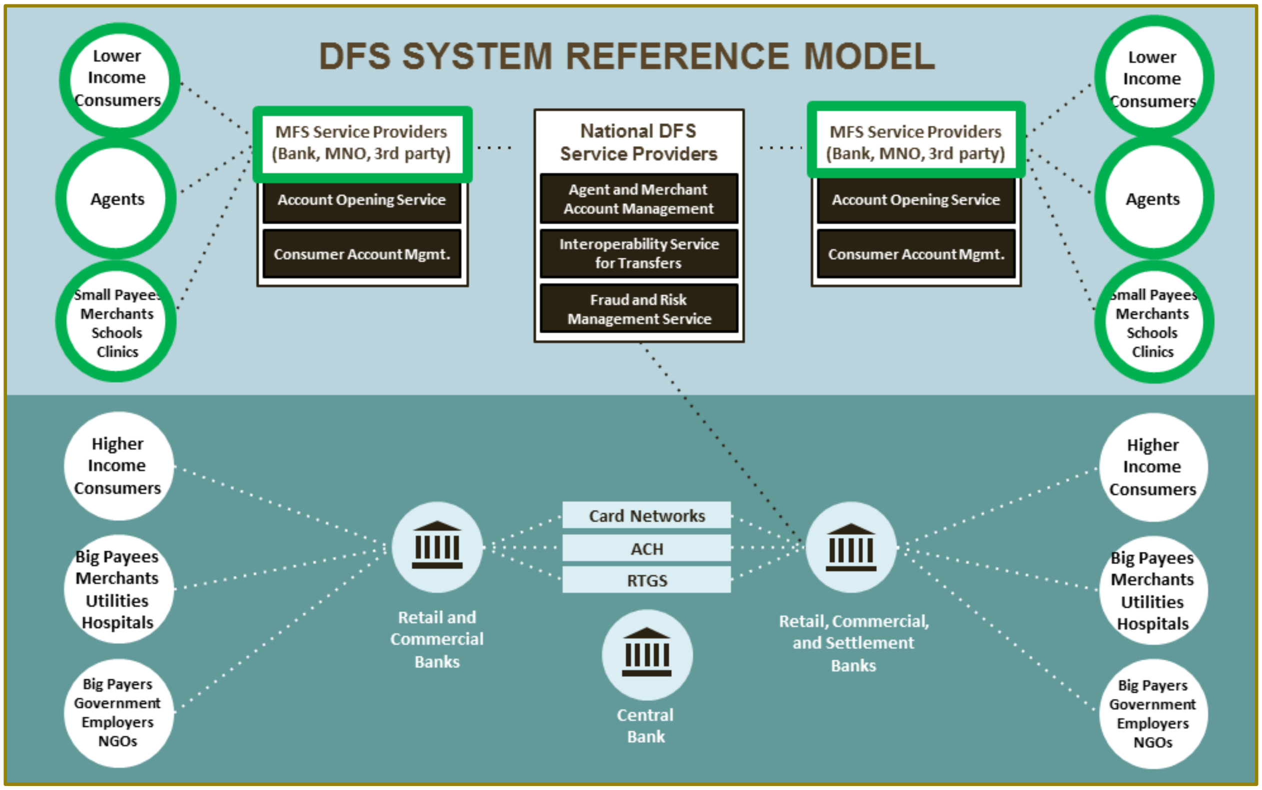
As a result, non-technical language is used to describe the system. Close attention was paid so that subject matter experts, stakeholders, and users can understand the terms and process models. The goal was to use terms contributed by participants that would also have explicit meaning to software and system engineers who might implement the requirements.

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

3.0 DFS System Reference Model

The figure below depicts the breadth of the digital payments ecosystem. The Interoperability Service for Transfers (IST) and supporting Fraud and Risk Management Service (FRMS) are outlined for easy identification in the context of the reference model.

It should be noted that while agent and merchant management are depicted as part of the national DFS System, these can be offered by separate mobile money operators or other third parties. Similarly, account opening services pictured as part of DFSPs could be provided as part of the National DFS Provider.


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 THE PAYMENT PROCESS OVERVIEW

All payment transactions follow a series of steps, and digital payments include explicit steps that are only implied in cash transactions:[6]

Step 1 – Payment Initiation: The payer presents the selected payment instrument through which a payment instruction can be submitted. In the case of a consumer, this might be a mobile wallet; for a bulk payer, this might be an enterprise resource planning (ERP) system integrated to the IST.

Step 2 – Authentication: The payer’s identity is confirmed. For a mobile wallet payment, multiple authentication factors may be involved, for instance: 1) the user-entered PIN number, associated with 2) the mobile wallet that is 3)

[6] Porteous, B. L. (2013). *Introduction to the National Payments System.* Somerville, MA: National Payment Systems Institute.

installed on the mobile phone SIM 4) that was previously registered to the phone number by the mobile network operator.

Step 3 – Authorization: The payer grants permission using the transaction protocol. For a mobile payment, the user-entered PIN would provide authorization as well.

Step 4 – Processing: The transaction is transported from the mobile wallet through the mobile network to the digital money operator serving the payer. If the payee and payer are on the same DFSP's system (an "on-us" transaction), the payer's account is debited and the payee's account is credited, then the process is completed. When the payee is on a different system (an "off-us" transaction), the transaction is transferred to a switch for routing to the payee's target financial service provider. The payee's system will receive and execute their side of the transaction. Additional steps are then required.

Step 5 – Clearing: Generically, payment instructions are exchanged (cleared) between the payer and payee financial institutions and reconciled to determine the obligations of each party to the other. Clearing may be done in real time, close to real time, or once several sets of instructions have accumulated (called *batch mode*).

Note: The payment is cleared (from the perspective of the payer) when the payer no longer has access to the funds, and cleared (from the perspective of the payee) when they gain access to the funds.

Step 6 – Settlement: Currency value is transferred between the participants in an "off-us" transaction, and the process is complete. This may occur in real time (often used for high-value transactions using real-time *gross settlement* systems, e.g., US Fedwire), or more commonly same or next day as *net settlement* after multiple transactions between parties have been accumulated. In our model, the IST performs same-day net settlement based on various trigger conditions.

Additionally, third-party providers may be utilized to provide the actual infrastructure or supporting services (e.g., authentication, fraud and risk management)

3.2 ACTORS

The following table provides a brief description of the *actors*, or roles played by a user or any other system that interacts with the mobile wallet.

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

3.3 PAYMENT-ACTOR MATRIX

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

4.0 Core Capabilities

The following subsections describe the primary capabilities expected in the completed system, providing a high-level functional description and supporting rationale.

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. 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.

4.2 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 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 ROUTE TRANSACTIONS

4.3.1 Description

A centralized transaction switch enables participants to implement a single connection, and then transact with any other appropriate participant of the switch. When compared with bilateral connection implementations, this *connect once, transact with many* model greatly reduces the overhead of developing, implementing, and maintaining connections with multiple transaction partners.

The primary function of the IST is to reliably connect all parties associated with a digital financial service transaction, accurately passing the transaction messages in real time to ensure participants are confident that funds are available and properly committed.

To enable routing capability, the IST may need to translate messages between existing financial industry messaging standards (e.g., ISO 8583, ISO 20022) and any proprietary formats dominant in a particular market. It is common for ISO 8583 message fields to be "overloaded" by message participants to transmit agreed-upon data. Thus, message translation capability may need to address custom overloading of standard message elements in a controlled and consistent manner, thereby reducing barriers to use and improving likelihood of acceptance. Also, closed-loop proprietary formats may require extensive mapping to translate into formal standards. Message translation will also be needed to extend the IST as new standards emerge.

Alternatively, the IST can publish a set of standards required for use by the MNOs, financial services companies and banks that connect to it. In this way a translation will not be required, but the connecting companies will need to change their installed base of connections.

Also, the IST **must** provide appropriate logging services to ensure issues or disputes can be properly analyzed and resolved as part of an exception handling capability.

Finally, the IST will need access to some directory service that identifies the carrier network associated with a particular phone number, to ensure accurate and efficient routing.

Note: Clearing—removing access to the funds by the payer and granting it to the payee—is a function of the respective DFSP systems. The IST routes the payment messages.

4.3.2 Rationale

The routing function needs to occur in near-real time, as delays might cause the parties to prefer cash over risks of clearing. Participating systems and services in the payment process would be expected to adhere to agreed-upon service level agreements (SLAs) to ensure the entire end-to-end payment process meets user expectations.

Standards promote adoption by reducing the overall work required to connect partners. The actual standards implemented may vary by country, based on overall payments ecosystem maturity level (e.g., forms of ISO 8583 are widely used in legacy financial systems, while the more recent ISO 20022 standard provides support for digital payments). Ultimately, the cost of transitioning to a new standard may be prohibitive, and impact adoption on a case-by-case basis.

CIO Note: Implementation of a centralized switching function can speed digital payment adoption across the entirety of the ecosystem by providing translation between differing interface formats and standards. To accomplish this, the IST's internal message format would be a super-set of the information provided in partner message interface formats. Inbound messages would be mapped from the sending partner format to the internal format, and then reconstructed in the outbound format of the intended recipient partner.

A commercial software provider implementing this way would benefit by building a library of translation maps that could then be re-used depending upon the country-specific environment. Because only partners' compliance with the published standard would need to be validated on subsequent deployments, there would be lower overall development and maintenance costs, and potentially faster implementation.

4.3.3 Requirements

1. The IST **shall** route transaction messages between authorized participants.

Rationale: This is the core function of the payment switch.

2. The IST **shall** support *push* payments (i.e., the transaction is initiated by the payer for the benefit of the payee).

Rationale: Push payments are considered critical in keeping system costs down, as fraud potential is lower than with pull mechanisms. Also, eliminating pull payments avoids delayed settlement, complexity, and related costs for chargeback mechanisms, etc. Finally, it is easier for participants to understand, "If you send a digital payment, there is no built-in way to get your money back, so be sure you want to pay and that this is the correct recipient."

3. The IST **shall *not*** permit transaction revocation of properly routed messages.

Rationale: As these are push payments, the sending DFSP is responsible for ensuring sufficient funds are available and providing clearing. A core principle of the IST is to keep complexity low, to reduce costs and avoid transfer of risk. If something does go wrong with payment processing after the payment request is sent by the DFSP, a dispute resolution process would address the return or crediting of funds.

4. The system **should** support a process to correct transactions routed in error.

Rationale: It is possible that administrative user or system processing errors may result in improper transactions being created and routed. There should be a mechanism in place to address an error that is caught in a timely manner.

5. The system **shall** support payment request messages from the payee to the payer.

Rationale: Frequent payees, such as merchants, will perform transactions much more frequently than an average consumer. Providing the ability to request payment reduces potential keying errors by the consumer and may reduce overall payment processing time.

6. The IST **shall** support the standardized messaging formats required by financial system participants.

Rationale: Standardized messaging is required for the system to scale cost-effectively. Examples include ISO 8583 and ISO 20022.

7. The IST **shall** translate between message formats as required to deliver messages from one participant to another where the formats may be dissimilar.

Rationale: All participants are unlikely to be on the same interface formats at all times. Providing the ability to translate between formats improves overall IST utility and reduces barriers to adoption.

8. The IST **shall** ***route*** financial transaction messages between connected participants in near-real time.

Rationale: To achieve widespread acceptance, typical digital retail payments must be completed in a similar timeframe to a cash purchase.

9. The IST **shall** ***accept*** connections **only** from authorized parties.

Rationale: We only want to take transactions for approved partners.

CIO Note: Allowing a large number of partners increases likelihood of reaching a broader customer or merchant base with more features and support for innovation. However, financial systems should be assumed to be targets for fraud, hacking, or breach. As such, only connections from vetted and pre-approved partners are typically accepted.

To ensure confidentiality, the transmission channel must be encrypted between the messaging partners. Various methods for securing the channel connectivity include point to point private circuits or leased lines, Mulitprotocol Label Switching (MPLS), virtual private networks (VPNs) over the public Internet (e.g., IPsec tunnel), and on-demand traffic encryption (e.g., HTTPS).

The selected method should support mutual authentication of messaging partners, so that each partner controls access and is confident of the identity of the connected partner. Firewalls should always be used to allow only the least amount of access necessary to perform the business activity, and to isolate the interface from their internal networks.

10. The IST **shall** ***ignore*** messages that are **not** authorized (i.e., transmitted through proper channels and processes by an authorized participant).

Rationale: Responding to unauthorized messages would waste system resources and potentially enable a denial of service (DoS) attack by overloading the IST as it responds to messages from an unauthorized party (i.e., amplification attack).

11. The IST **shall** ***reject*** messages that do **not** conform to the agreed standard.

Rationale: Rejecting the message will clearly indicate to the sending party that there is a problem and enable them to address it.

12. The IST **shall** track transactions from the time a complete message is received from an approved participant, until processing is complete.

Rationale: Users need to know that the state of transactions to address exceptions and provide business feedback.

13. The IST **shall** log all accepted transactions.

Rationale: Logging is required for system performance management, business analysis, audits, reconciliation, and billing and dispute resolution.

14. IST transaction log messages **shall** include the information needed to identify all participants, the activities each participant performed, the amount transacted, and when the transaction started and finished.

Rationale: This is a starting point for the information that is needed in a useful log message.

15. The IST **should** provide an error response when a received message cannot be processed. The response should include a detailed error code identifying the reason the message could not be processed, or indicate that the reason could not be determined.

Rationale: Message exceptions are likely to occur. By providing exception details the system facilitates error correction by the sender.

Message Delivery Error Handling

16. The IST **should** provide resilient message delivery capabilities to automatically recover from common message routing or delivery failures.

Rationale: Power outages, downed lines, hardware failure, software bugs, human error, and other factors result in outages worldwide. Including automated recovery and error handling will improve the overall resiliency

a. The IST **should** determine if message failures are terminal or recoverable.

Rationale: Messages might fail because of some data error or failure situation that is deemed unrecoverable (terminal) or recoverable (e.g., intermittent connectivity to participant). Having the ability to determine or classify failure modes allows enables automated recovery.

b. The IST **may** retry distribution of any "recoverable" failed transaction messages on a defined retry period or when the failure condition is resolved. For example:

- The participating system (e.g., DFSP) is intermittently reachable.
- The participating system is requesting a redelivery attempt.
- Internal system congestion causes a processing time-out.
- There are other recoverable errors that do not require changing the message information.

Rationale: Defining a retry period allows for automatic completion or improved distribution where the reason for failure can be corrected (e.g., beneficiary signs up for a mobile wallet upon notification of available benefit, a DFSP comes back online)

c. The IST **should** not retry messages when a terminal delivery condition is identified. For example:

- Participant authentication failure.
- A destination participant cannot be identified from the information provided.
- The receiving participant rejects the message with an error.
- The message fails fraud check or risk scoring.

Rationale: It is a waste of system resources to attempt redelivery of a message that by definition will never be deliverable.

17. The IST **should** have an administrator-configurable minimum message retry time.

Rationale: High frequency retries could degrade or overload processing capability. The administrator should identify and set a safe floor limit that balances delivery speed with system throughput limitations.

18. The IST **should** have an administrator configurable maximum message time to live (TTL).

Rationale: High retry frequency could degrade or overload processing capability. The administrator should identify and set a safe floor limit that balances delivery speed with system throughput limitations.

19. The IST **should** have an administrator configurable maximum message retry count.

Rationale: Excessive retries will build pressure on the system, as the sender of the message has to wait to determine if a message is ultimately delivered or rejected. Providing a retry limit in conjunction with a retry frequency allows the total retry time to be set as an alternative to a hard TTL.

20. The IST **shall** discontinue retries when a defined maximum retry limit is reached or processing completes successfully.

Rationale: If there were no retry limit, failed transactions could increase forever, potentially consuming enough system resources to degrade or prevent transaction delivery.

21. The IST **should** enable an administrator to apply error-handling methods by message type or participants.

Rationale: Different kinds of messages have different time sensitivity. For example, a payment to a merchant might have a very limited TTL or fast retry rate, to prevent congestion at the point of sale; while a notification of a new voucher is a lower priority and thus has a slower retry rate and longer TTL.

22. The IST **should** enable a system administrator to manually retry message delivery for all or selected messages.

Rationale: There will likely be processing scenarios (e.g., one DFSP is unavailable) that require manual intervention to clear backlogged transactions.

23. The IST **should** support automatic rejection of messages when critical system errors will ultimately result in delivery failure due to time-out or retry limitations.

Rationale: In conjunction with proper error message responses, rejecting messages from participants may be a more effective method when system issues or maintenance will result in processing failure. For example, if a critical path service (e.g., directory service) is unavailable, the IST will be unable to identify the message destination, and thus the message will not be delivered.

4.4 PROVIDE DIRECTORY SERVICES

4.4.1 Description

A core capability of the IST is to route transactions between digital users and other participants residing on any number of networks within the payment ecosystem. From the perspective of the IST, the message arrives at the payer system interface and must be delivered to the payee system interface. Once a payment is delivered to the payee's system, that system must process the payment and credit the destination payee account—typically a stored-value account at a digital financial service provider, or a currency account held at a bank.

> Note: The IST routes "off-us" transactions, where a digital money user on one network wants to pay a user on another network, and each uses a different digital payment services provider. "On-us" transactions (where payer and payee accounts are on the same system) may not be routed by the IST. However, if the IST is to track account balances for individuals across the ecosystem, even "on-us" transactions would need to be forwarded to the IST for balance updating.

For the IST to correctly route payment to the proper payee system, the payment sender must provide the payee destination "address" (i.e., identify the destination system and unique account identifier of the payee), or the IST must determine the address of the payee destination account in some fashion.

A payer will likely have some limited information about the payee. For example, the payee may provide their name, phone number, bank and bank account number, national account ID, mobile wallet ID, or some combination of these, depending upon the minimum data requirements of the mobile payment ecosystem.

In a simple implementation where every end user has a mobile device, and that device has a mobile wallet associated with a single stored value account, the minimum detail needed is the payee's phone number. However, more complex scenarios are possible, including:

- Payee has multiple accounts within the mobile wallet that is tied to the phone.
- Payee shares the phone with others, but has a unique account tied to the phone number.
- Payee has a mobile wallet, but no phone or phone number (i.e., hosted virtual wallet).

These scenarios imply the need to target a specific account associated with the payee's mobile wallet, so the phone number alone won't be sufficient to identify the payee address (or won't exist, in the case of the "no phone" scenario).

Identifying the Destination for Message Delivery

A single digital financial service provider will have detailed information account for its customers (e.g., name, phone number, date of birth, national ID), but won't inherently know anything about the mobile users or payment recipients served by other providers or bank customers.

Thus, when a payment is received from a payer's system without a complete destination address, the IST must determine the payee's address through some means. The options include:

Blind delivery options

1. Broadcast: All payment messages are sent to all system participants (i.e., digital financial service providers and banks). This is simple and potentially effective when there are a very small number of participants. However, transmission volume increases exponentially with the number of participants, so this is generally unacceptable for large systems. Further, the private payment details would be sent to participants that have no need for the information, creating a broad potential for abuse of the information (e.g., mining a competitor's customer base for solicitation via SMS).
2. Round-robin: Messages are sent to participants in a rotating, repeating order until acknowledged by one or rejected by all.

Destination lookup options

3. Shared account listings: Every participant shares their account listing information with every other participant, allowing the sending system to address the payment to the specific target system holding the payee account. In this case the switch would simply route payment messages as directed, without validation. The participants would be responsible for proper addressing. This model duplicates the account information at all participants, providing customer information to all competitors.
4. Directory service: Participants contribute to and update a centralized, query-able data service. This customer information would potentially include phone number, system-wide unique account identifier(s), customer name, and any other addressable attribute (e.g., national ID, unique mobile wallet account ID).
5. Hybrid model: Elements of each model are leveraged. For example, the system might initially use broadcast or round-robin routing, and then, over time, store each success to build a mapping of customers to providers.

Except in broadcast or round-robin scenarios, it is clear that the ***minimum*** amount of shared information shared is correlation of DFSP to unique payee identifier. Thus, if the operating model allowed payment targeting by phone number, national ID, or unique mobile wallet account ID, *all* of those data elements would need to be shared for efficient routing. Therefore, limiting the number of data elements that might be used to address a payment dramatically reduces the amount of information that must be shared.

Again, in a closed system the mobile network operator may know both the sender and recipient information. But in an open system supported by multiple mobile network operators, the information will need to be query-able to provide the needed visibility. Given that the IST **must** route transactions to all participants and is the only centralized system connecting all of the participants, we chose to implement the directory service as an internal function in the prototype. However, this service might alternatively be a stand-alone function external to the IST. In that scenario, the IST would make a call to the service to determine the home DFSP of the payment recipient's mobile wallet account.

Inquiry Services

At a minimum, a directory service must include information needed to identify the DFSP holding the payee account (i.e., DFSP ID, and either phone number or account ID). The directory must then accept lookup inquiry messages from permitted systems, and respond with the correlated data. For example, if the IST provided the payer phone number, the directory service would respond with the DFSP ID, and the IST could then direct the payment message to the specified provider.

A key element to reducing misdirected payments is to provide feedback to the payer that the provided destination address (e.g., account or mobile phone number) belongs to the intended recipient. One option is to return the name of the destination account holder when the payer inputs the destination account ID or phone number.

This account holder inquiry could be supported directly in the directory service if the information is provided to the routing service, or be directly supported by the mobile wallet account holder (i.e., DFSP or bank) if the data is not shared to and query-able from the routing service.

Managing the Directory Service Data

For the directory service to be effective, it **must** be accurate and inclusive of mobile wallet accounts, phone numbers, or other addressable data elements. This implies that every participant mobile wallet provider or bank **must** update the directory service when pertinent account details are created, updated, or deleted. A regular full refresh of the data from account holder systems would also ensure data accuracy over time. Depending upon the implementation, some delay in updating the directory data may be desirable to prevent propagation of errors.

To ensure the integrity of the mobile phone infrastructure, telecomm regulations govern the registration of mobile numbers to mobile network operators, controlling number portability, service initiation/termination timeframes and conditions, mobile number reassignment or reuse, etc. The directory service requirements would need to be aligned with local regulations.

4.4.2 Rationale

If a common directory service were not created, the sending DFSP would need to ask every other DFSP if they held the target phone or account. This broadcast traffic would consume considerable resources from all participants, and the number of requests would grow exponentially as more networks are added.

Similarly, if each DFSP built their own directory of external phone numbers or accounts, and other partners were not obligated to provide updates, the information would quickly be out of date. All partners would have to create shadow copies of accounts or phone numbers on all other partner systems, and agree to share that information. As a result, some regular synchronization with the actual account owner’s system would need to be performed, adding complexity for all partners.

In each scenario, additional resources would be needed, impacting the ability of the systems to scale. Thus, it makes sense to house or access a common directory service.

4.4.3 Requirements

1. The directory service **shall** enable authorized participants to determine the digital money provider associated with a phone number (i.e., MSISDN), account ID, or any other agreed common alternate ID.

Rationale: This is the minimum functionality needed to enable a sender to identify the recipient system.

2. The directory service **shall** permit only a single mobile wallet money provider to be associated with a uniquely identified account.

Rationale: The IST would be unable to accurately route messages if multiple providers were associated with a single account (identified to the system-wide requirements for a unique identifier)

3. If a mobile wallet money provider attempts to register a unique account that is already associated with another provider, the directory service **shall** reject the request, and provide an error message indicating the information provided is already registered with another provider.

Rationale: Providing an error message will help the sender resolve the issue.

4. The directory service **should** enable authorized participants to determine the account holder name associated with a phone number (i.e., MSISDN), account ID, or any other agreed common alternate ID.

Rationale: The reference model is a push payment system. Payers will need some confirmation that the payee information entered at transaction initiation is accurate. The cross-referenced information enables the payee to receive a secondary attribute of the target payee for confirmation. If not provided by the directory service, each DFSP must support such an inquiry.

5. The directory service **shall** return the name of an account owner when the account owner's public identifier is presented as part of a financial transaction.

Rationale: A merchant trying to send a request for payment, or a payer initiating a push payment, needs some way to confirm the recipient is the expected person when an ID number is presented by the buyer or entered by the payer. This reduces the likelihood that a transaction will be sent to the incorrect party.

Note: This is a privacy concern, as the transaction initiator could use the system to associate names with identifiers and phone numbers, making it easier for a fraudster to trick someone into sharing even more details, and eventually amassing enough information to perpetrate a theft.

6. Alternatively, the directory service **may** provide affirmation that two or more pieces of information correlate (e.g., name and phone number, phone number and bank account, mobile money account number and phone number), providing increased assurance that the target account is the intended account without disclosing information not provided by the sender.

Rationale: In locales where disclosing the name of an account holder in response to submission of the account ID or phone number is undesirable, a non-disclosing model ensures only the association is disclosed and no other information is provided to the sender than that which they already possess.

7. The directory service **shall** provide an error response if the presented challenge data cannot be located in the service.

*Rationale: Input errors are inevitable, thus some inquiries will not match any records and the sender **must** be notified so the information can be reviewed and an alternative action determined.*

8. The directory service **may** track whether an entity (person or organization) is prohibited ("blacklisted") from transacting on the system.

Rationale: The payment ecosystem will have many such blacklists as part of regulatory Anti-Money Laundering/Combating the Financing of Terrorism (AML/CFT) requirements, fraud controls, etc. Our prototype chose to implement an indicator within the directory service, though the capability would appropriately reside within a separate Fraud and Risk Management Service.

9. The directory service **may** provide the entity blacklist status in response to an inquiry. Note: Due to privacy constraints, the actual response **should** be a generic message to contact customer support.

Rationale: The data will be integral to any risk management methodology designed to block transactions with bad actors, typically needed during account setup.

10. The directory service **may** provide the current status of any identified entity in response to an inquiry.

Rationale: Knowing the status of the target entity will enable the inquirer to perform an alternative action in the event the status is unacceptable, potentially improving the overall usability of the ecosystem components. For example, if the system responds that a payee account is currently inactive, the payer can request alternative payment options instead of sending funds to a suspended or blocked account. The ecosystem may allow the DFSP to provide the status in an error response if the payment message is not actionable.

11. The directory service **shall** provide an update mechanism, allowing designated authorized participants to create, update, or delete the information contained therein.

Rationale: The data need to be maintained to ensure durability of the service and ongoing usability by the participants.

12. The directory service **shall** enable an authorized administrator to update the information contained within.

Rationale: Internal and external authorized parties will need to maintain the data.

13. The directory service **should** provide a set of defined APIs to enable standardized inquiry or update of the data contained therein.

Rationale: This makes the service more consumable by the participants, and reduces support and maintainability expense over time.

14. The directory service **should** provide a user interface enabling management of the service and data.

Rationale: The data needs to be maintained.

15. The directory service **should** permit a participant to update some or all of its records in a batch process.

Rationale: This enables a partial or full refresh of the data.

16. The directory service **shall not** allow service providers to update records of other providers.

Rationale: Basic control to improve data integrity.

17. The directory service **must** be highly available.

Rationale: This is a critical enabling piece of the digital payment ecosystem. If it is not available, the ecosystem routing capability will be degraded or potentially halted.

18. The IST **shall** return the account holder name in response to a request by the payee's system.

Rationale: The IST must ultimately route the message and response. The detailed process would interact with the directory service.

4.5 ENFORCE ACCOUNT LIMITS

4.5.1 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 *know 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.

Tiered KYC in the Prototype

For the purposes of demonstration, tiered KYC was implemented at the switch level and embedded in the IST prototype. This function is normally performed at the account holder level (i.e., DFSP or bank), as those organizations have the direct relationship with the end user. While we are not aware of this scenario being used in practice, should a regulator require system-wide controls centered on the individual, a central switch would be a logical place to implement the control as it has visibility across account providers.

The capability is included here as the prototype provides a basic level of centralized KYC capability. In practice, this consolidated KYC enforcement capability creates many dependencies on information flow between participants (e.g., all DFSP "on-us" transactions would need to be reported to the switch) that would increase switch complexity and message volume, and likely the fragility of the switch.

The following requirements describe tiered account limits functionality that could be utilized at the switch- or account level. It is important to note that the system will need to be flexible in handling cases when limit rules need to be overridden to support special situations. To be effective, exceptions would need to be minimized.

For example, a consumer has an account balance of 50 local currency units and a maximum account value of 100: a trusted government payer sends a 60-unit support payment. Should the payment be rejected, the maximum account value be increased (permanently or temporarily), or only a partial deposit be accepted? A supporting system rules engine will need to address whichever scenario the participants ultimately agree is appropriate.

4.5.2 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.

4.5.3 Requirements

These requirements represent *thick* switch functionality that may be more practically applied to DFSP and bank participants, and include capabilities that could require significant effort to implement. As stated previously, account-limiting controls are needed at the DFSP and bank level, with the IST providing an aggregating function across accounts when regulation requires an entity level view (e.g., natural person) across the entire payments ecosystem.

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 IST **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 IST **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 behavior occur.

4. The IST **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 US$10,000 between accounts than to send US$10,000 in payments to a third party.

5. The IST **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 IST **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.

7. The IST **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.

8. The IST **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.

9. The IST **shall** allow individual TACRs to be assigned a processing priority.

Rationale: Enables hierarchical rules processing.

10. 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.

11. The IST **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.

4.6 DETECT TRANSACTION FRAUD

4.6.1 Description

Fraud in digital payments is a very real concern, as the payments are designed to be irrevocable. To reduce this risk, several layers of mitigation exist to weed out bad actors (KYC, strong authentication), limit potential losses (tiered account limits), and reduce external access to accounts (only push payments supported).

To a great extent, the front line responsibility for preventing fraud lies with the DFSPs, requiring them to verify their agent and customer identities at account setup, provide secure communication with the mobile device, limit user capabilities/balances based on evaluated risk, monitor for abnormal payment behavior on their accounts, etc.

However, the DFSP can only see full details of transactions on their network. They cannot see transactions or potential fraud schemes playing out on other provider networks, or correlate activities that span multiple providers.

As the central switching function in the digital financial transaction ecosystem, the IST is uniquely positioned to enable the analysis of all transactions between providers. The ability to detect system-wide fraud could be enhanced if the ecosystem rules required intra-provider transactions be mirrored to the IST for inclusion in the fraud system database.

While the IST could provide its own fraud detection analysis (e.g., identify payments not following normal patterns), it is likely that external partners will have greater expertise in performing that analysis. Thus, the IST **should** be able to redirect a copy of specific transaction sets (e.g., P2P payments) to a partner for analysis, and then be able to receive notification of any suspected fraud. That notification may then be routed back to the affected partners for action.

If actually blocking the fraud in real time (i.e., suspending the payment clearing) is required, the switch will need to be able to support fraud detection, reporting, escalation, and resolution services as part of the inline transaction routing capability.

Finally, the IST **should** support many such fraud partner services, to allow choice within the network and to enable advancements through innovation.

For demonstration purposes, the prototype includes a basic flag to indicate if the account holder is blacklisted. The expectation is that an actual production implementation would include much broader fraud detection and mitigation capabilities. Rationale

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

4.6.2 Rationale

Allowing third-party partners to provide fraud services or software at the switch level enables detection of fraud across the entire ecosystem, identification of inter-provider schemes, and the sharing of fraud trends that have affected only some providers.

By supporting external fraud detection services or software at the switch level, mobile wallet providers could potentially outsource that work to specialized partners or vendors for better results at a lower cost. This would provide an incentive for multiple providers to compete on both price and capability, benefitting all.

In the proposed pro-poor model, all participants would agree to share appropriate information to help reduce overall ecosystem fraud.

4.6.3 Requirements

1. The IST **shall** provide the ability to route any transaction to a fraud detection service for risk evaluation.

Rationale: Transactions cannot be analyzed if they cannot reach the analysis service.

2. The IST **should** allow fraud analysis to be performed serially or in parallel with the primary transaction routing process.

Rationale: Payment systems may value transaction throughput time over risk avoidance, or vice versa. The selected implementation in a particular environment would be dictated by regulations defining who is responsible for any loss.

3. The IST **should** support concurrent integration to multiple fraud detection services.

Rationale: More options are better to enable innovation in the marketplace.

4. The IST **should** support the ability to selectively route transactions to one or more desired fraud detection services.

Rationale: The ability to route the same transaction to multiple services enables fraud service effectiveness evaluation.

5. The IST **may** support the ability to selectively route transactions to different providers based on criteria including percentage of transaction volume, random selection, round robin, type of transaction, value of transaction, account type, account risk score, transacting sender, transacting receiver, etc.

Rationale: Transactions have varying levels of risk, and certain providers may be stronger in detecting fraud in one type of transaction than another provider.

6. The IST **shall** provide the ability to notify stakeholders if a fraud condition is detected.

Rationale: Notification provides the ability for stakeholders to take action to mitigate risk.

7. The IST fraud notification **should** include enough detail (e.g., transaction id, condition triggering the notification) so the affected stakeholders can determine an appropriate course of action to mitigate the condition.

Rationale: Detail is needed to make the notification useful in resolving the issue.

8. When a fraud condition of sufficient severity is detected, the IST **shall** either complete the payment transaction as directed or terminate the transaction with an error status.

Rationale: Completing or terminating the transaction ensures the payee and payer can conduct business or determine if alternative action is needed.

4.7 ON-BOARD TRANSACTION PARTNERS

4.7.1 Description

For the IST to be effective at scale, it must be connected to the vast majority of the digital payment ecosystem participants. This implies the IST must provide an efficient and reliable mechanism to establish a functioning interface and well-defined relationship with those partners.

4.7.2 Rationale

If partners cannot be connected to the IST, it will not be able to facilitate transaction routing. If the process isn't formalized, errors in setup and configuration will be higher, partner expectations may be misaligned, and the overall level of friction will be higher, increasing the costs of operation.

4.7.3 Requirements

1. The IST **shall** allow partner interfaces to be set up independently of the production status of the specific integration.

Rationale: Staging partners in the system without enabling production or test access allows for administration outside of specific time constraints.

2. The IST **should** keep all non-production transactions logically and physically separate from production transactions.

Rationale: Best practice for financial services. Segregation of production and non-production traffic reduces likelihood that production resources will be consumed for non-production processing.

3. The IST **shall** provide an error response of sufficient detail needed to identify the root failure cause of an authorized transaction that is not successfully processed.

Rationale: Error responses are integral to troubleshooting when processing does not complete as expected.

4. The IST **must** provide credential management capability to control access to processing capabilities.

Rationale: If credentials were not used, there are limited alternative ways to control unauthorized system use.

5. The IST **should** provide a formal API for integration with third-party systems.

Rationale: An API provides partners with flexibility in how they integrate switch routing into their systems, promotes consistency across partners, reduces interface development learning curve for partners, reduces interface support effort for the switch provider, and more.

> a. If an API is provided, the IST **shall** accept API messages from authorized parties.
>
> *Rationale: If a party is authorized (i.e., authenticated, and the account is in good standing or active), then its transactions **should** be processed.*
>
> b. If an API is provided, the IST **shall** ignore API messages that are not authorized.
>
> *Rationale: Ignoring the message instead of responding with an error avoids using resources to processed unauthorized messages.*
>
> c. If an API is provided, the IST **shall** allow logging of the messages.
>
> *Rationale: Logging may be necessary to support troubleshooting new partner setups, to analyze traffic details, or to provide data for forensic analysis.*

6. The IST **may** implement a software development kit (SDK).

Rationale: Providing an SDK can improve distribution and utilization by reducing the level of skill and coding needed to integrate with the IST.

7. The IST **should** allow partner interfaces to be enabled or suspended through an administrative interface.

Rationale: Enables staging on the environment without live processing, and the ability to disable an interface if problems (e.g., DFSP compromise) arise.

8. The IST **shall** keep a registry of all participants (i.e., transaction partners authorized to interact with the IST).

Rationale: The system needs some listing of participants to provision access.

9. The IST **shall** classify participants by role (e.g., DFSP, merchant, agent, bank)

Rationale: Classification provides for management or provisioning of similar participants in a controlled manner.

10. The IST **should** enforce transaction velocity and transaction magnitude controls on participant transaction messages.

Rationale: These are key controls to reduce potential fraud, and to protect against system errors or data entry issues that might impact the participant's ability to process transactions. For example, if a runaway process at a participant repeatedly sent a payment message, it could potentially deplete the participant's account and shut down the service. Alternatively, a single improper payment with a very large (incorrect) payment would have the same effect.

11. The IST **should** provide the ability to limit the type of transaction message that a participant can send and/or receive.

Rationale: Enabling control of message types at the participant level reduces the opportunity for abuse or fraud, and enforces the integrity of the ecosystem.

12. The IST **shall** allow an administrator to enable or disable participant access and processing capability through an administrative user interface.

Rationale: Enables staging of partner accounts or stop loss control in the event of issues.

13. The IST **should** store participant contact information for billing, technical and business functions.

Rationale: Enables administrators or support personnel to quickly identify method to contact participant if needed.

14. The IST **should** log all participant configuration changes from creation through deletion and including what changed, when it changed, and who changed it.

Rationale: Supports forensic analysis for issue resolution or auditing.

4.8 ENABLE TRANSACTION COMMISSIONS

4.8.1 Description

The payments ecosystem is a complex interaction of stakeholders with varying needs and expectations. Some may be motivated by a sense of greater good with a goal of lifting others out of poverty, while others perform activities in the ecosystem to generate income. Regardless of the motivation, the ecosystem **must** be financially viable or it will collapse. Thus, it is reasonable to expect that some activities would not occur at the required scale unless a participant was financially compensated to perform the activity. In banking, the practice of interchange payment provides that incentive.

A key principle in the model is that added transaction expenses must be transparent (i.e., visible) to the stakeholder who is directly paying the fee or charge. This does not necessarily mean that the end user will see all fee details associated with a transaction, as ecosystem partners have the choice to absorb the individual expenses or pass them on to the benefitting participant. But where the end user is paying the fee, they should see the fee details at the time of payment.

Typically, the account provider (e.g., bank or DFSP) will manage customer-facing fees and detail the fees in the payment messages transmitted to other partners. In that scenario, the IST might only forward the message without interacting with the fee detail. The same is true for any governmentally defined tax or fee related to digital payments.

Fee calculation might also be imposed and collected at the switch level, potentially simplifying the complexity of the partner systems, while increasing the complexity of the centralized switch (i.e., making the switch "thicker").

To inform and foster discussion, the prototype includes support for common fee/commission structures imposed at the switch level. The requirements below include and extend those prototype capabilities, supporting the ability to collect a commission, charge a fee or levy a tax to compensate participants for the work they may perform in fulfilling some type of transaction. The requirements support the potential need for multiple types of fees/commissions, including a flat fee or a percentage of the transaction amount. These fees may be paid at varying levels to more than one role/participant with an interest in the transaction. By default, the fee may be zero, but the assumption is that some transaction activities will be greater than zero.

As relationships between ecosystem members may be very complex, future options would include the opportunity to define differing charges for the same transaction type depending upon the specific instance or classification of a particular partner. For example, one environment may have many banks, with some having partnerships with digital financial services providers. In one instance, Bank A is partnered with Digital Financial Services Provider A, but has no relationship with Digital Financial Services Operator B. If a consumer uses DFSP A to transfer funds from an account at Bank A to another person, there is no fee imposed by Bank A. Alternatively, if the same consumer uses DFSO B for the same transfer, Bank A may impose a surcharge.

4.8.2 Rationale

To enable financial inclusion, the IST must support ubiquity of digital payments. This level of acceptance requires a financially viable ecosystem, where participants are reasonably rewarded for the critical services provided.

As transactions may be complex, different participants may have varying cost structures, operating expenses, or income expectations. Thus, the system needs the flexibility to apply known and future expense models in the context of transaction processing.

4.8.3 Requirements

1. The IST **shall** provide the capability to charge a fee for performing any transaction flow.

Rationale: A fee may be required to recover costs or incent transaction partners to participate.

2. The IST **shall** provide the ability to add one or more surcharge amounts to any transaction step.

Rationale: Any step in a larger transaction flow may include a surcharge amount. Further, multiple participants may be independently compensated in a single step. For example, the participant performing the task may charge a flat fee for the activity and have a second charge as a percentage of the transaction to support a tax model.

3. The IST **shall** calculate a transaction fee as the total of all transaction step surcharge amounts within a complete transaction flow.

Rationale: Fees are cumulative over the life of the transaction.

4. The IST **shall** enable surcharge amounts to be dependent upon the specific entity performing the step, or the class of which the entity is an instance.

Rationale: All banks may be required to charge a specific surcharge by regulation, while some mobile operators may choose to forego a fee charged by a competitor for the same activity.

5. The IST **shall** support positive and negative transaction fees.

Rationale: Participants may want to incentivize certain transactions by subsidizing the expense directly. For example, a bank may rebate a transaction fee that was paid.

6. Logging: The IST **shall** log all fees for analysis and reporting.

Rationale: General Auditability requirement.

7. Logging: The IST fee logs **shall** include the detail needed to see exactly who charged or paid the fee at each transaction step.

Rationale: General Auditability requirement.

8. Reporting: The IST **shall** enable any participant to report out historical fees paid or charged within the context of any rules limiting visibility of the transaction step detail.

Rationale: Fee transparency may be limited to the amount.

9. Reporting: In all cases, the total amount paid **shall** be visible by the fee payer, regardless of any other visibility restrictions.

*Rationale: A non-negotiable principle is that fees **shall** be transparent.*

10. The IST **shall** support a transaction step surcharge as a flat fee.

Rationale: Common fee structure.

11. The IST **shall** support a transaction step surcharge as a percentage of the total transaction amount.

Rationale: Common fee structure ad valorem ("according to value").

4.9 PROCESS BULK PAYMENTS

4.9.1 Description

Governments, charitable organizations and large private-sector employers frequently need to distribute high volumes of payments to large numbers of varied beneficiaries. These payments might include payroll to employees, financial support in the form of retirement or welfare payments, agricultural subsidies, or payments to vendors. For these organizations, cash payments are inconvenient and undesirable, as they increase risk due to loss, theft, and corruption, and add expense for distribution and handling.

Beneficiaries in developing countries face additional challenges, as they:

- May not have a bank account to receive digital payments.
- May have limited access to the formal banking system or to bank branches in rural areas.
- May lack formal identification and be challenged to prove their identity.
- May not have a consistent physical address to receive payment.

Fortunately, the rapid growth of mobile phone services in developing countries increases the likelihood that individual recipients will have a mobile phone, a SIM with access to a phone, or a local digital money agent. The potential intersection of payees with the population of mobile wallet holders creates a significant opportunity for bulk payers to reach a much larger set of payees with digital payments, utilizing the low-cost mobile distribution channel as an alternative to legacy payment methods such as cash.

How the IST can help

As the IST would provide centralized switching of payments to many DFSPs and their constituent mobile wallet users, a bulk payer could interface directly to the IST and allow the IST to handle distribution to the participating DFSPs, avoiding the need to integrate to all of the DFSPs directly.

While the high-volume payer could send individual payment transactions, it is much more efficient to bundle a large number of transactions and send them as a single batch. Fortunately, organizations that routinely provide payments to large numbers of recipients (e.g., governments, NGOs) typically have sophisticated payment systems capable of generating a single batch file or streaming transaction sets containing the instructions for many individual beneficiary payments.

The IST must be able to receive these bulk payment sets and decompose them into individual transactions for routing to the payee's DFSP. This "de-bulking" process typically also provides the ability to *throttle* (slow down) the conversion to individual payments, allowing the system to spread the processing load over a longer timeframe, and avoid impacting other transaction processing.

Accepting that bulk processing can be good for all participants, the IST should be able to send either individual transactions to the DFSPs, or re-bundle all of the payments destined for the specific DFSP into an outbound bulk payment file (i.e., "re-bulk") and allow the DFSP to de-bulk on the DFSP's system.

The process would need to be repeated in the opposite direction, allowing the IST to aggregate and return any status messages or error conditions from the DFSPs to the bulk payer. Given the additional needs to de-bulk, re-bulk and aggregate responses, a separate specialized *bulk payment service* might be implemented to avoid overcomplicating the core IST functionality.

The IST prototype implemented a bulk payment service within the thick switch for functional demonstration. Whether as a separate service or as part of the IST, the bulk payment service will need to:

- Securely receive bulk payment files or streamed transaction sets (e.g., XML data feeds) from the bulk payer system.
- Create the necessary individual or re-bulked payment transactions, properly targeting each beneficiary recipient's account with the allocated funds.
- Forward the individual or bulk messages to the core IST for routing to the DFSP hosting the account/mobile wallet.

The core IST will need to provide individual response messages indicating success or failure, relying on the bulk payment service to aggregate, track, and report on the overall health of the batch to the sender. The switch and bulk service would create the appropriate log entries and reports to allow auditors to confirm that payments were properly disbursed and the recipient's account credited.

The IST will also need to handle situations where the intended recipient is not able to accept a digital payment.

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.

4.9.2 Rationale

Providing support for batch payment processing, whether as an interface to an external service or component module, enables the IST to automatically process payments from large payers, thus adding a large number of "off-us" transactions to the payment ecosystem. This capability increases the overall usage of the system and facilitates increased membership, as payment beneficiaries are incented to sign up for digital financial services to gain better access to the payments. This is a key use case for governments; as discussed in *The Level One Project Guide*, government adoption of the system by government is a key condition of success for DFS System deployments, government adoption of the system is a key condition of success for DFS System deployments. This not only drives initial transaction volume (thus immediately lowering costs), but it's also a visible endorsement of the payment system.

For payers, it provides the opportunity to reduce the costs and risks associated with cash payments, including fraud, corruption, theft, and logistical expense of cash distribution.

Benefits to beneficiaries include access to funds at an increased number of non-bank, receipt of their payments without a specific address, and reduced risk of loss or theft of cash.

4.9.3 Requirements

NOTE: This is a thick switch function that may be alternatively provided by some third-party system or service connected to the IST core switching engine.

To facilitate payments from large payers to users of the digital financial system, the IST may need to support interfaces to specialized services that perform the non-core routing capabilities (e.g., directory services, fraud and risk management, bulk payment processing).

For clarity, the requirements are broken out between IST and the specialized bulk payment service:

1. The bulk payment service **shall** support receipt of bulk payment **files** containing payments for multiple recipients.

Rationale: Incents large payers to use the digital financial system.

2. The bulk payment service **shall** support receipt of streamed transaction sets (e.g., POST method of an XML data structure) containing payments for multiple recipients.

Rationale: Incents large payers to use the digital financial system.

3. The bulk payment service **shall** decompose bulk payment files and streams and either:

   a. process as individual payment transactions, or

   b. re-bulk in to a batch payment set where all transactions are destined for the same DFSP

Rationale: Required to route the contained transaction to multiple recipients and support efficient transmission and processing by the DFSP

4. The bulk payment service **shall** identify processing exceptions.

Rationale: If exceptions are not identified and tracked they cannot be easily resolved. This may include cases where the recipient DFSP is not available, the recipient phone number or account does not exist, the recipient mobile wallet is not configured for the phone number, etc.

5. The bulk payment service **shall** notify identified stakeholders (e.g., payer, DFSP) when processing exceptions occur.

Rationale: Notification is required so the appropriate person can take action to resolve the exception.

6. The bulk payment service **shall** include processing exception notifications indicating the specific error condition encountered or an indication that the error reason is unidentified.

Rationale: Providing detailed error codes improves troubleshooting ability and facilitates faster and more accurate resolution.

7. The bulk payment service **shall** provide reporting of batch processing details, whether related to success or failure, to the payer.

Rationale: It is likely that some transactions will fail for some reason (e.g., invalid recipient phone number) and thus the payer needs the ability to identify and work exceptions.

8. The bulk payment service **should** provide the ability to aggregate batch processing response detail messages for return to the payer as a batch transaction.

Rationale: Efficient processing improves scalability of the overall ecosystem.

9. The IST **shall** support a mechanism enabling individual transactions to be tracked to a parent batch group.

Rationale: While the core IST may not decompose the payment batch or specifically report the aggregate response/health of the batch, it needs to retain the association between the batch and the individual transaction in some way. This association may be directly supported by attaching an identifier tag provided by the batch processor, or indirectly by responding to each payment message with the unique transaction ID, with the batch processor being responsible for associating the transaction ID with the batch.

10. The IST **shall** confirm the payer settlement account has sufficient funds to meet the maximum potential cumulative payout of the contained individual beneficiary benefits or the defined maximum for the total batch.

Rationale: Ensuring the payer has sufficient funds is a primary pre-condition in any push payment.

11. The IST **shall** reject component transactions where named participants are ineligible to transact.

Rationale: Payments must be subject to fraud and AML/CFT checks, and blocked where the participant is deemed an unacceptable recipient.

12. The IST **shall** reject any component transactions contained within the bulk payment file that do not include the minimum required data fields.

Rationale: Incomplete records must be rejected to enable resolution by the payee.

13. The IST **shall** reject any component transaction contained within the bulk payment file if the beneficiary phone number or account number is unassigned or not valid.

Rationale: This would likely be due to incorrect information, and would require correction and resubmission by the payer.

14. The IST **shall** reject any component transaction contained within the bulk payment file if the beneficiary identity fails validation (e.g., name and national ID do not match)

Rationale: This would likely be due to incorrect information, and would require correction and resubmission by the payer.

15. The IST **shall** retry distribution of any component transactions contained within the bulk payment file on a defined retry period or when the failure condition is resolved, if it failed because:

a. No mobile wallet account is associated with the phone number.

b. The DFSP was not reachable.

c. There were other recoverable errors that do not require changes to the submitted information.

Rationale: Defining a retry period allows for automatic completion or improved distribution where the reason for failure can be corrected (e.g., beneficiary signs up for a mobile wallet upon notification of available benefit, a DFSP comes back online)

16. The IST **should** have a minimum retry time. (e.g., no less than 15 minutes).

Rationale: High-frequency retries could degrade or overload processing capability without a defined and enforced safe floor limit.

17. The IST **should** enable a system administrator to manually retry or trigger distribution.

Rationale: There will likely be processing scenarios (e.g., one DFSP is unavailable) that require manual intervention to clear backlogged transactions.

18. The IST **shall** discontinue retries when a defined maximum retry limit is reached or processing completes successfully.

Rationale: If there were no retry limit, failed transactions could increase forever, potentially consuming enough system resources to degrade or prevent transaction delivery.

4.10 MANAGE VOUCHERS

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.[7] 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.[8]

The demonstration IST prototype includes a method for distributing *subsidy vouchers* through the mobile channel. The voucher is effectively a digital coupon that can be used at pre-approved merchants to purchase a selected set of products (e.g., fertilizer, seeds). The function does not attempt to provide sophisticated point-of-use control (e.g., limited to specific products), as widespread sophisticated inventory management and point of sale systems may not be prevalent in the target countries. Instead, the merchant is relied upon to follow the rules when redeeming the voucher to ensure it's used only as intended.

[7] 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.

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

We chose to directly integrate voucher management with the IST, but a separate service might aggregate responses, provide reporting and analytics to the benefactor, or otherwise handle non-routing aspects.

As envisioned in the prototype, a voucher provider would setup a voucher batch containing a set of individual vouchers targeted at specific recipients. The batch would be uniquely identified for tracking purposes and include common constraints affecting all vouchers in the batch, including:

- Total available funds.
- Percentage value of the total sale that the voucher will cover.
- Merchant locations where the voucher may be used.
- Type of goods that may be purchased.
- A common notification message for recipients.

Each voucher in the batch would be assigned to a specific beneficiary (i.e., designated consumer) and include the value of their voucher, its expiration date, and approved merchant(s) for redemption.

CIO Note: A similar solution was implemented in Nigeria. In that implementation, the consumer designated a preferred merchant with the benefactor prior to voucher creation and distribution. This one-to-one relationship is a simpler case than implemented in the prototype, where many eligible vendors might be designated for a single voucher. However, it is generally easier to build support for one-to-many relationships from the start than redesign the system when conditions change—in any event, one-to-many relationship designs support one-to-one configurations. However, in a one-to-many implementation the database cross-reference tables are potentially much larger, as each entity must be related to the voucher.

As in the case of the bulk payment processing, the *voucher management system* would process the batch instructions on command, iterating through all contained records to send notification to the DFSP of the beneficiary and, potentially, the merchants. Any delivery exceptions would be tracked and made available to the sender (i.e., benefactor or delegate) for exception resolution.

The vouchers are converted into payment instructions only when used for a purchase meeting the defined constraints. This implies that the system will need the ability to cancel or retract a voucher if the batch funds are depleted or the batch or voucher expires.

Alternatively, the funds may be transferred at the time of voucher distribution to be held in escrow by the DFSP. However, some business arrangement would be needed to recover unused funds, as the model payment system does not permit payment reversal.

4.10.2 Rationale

Vouchers are an important tool for providing support payments, as they give the donor better targeting and visibility into how the funds are actually used. Vouchers have the potential to greatly decrease leakage and improve the utilization of the provided funds for their intended purpose. The sophistication of the operating model is limited by the systems capabilities of the merchants.

4.10.3 Requirements

The voucher distribution process is very similar to the bulk payment distribution process, except that only notifications are sent as part of the initial bulk voucher distribution process, as the actual payment is performed only when the voucher is redeemed. As such**, the requirements of Section** *Error! Reference source not found.***,** *Error! Reference source not found.* **section apply, as do general message resiliency requirements of *Section*** *Error! Reference source not found.***,** *Error! Reference source not found.*.

Note: It is important that the IST **does not** communicate with the end-user mobile wallet, but relies on DFSPs to process and forward any notification messages to (and responses from) the consumer's mobile wallet.

1. Voucher beneficiaries **shall** be notified when a new voucher is created.

    a. The voucher management system **shall** generate notification messages and deliver to the IST for eventual delivery to targeted *beneficiaries* when a voucher is distributed for their use.

    Rationale: Notifying the recipient reduces need for the beneficiary to check and see if a voucher is available.

b. The voucher management function **may** send notification messages to the IST for eventual delivery to targeted merchants when a voucher is distributed for use at their business.

Rationale: Notifying the merchant potentially enables them to market or proactively advocate the use of available vouchers.

c. The IST **shall** route voucher notification messages between the voucher management system and the identified DFSP of the beneficiary and/or merchant.

Rationale: The IST doesn't directly communicate with the beneficiary or merchant, but rather with their mobile wallet provider.

d. The voucher management system **shall** notify participants (e.g., DFSP) if an outstanding voucher is retracted for any reason (i.e., sent by mistake, total funds exceeded, voucher expires, batch expires)

*Rationale: The nature of the voucher is that it **can** be retracted. Notifying the recipient eliminates the expectation that the voucher is still available to use.*

2. The voucher notification **shall** identify the recipient, donor/funder (e.g., government, NGO), one or more approved merchants, and any use constraints (e.g., maximum value, percentage of purchase value, expiration date, eligible class of products)

Rationale: The recipient should have full visibility into the intended use of the voucher so they can plan accordingly.

3. The IST **shall** notify the voucher provider of any individual voucher notifications that cannot be delivered.

Rationale: Delivery failures will potentially occur for multiple reasons (e.g., recipient has a mobile phone but no mobile wallet). Thus, the provider needs to receive notification of exceptions so exception processes can be activated.

4. The IST **may** send voucher notifications as they are received, or collect and send as a single batch, as agreed upon with the messaging partner.

Rationale: Reduces messaging overhead on networks with limited bandwidth.

5. The voucher management system **shall** resend notification of any suspended vouchers to the beneficiary's DFSP if the beneficiary registers a mobile wallet account.

Rationale: Upon clearing the specific exception case where the beneficiary had a phone but not a mobile wallet, the IST voucher notification process can be automatically continued.

6. The voucher management system **shall** process voucher payments (payer to merchant) at the time the voucher is redeemed.

Rationale: The voucher notification is converted to a payment by the action of use. In some cases, vouchers may expire or be retracted before use, so it is improper to consider the voucher as a transfer of value until redeemed.

7. The voucher management system **shall** only complete a payment within the defined constraints of the voucher (e.g., approved merchant, within maximum value, prior to expiration or cancelation, for credit to designated beneficiary, funds availability).

*Rationale: The unique value proposition of the voucher mechanism is that its use by the recipient **can** be constrained to align with the intent of the donor.*

8. The voucher management system **shall** support incremental expenditure of voucher funds until constraints apply (e.g., value exhausted, poll funds exhausted, expiration reached)

Rationale: This provides more flexibility on the use by the beneficiary, allowing them to purchase just what they need and make purchases at a later date, until the value of the voucher is expended or the voucher is retracted.

9. The voucher management system **may** link any copayment transaction to the voucher to provide evidence of compliance with the voucher terms of use (i.e., constraints).

Rationale: Linking a copayment transaction provides demonstration of compliance with the terms of use for the voucher.

10. The voucher management system **may** reject payment requests if a copayment transaction is not provided in compliance with the voucher's terms of use.

Rationale: If it is possible to tie copayment to voucher use and require the copayment first. The system should then reject payment requests for vouchers that are missing the copayment.

11. The voucher management system **shall** notify the benefactor if a voucher is utilized for payment outside of the voucher's terms of use (e.g., no linked copayment when copayment is required).

Rationale: The benefactor should have visibility and rapid notification of non-compliant voucher use so that issues can be quickly identified and potentially investigated and remediated.

4.11 PROVIDE SETTLEMENT INSTRUCTIONS

4.11.1 Description

Settlement, the exchange of value (i.e., funds in the national currency) between the transacting parties, is typically performed through the formal national payment systems. A goal of the IST is to ensure participants can settle funds in a manner meeting their risk tolerance.

Same-day settlement is a design principle of *The Level One Project Guide:*

> The [DFS] 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.

To demonstrate this principle, the prototype includes an internal capability that simulates net settlement among participants on a rolling, same-day basis, tracking how much each participant owes the others. In practice, the IST would provide settlement instructions to formal financial institutions that would, in turn, manage the transfer of currency between participants. The timing and frequency of the settlement initiation process should be dynamic, supporting multiple intra-day payments as needed to reduce participant risk.

Alternatively, participants could directly interface with their financial institutions to perform cash management activities outside of the IST, or the IST could indeed provide settlement between participants as demonstrated in the prototype. However, if the IST provides settlement services, the expectation is that regulatory scrutiny of the IST would be consistent with that imposed on banks or other formal financial institutions that actually hold currency.

Given the varying needs of potential participants, initiation of the settlement process could be performed based on several triggering conditions:

- Manual activity: allows for settlement on demand to support exception needs of participants.
- Transaction count threshold is reached: controls number of transactions impacted if issues.
- Settlement amount threshold is reached: controls total value impacted if issues arise and is used for risk management and mitigation.
- Scheduled time reached: provides predictability for all participants.

4.11.2 Rationale

Same-day settlement reduces the exposure of the transacting parties in the event of failure of one of the parties. Further, it improves liquidity by freeing up funds more frequently, which in turn lowers risk and reduces costs. Frequent intra-day settlement further reduces this exposure.

4.11.3 Requirements

Note: These requirements represent thick switch capability.

1. The IST **shall** provide settlement instructions on at least a same-day basis.

Rationale: Reduces exposure to participant failure and improves liquidity.

2. The IST **may** provide settlement instructions on a per-transaction basis.

Rationale: Significantly reduces exposure to participant failure and improves liquidity, though increasing potential fraud loss from a compromised account.

3. The IST **should** support multiple settlement instruction initiation trigger conditions including, manual initiation, unsettled transaction count limit reached, unsettled value limit reached, and scheduled settlement time reached.

Rationale: Sophistication and needs of varying participants might require more flexibility for settlement than a single option.

4. The IST **should** allow participants to agree, within the regulatory and legal requirements of the country, on how to settle and trigger settlement between those partners under the agreed conditions.

Rationale: Provides greater opportunity to accommodate participant needs than a one-size-fits-all approach. Depending on participant risk appetite and needs, this could increase adoption by allowing agreement on settlement timing between specific participants.

4.12 REPORTING AND DASHBOARDS

4.12.1 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. 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.

In the case of the IST, the stakeholders may be internal or external users of the system. Thus, the expectation is that the needed information will be accessible both internally and externally.

CIO Note:Typically, reporting is performed against a purpose-built data warehouse and not the production transaction system. This method ensures reporting activities, which may be resource intensive, do not impact production transaction processing. The reporting system data may be pushed or pulled from the production system, but generally the production system data is read-only, and not updated from the reporting system. The reporting data might also lag production, with updates to the reporting data performed only during off-peak hours when system usage is low, to minimize impact of the data extraction.

4.12.2 Rationale

Without some reporting capability, the system's stakeholders would be 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.

4.12.3 Requirements

1. The IST **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 easy analysis.[9]

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

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

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

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

Rationale: The prototype includes some basic reporting capability.

4. The IST **should** provide pre-configured ("canned") reports for common business process needs.

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

[9] *Principles for Financial Market Infrastructures*, International Settlements and International Organization of Securities Commissions, 2012

5. For basic reporting, the IST **should** enable data targeting by timeframe, activity, and value.

Rationale: Simple filters are required to selectively retrieve data.

6. For basic reporting, the IST **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.

7. For basic reporting, the IST **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.

8. The IST 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.

4.13 BIOMETRIC REPOSITORY AND VERIFICATION SERVICE

4.13.1 Description

A key need in operating a risk-managed payment ecosystem is the establishment of identity of the people performing transactions. This can be a challenge in populations that might lack formal identity establishment/assurance documents from an authoritative trusted party. The inability to establish identity can be a primary barrier to financial inclusion. One solution that does not require any documentation, but only the physical presence of the individual is biometric verification.

Biometric verification provides the ability to confirm an individual's is associated with the account through the following process:

1. First a person's unique distinguishing biological traits (e.g., fingerprints, iris or retina scans, facial geometry, voice waveform) are recorded, stored, and associated with their account.
2. When account control needs to be confirmed, the same traits are again captured and the new record compared to the data on file.
3. If the traits match, the person's control of the account is verified.

It is important to note that biometric verification simply confirms that the person is the same individual whose data was collected at the time of registration. By itself, biometric confirmation does not provide any assertion of the person's behavior or confirm that the registered person was who they claimed at the time of registration. Those elements require other verification means (e.g., comparison against legally recognized identity documents, or assurance by a trusted source such as a known village leader).

In practice, the registered biometric records and access services might be implemented at a national level (e.g., India's Aadhaar system) or at some lower level. A larger scope of registration reasonably implies the potential for higher levels of inclusion.

Regardless of registration scope, the biometric verification service must be accessible by the payments ecosystem at the point of interaction and at the time the transaction is occurring, in order to provide identity verification and subsequent transaction authorization by the individual.

For functional demonstration, the prototype implements a biometric registration service that uses an external service to compare the submitted biometric file against the biometric file registered with the account and stored at the IST. The service compares the two files and indicates if they match. The actual identity of the consumer or linkage to a specific account is not shared. However, a verification service might be able to identify the real person if that information was provided by another service user of which the consumer was also a customer.

4.13.2 Rationale

Biometric registration provides the ability to assert account access through confirmation of a person's measurable distinguishing physical traits and thus doesn't require anything except the person's presence to confirm they have the right to interact with an account. The fact that the confirmation is based on the individual's physical characteristics eliminates the need for any authority to assert their identity, and thus enables account ownership without formal identification documentation, albeit for an account with limited capability.

4.13.3 Requirements

Note: The following requirements could be applied to the DFS System if a centralized repository is not feasible or desirable.

1. The system **should** accept biometric verification to authorize financial transactions.

Rationale: Biometric verification increases opportunity for financial inclusion, as no formal identity documentation is required. NOTE: The DFSP might choose to send the request on to another system that can confirm the person's true identity if additional information is available from that external service.

2. The system **should** provide a central repository for biometric measurement comparison files associated with a user identify/account.

Rationale: The system will need to store the known good biometric datasets and relate them to the individual persona or account, to enable authorization after verification.

3. The biometric verification service **shall** confirm or deny a match in response to a valid biometric verification request. The actual matching is typically performed by comparing a biometric dataset linked to an identity or account with a biometric dataset submitted for comparison.

Rationale: Authorization should succeed or fail. A control file needs to be associated with the account to enable comparison.

4. The system **shall** never transmit or store biometric data in unencrypted format.

Rationale: Unlike a password or PIN, biometric measurements cannot be changed if stolen, and must therefore be protected when in transit and in storage, to protect the individual and the integrity of the system.

5. The system **shall** enforce information protection of biometric data to at least the same level required for administrative passwords.

Rationale: Unlike a password or PIN, biometric measurements cannot be changed if stolen, and must therefore by protected at the highest level of control.

6. When biometric registration is performed, the system **may** support multiple biometric measurement methods (e.g., fingerprints, iris or retina scans, facial geometry, voice waveform)

Rationale: Varying types of measurement support different capabilities. For example, voice waveform can be confirmed remotely without special equipment at the point of customer interaction, while scanner hardware is required to verify fingerprints. Equipment price may also drive selection, though standardization is critical to wide acceptance and use.

7. When using a biometric matching service, the system **shall** only transmit the control biometric file linked to the account and the candidate biometric file provided with the authentication request.

Rationale: Customer or account information is not needed for the match, as two biometric datasets should be sufficient. Sending unnecessary detail exposes private data to a third party.

8. The matching and authentication service availability **must** meet or exceed that of the IST.

Rationale: Biometric users should expect the service to be available whenever the payments ecosystem can transfer payment messages.

9. The system **may** require a PIN in conjunction with a biometric verfication to authorize a transaction.

Rationale: A second factor of authentication increases the level of security, for instance something you know (PIN) and something you are (biometric measurement). Note: The DFSP doesn't necessarily need to forward the PIN, but may instead take responsibility for this requirement. In that case, the IST would simply accept the registrations provided by the participating mobile wallet providers.

10. The system **shall** require a registrant to provide their PIN to register their biometric data and associate it with their account.

Rationale: The PIN is the primary account control until biometric registration is completed, and thus ensures that an unauthorized person cannot register their own biometric data with the authorized user's account. Note: The DFSP doesn't necessarily need to forward the PIN, but may instead take responsibility for this requirement. In that case, the IST would simply accept the registrations provided by the participating mobile wallet providers.

11. Biometric data collection **must** be performed by an authorized agent of the accepted registration authority.

Rationale: Limits opportunity for registration to trusted and known parties.

12. The system **shall** allow an authorized administrative user or participant to associate biometric data with an identity or account, thus authorizing to use the biometric data for authentication.

Rationale: The ability to register and authorize use of biometric data must be controlled to avoid identity or account misuse. This limits opportunity for registration to trusted and known parties.

13. The system **shall** allow an authorized administrative user or participant to de-register biometric data, thus revoking authorization to use the biometric data for authentication.

Rationale: Privacy concerns, fraud, or even disfigurement may drive the need.

14. Biometric authentication **shall** be logged in the same manner as password or PIN authentication.

Rationale: Authentication should be logged regardless of the mechanism.

5.0 Non-functional Requirements (NFR)

This section contains non-functional requirements not included in previous sections.[10]

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. Batch processing of imported payment files **must** conform to average message processing times for the aggregate set of transactions contained in the batch.

Rationale: The submission of individual transactions contained in a batch may be throttled to avoid slowing overall system processing. This requirement indicates that regardless of the rate of de-bulked transactions submitted for processing, the actual processing throughput will still conform to system level processing times.

5. 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.

6. Average webpage user interface load time **should** average no more than 3 seconds over a T-1 connection.

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

7. Maximum webpage user interface load time **should** be no more than 7 seconds over a T-1 connection.

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

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

8. System report generation **must not** impact production transaction processing such that other performance metrics are not met.

Rationale: Reporting is a lower-priority function than transaction processing, and therefore must not impact the switch's primary function.

5.2 SECURITY

Confidentiality and integrity requirements help 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.

5.2.1 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/modify/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 where the impact of a change may have negative impact on the system or users.

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

5.2.2 Authentication

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 **should** support provisioning of roles (i.e., user profiles) to collect rights and privileges, enabling consistency and manageability of user rights and privileges.

Rationale: Enables efficient configuration of rights and privileges into collections. For example, a salesperson has different needs than an administrator. By configuring all the privileges for the salesperson role in one place, it would reduce the need to manage rights for each salesperson account individually, but rather within the assigned "salesperson" role.

3. The system **should** support assignment of roles to user accounts.

Rationale: Enables scalability of account permission provisioning management with consistency of rights and privileges.

4. The system **should** support email addresses as usernames.

Rationale: A common method, as email addresses are generally globally unique.

5. The system **shall** 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.

6. The system **must** support password expiration, requiring a password be changed after an administrator-defined period, not to exceed 90 days.

Rationale: Expiration of passwords reduces their potential timeframe for unauthorized use by if exposed.

7. 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.

8. The system **must** require that the user change their 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.

9. The system **should** support federation with external authentication providers.

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

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

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

11. The system **should** 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.

12. The system **should** require multifactor authentication for any privileged account (e.g., administrator, developer, support) that can modify roles, rights, or privileges, or create users or other entities.

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.

13. The system **must** provide auditable logging of 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.

5.2.3 System Communication and Interaction

1. All internal and external communications between systems and partners **shall** be encrypted.

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

2. The system **should** automatically terminate an idle user session exceeding an administrator-defined time period (e.g., 10 minutes).

Rationale: Terminating idle user sessions reduces exposure to hijacking or use by unauthorized individuals, and frees up system resources.

3. A user session **shall** be considered idle if the user has not caused system data to change or be transferred through interaction with the keyboard, mouse, touchscreen, or other human interface device. Assignment of idle state initiates calculation of session termination time.

Rationale: If the user is not interacting with the system, the session is defined as idle and a termination countdown should begin.

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.

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.

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.

5.4 RELIABILITY

These attributes describe the capability of software to maintain its level of performance, under stated conditions for a stated period of time.

1. The IST **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. TheIST **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 IST architecture and implementation **must** have no single point of failure.

Rationale: Improves system resiliency, leading to higher availability.

4. When a failure occurs, the IST **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. IST 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 IST implementation **should** utilize path and switch diverse redundant telecommunications components.[11]

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 **should** exhibit ACID (atomicity, consistency, isolation, durability) properties to guarantee that database transactions are processed reliably.[12] Note: In the context of databases, a single logical operation on the data is called a *transaction*.

Rationale: Good design practice.

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)

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)

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

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

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

5.6 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 out
- 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 up, allowing increased capacity and performance through replacement or upgrade of existing hardware with more capable hardware.

Rationale: Advances in hardware capability often provide significant performance and scalability benefits without requiring recoding of the software.

2. 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.

3. 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.

4. 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.

5. 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.

5.7 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.

5.8 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.

5.9 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.

5.10 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 User Stories

6.1 LIST OF USER STORIES

This section lists key user stories represented within the requirements of the document.

User Story #	Name	Description	Actors
1	Partner Onboarding	As an IST, I need to provide simple and efficient partner onboarding services, so that I can quickly and efficiently scale to support partners in the marketplace.	IST, MNO, DFSP, NGO, Bank, FRMS,
2	Routing	As an IST, I need to route and clear transactions in real time so payment stakeholders are confident that funds are good and the transaction was completed.	IST, MNO, DFSP, MNO
3	Directory Services	As an IST, I need to manage person/phone/carrier relationship directory services, so that I can route transactions.	IST, DFSP, MNO
4	KYC	As an IST, I need to limit the value and frequency of certain types of transactions by participant, to manage financial risk and comply with law.	IST, DFSP, Bank, MNO, Agent
5	Fraud Detection	As an IST, I need to support fraud detection services so that I can block fraudulent transactions, and reduce transaction risk and financial loss to participants.	IST, FRMS, DFSP, MNO
6	Commissions	As an IST, I need to support payment of commission and fees for specified transaction types and activities, so I can support the operating models in the marketplace.	IST, Agent, Bank, MNO, DFSP
7	Vouchers	As an IST, I need to support the distribution, management, and redemption of subsidiary vouchers for purchases at approved merchants by consumer beneficiaries.	IST, NGO, GOVT, DFSP, MNO
8	Bulk Payments	As an IST, I need to accept and distribute bulk payments sto the needs of government and NGOs that provide support payments to mobile device users.	IST, GOVT, NGO, DFSP, MNO
9	Settlement	As an IST, I need to ensure funds are settled, so that I can enforce integrity of the financial transaction.	IST, Bank, DFSP

7.0 References and Related Documentation

7.1 INDUSTRY GROUPS

The IST is a key component of the overall mobile payments ecosystem. As such, there are many stakeholders involved in the development and use of the IST 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.

7.2 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.

7.3 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
ISV	Integrated Solution Vendor
IVR	Interactive Voice Response

Abbreviation/Acronym/Term	Definition
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