TECHNOLOGY EVOLUTION AND INNOVATION IN DFS

ITU-T FOCUS GROUP ON DIGITAL FINANCIAL SERVICES

International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

FG-DFS

(03/2017)

ITU-T Focus Group Digital Financial Services

Technology evolution and innovation in Digital Financial Services (DFS)

Focus Group Technical Report

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The procedures for establishment of focus groups are defined in Recommendation ITU-T A.7. TSAG set up the ITU-T Focus Group Digital Financial Services (FG DFS) at its meeting in June 2014. TSAG is the parent group of FG DFS.

Deliverables of focus groups can take the form of technical reports, specifications, etc., and aim to provide material for consideration by the parent group in its standardization activities. Deliverables of focus groups are not ITU-T Recommendations.

Technology evolution and innovation in Digital Financial Services (DFS)

About this report

This technical report was written by Leon Perlman, PhD.

The author would like to thank members of the Technology, Innovation and Competition Working Group of the Focus Group Digital Financial Services for their constructive comments on drafts of this report.

If you would like to provide any additional information, please contact Vijay Mauree at tsbfgdfs@itu.int

Table of contents

Executive summary

This report investigates the evolution and sampling of the types of technologies used in digital financial services (DFS). Many of the DFS systems operating today have evolved in some form from progenitor value added services (VAS) products offered by mobile network operations (MNOs) in the mid-1990s.

With basic and feature phones dominating most DFS markets, service providers (SPs) mostly facilitate access to DFS systems via text-based unstructured supplementary service data (USSD) and the short message service (SMS)-based subscriber identity module (SIM) Toolkit, both developed in the 1980s and 1990s, and which operate on almost all general system for mobile communications (GSM)-based handsets.

In more recent implementations, graphical DFS-oriented apps using Java and smartphones have emerged, but these are not as yet in mainstream use in DFS markets.

Merchant services in DFS are growing, with merchants implementing near field communication (NFC)-based and magnetic stripe-based point of sale (POS) devices to accept payments. But while NFC-based payment facilities are growing, they are still smartphone-centric. NFC sticker technology can retrofit all phones with NFC capabilities. Java applets providing DFS on feature phones are gaining in popularity. Similarly, sound-based access is growing, but still in limited use.

The thin SIM is an innovative technology being implemented to obtain alternative network access and to secure DFS transactions.

Iris is becoming the preferred biometric capture method in DFS countries. This is set to increase with the emergence of application programming interfaces (APIs) for Iris capture and phones with Iris scanners.

Access to and integration with existing payments infrastructure for non-bank payment service providers (SPs) is an evolving technical enhancement to DFS, especially as services between SPs become interoperable and some integrate into national payment switches.

1 Abbreviations and acronyms

The following abbreviations and acronyms are used in this report:

1G	First Generation Mobile
2G	Second Generation Mobile
3G	Third Generation Mobile
3GPP	Third Generation Partnership Project
4G	Fourth Generation Mobile
5G	Fifth Generation Mobile
AC	Authentication Centre
AML	Anti-Money Laundering
API	Application Programming Interface
ATM	Automated Teller Machine
BLE	Bluetooth Low Energy
BOP	Bottom of the Pyramid
CICO	Cash In/Cash Out
CLI	Caller Line Identity
CSD	Circuit Switched Data
DFS	Digital Financial Services
EDGE	Enhanced Data for Global Evolution
EMV	EuroPay, MasterCard & Visa
EIR	Equipment Identity Register
ETSI	European Telecommunications Standards Institute
GPR	General Purpose Reloadable
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communications
GSMA	Global System for Mobile Communications Association
HLR	Home Location Register
HSPA	High Speed Packet Access
IP	Internet Protocol
IVR	Interactive Voice Response
KYC	Know Your Customer
LTE	Long Term Evolution
LTE-A	Long Term Evolution Advanced

MAP	Mobile Application Part
MNO	Mobile Network Operator
MO	Mobile Originating
MO-SMS	Mobile Originating SMS
MRE	MAUI Runtime Environment
MSC	Mobile Switching Centre
MT	Mobile Terminating
MVNO	Mobile Virtual Network Operator
NFC	Near Field Communication
NSDT	Near Sound Data Transfer
OS	Operating System
OTA	Over the Air
OTP	One-Time Password
OTT	Over-the-Top
P2A	Person-to-Account
P2M	Person-to-Machine
P2P	Person-to-Person
PIN	Personal Identification Number
POS	Point of Sale
QR	Quick Response
RIVR	Remote Interactive Voice Response
SIM	Subscriber Identity Module
SMS	Short Message Service
SOV	Store of Value
SP	Service Provider
SS7	Signalling System Seven
STK	Subscriber Identity Module Toolkit
UI	User Interface
UMTS	Universal Mobile Telecomunication Service
USSD	Unstructured Supplementary Service Data
UX	User Experience
VAS	Value-Added Services
VLR	Visitor Location Register
VoLTE	Voice over LTE
WAP	Wireless Application Protocol

2 Digital financial services (DFS) technology overview

DFS[1] are rapidly becoming a ubiquitous and affordable platform to access basic financial services to increase financial inclusion.[2]

In many instances, DFS is enabled by technological innovations that allow non-banks to provide basic financial services that are similar to those traditionally offered by banks but which have hitherto been unavailable to those at the bottom of the pyramid (BOP) who are typically, 'unbanked.'[3]

DFS products[4] are offered by banks, non-bank third-party providers, and mobile network operators (MNOs), together with service providers (SPs).[5]

The ability of these providers to make these services global and at scale has been enabled[6] by:

- Improvements in mobile network technology and coverage.
- Greater reliability and sophistication of mobile handsets.
- Better mechanisms to identify and authenticate users.[7]
- Increasing acceptance by merchants of electronic payment instruments.[8]
- New vendor platforms that allow non-banks to safely store both fiat-backed and airtime-based stored user value.[9]
- The leveraging of features of Global System for Mobile Communications (GSM)[10] mobile technology[11] that allow them to act as both an access mechanism and a seamless user interface (UI) for navigating DFS service options.

---

[1] These services are also variously also known as 'mobile money' and 'mobile financial services'.

[2] The BOP which actually means the bottom of the wealth pyramid or the bottom of the income pyramid is the largest, but poorest socio-economic group.

[3] This is a generic term to indicate that they have not had access to a bank account, or are underserved by lack of ready access to a financial services facility.

[4] The predominant transaction types currently in DFS are P2P Payments, CICO, and mobile airtime purchases, bill payments, and merchant payments. See further ITU Focus Group on Digital Financial Services report: *Introduction to the DFS Ecosystem* (2017)

[5] In most cases and for reasons of brevity, this study will mostly conflate third-party SPs – which may include banks – with MNOs, to mean entities providing DFS. Where a distinction is necessary per context, SPs will be differentiated from MNOs: For example, in relation to competition issues and MNO mobile data coverage.

[6] Data in this paper is drawn from Perlman, L (2003) *Mobile Commerce*, Payments Conference, Cape Town; Perlman, L (2010) *Mobile Money*, Mobile Money Conference at Columbia Business School; Perlman, L (2012) *Legal and Regulatory Aspects of Mobile Financial Services;* Perlman, L (2015a) *Security Issues in Digital Financial Services*; Perlman, L (2015b) *Technologies Used in Mobile Financial Services,* Perlman, L (2016a) *Risks in Digital Financial Services;* and Perlman, L (2016b) *CFI/Accion: Access at The Frontier*; and Perlman, L (2017) ITU Focus Group on Digital Financial Services report*: Mobile Handsets Features for DFS*.

[7] Identity designs and platforms are covered in a separate report in the ITU Focus Group on Digital Financial Services and hence will not be covered in great depth here. See ITU Focus Group on Digital Financial Services report: *Identity and Authentication* (2017).

[8] Merchant services are covered in separate ITU DFS FG studies and hence will not be covered in great depth here. See ITU Focus Group on Digital Financial Services report: *Enabling merchant payments acceptance in digital financial services ecosystems* (2016).

[9] Vendor platforms and integration into financial infrastructure are covered in a separate study and hence will not be covered here. See ITU Focus Group on Digital Financial Services report: DFS vendor platform features (2017)

[10] Originally *Groupe Spécial Mobile.* GSM was developed in the 1980s by the European Telecommunications Standards Institute to describe the protocols for second-generation digital mobile networks. See GSMA (2016a) *History*, available at http://www.gsma.com/aboutus/history

[11] These include features such as voice, short message services (SMS) and unstructured supplementary service data (USSD).

A number of 'contactless' facilities such as Near Field Communication (NFC), Near Sound Data Transfer (NSDT), and linkages of DFS accounts to companion debit cards through national switches are all also spurring the growth of merchant payments in DFS.

3 Technologies used to remotely access DFS[12]

3.1 Overview

SPs will provide the remote access method(s) that are best suited to the access devices prevalent in the markets in which they operate whilst also taking into account the technical literacy levels of their customers. So with basic and feature phones dominating most DFS markets, SPs mostly facilitate access to DFS systems primarily via text-based unstructured supplementary service data (USSD) and the short message service (SMS)-based subscriber identity module Toolkit (STK) – both of which work on almost all GSM-based handsets.[13]

USSD and SMS (using STK) do multiple duty in DFS as mobile network data transport mechanisms – also known as 'bearers' – across GSM networks,[14] as payment instruments using the handsets themselves for payment, and as the UI to interact with DFS services.

Indeed, USSD – and voice, via interactive voice response (IVR) – were initially the core mobile bearers and UIs used in the mid-1990s for executing user recharges of mobile network prepaid airtime-based stored value accounts, and as access mechanisms and payment instruments with progenitor DFS-type ecosystems that allowed purchase of infotainment-type value-added services (VAS) using the MNO airtime-based value.[15]

Utilizing opportunities by new enabling regulatory regimes,[16] this concept of using a mobile-based store of value (SoV) for transactional purposes has evolved to the DFS systems which instead use accounts with fiat money-backed stores of value.

In more recent implementations from mid-2012, DFS-oriented apps using over-the-top (OTT) internet connectivity via smartphones have emerged. These are not as of yet in mainstream use in most DFS markets for a number of reasons[17] which include the relative cost of the devices for those at the BOP and lack of national high-speed data networks required to efficiently use all the features of these apps.[18]

3.2 Mobile network evolution

GSM was invented in the late 1980s in Europe and has evolved to become the dominant mobile technology worldwide. It is the digital successor to first generation mobile (1G) analogue and the largely insecure mobile networks introduced in the 1970s. The initial GSM incarnations from the early 1990s to early 2000s were characterized by 'narrowband' or low-speed second generation mobile (2G) technologies that used data transport mechanisms (bearers) such as USSD, circuit switched data (CSD), and SMS. These have evolved to Internet Protocol (IP)-based access

[12] Data based on Perlman (2003) *ibid*; Perlman (2010) *ibid*; Perlman (2012) *ibid*; Perlman, L (2015a) *ibid*; Perlman (2015b) *ibid.*

[13] Excluding some smartphones.

[14] A bearer service – or just bearer - is a telecommunications term describing a service that allows transmission of information signals between network interfaces. USSD, SMS, and 3G networks can be considered bearer technologies used in mobile.

[15] See Section 5.

[16] *ibid*

[17] See further, Perlman (2016b) *ibid*; and Perlman (2017) *ibid.*

[18] For example, mapping services needed to locate DFS agents.

technologies based on low speed 2.5G and higher speed third generation mobile (3G), 3.75G, and fourth generation mobile (4G) technology.[19]

While many countries with DFS have national 2G coverage, 3G/4G coverage in emerging markets is found mostly only in urban areas and on or near national roads.

The GSM specification has at its core the mobile application part (MAP) protocol which specifies how handsets with GSM-based SIM cards can gain seamless access to key GSM network features such as the Home Location Register (HLR), Visitor Location Register (VLR), Mobile Switching Centre (MSC), Equipment Identity Register (EIR), and Authentication Centre (AC). USSD and SMS messages also travel over MAP. Many of the GSM technologies used in DFS – such as USSD and SMS – operate over what is known as the GSM 'signalling' channel.

MAP itself operates over Signalling System 7 (SS7), a communication technology used by most telecommunication network operators around the world to allow their mobile and fixed line networks to interact, as well as for mediating multiple voice calls used on the GSM 'traffic' channel.[20] These inter-network interactions facilitate the exchange of information needed to make calls and pass text messages between each other, ensure correct billing, and allowing customers on one network to easily roam on any other GSM network in the world.

However, SS7 is not thought to be entirely secure: It was designed in the 1970s with no real authentication and intrusion-prevention in mind.[21] This has implications for the use of USSD and SMS in financial transactions.

3.3 GSM voice channel

Key to the growth of DFS in many emerging markets is the ability to effectively 'bolt-on' services to GSM mobile network access mechanisms and UIs. For example, the GSM voice channel[22] which uses the traffic channel component of GSM, was the original method of access to basic transactional services offered by MNOs and other SPs. Users could, for example, access VAS-type infotainment-type menus and general services by simply dialling special IVR numbers linked to infotainment services provided by VAS SPs.

Other transactional mechanisms using GSM-based technology and its successors are described in further detail below.

3.4 GSM signalling channel

3.4.1 SMS

SMS – also known as 'text messaging' – was designed in the 1980s to act as a data bearer for mobile network system engineers developing and maintaining the initial version of GSM systems. From these humble beginnings, text messaging has become a ubiquitous consumer-facing person-to-person (P2P) messaging facility.

[19] The 'G' (generation) designation refers to a significant enhancement of mobile network technology, mostly signifying faster mobile data speeds. Fifth generation mobile (5G) mobile data technologies are still in development.

[20] This signalling mediation allows multiple calls to efficiently take place on a known frequency without overlap.

[21] For further insights into these vulnerabilities, see Perlman L (2015a) *ibid*; Perlman (2016) *ibid*; and Kurbatov, D (2016) *Statistics of Vulnerabilities in SS7 Networks and Ways to Make Them Secure*; and ITU Focus Group Digital Financial Services report on Security aspects of DFS (2017).

[22] During a GSM call, speech is converted from analogue sound waves to digital data by the phone itself, and transmitted through the *mobile* phone network by digital means. The digital algorithm used to encode speech signals is called a codec.

SMS uses GSM signalling channels. The initial SMS protocol allowed users to send and receive messages of up to 160 alpha-numeric characters.[23]

A SMS sent by a user from their mobile handset is known as a mobile originating (MO)-SMS, or MO. A SMS received by the user on their handset - whether it be from another person or from an automated machine - is known as a mobile terminating-short message service (MT-SMS), or simply mobile terminating (MT), to indicate that a SMS has terminated on a mobile handset.

3.4.2 USSD

USSD is a novel standard within the GSM and 3G/4G specifications. It can be used for transmitting information over the signalling channel of mobile networks and for accessing standard services and VAS. USSD is session-based – meaning it does not store any data on the mobile handset – and as such it can only be reliably accessed or be consistently accessible when there is robust handset communication with a MNO base station.[24]

USSD is activated either by users inputting a series of predefined star or hash/pound commands on the mobile handset, or via a session initiated by the MNO or a SP. In both methods, the user is presented with a numbered menu and can use the mobile keypad to respond to and to input any data required.

3.5 Internet-based access to DFS

3.5.1 Low-speed data networks

3.5.1.1 General packet radio service (GPRS) and enhanced data for global evolution (EDGE/EDGE+)

GPRS is an IP-based technology used to upgrade GSM networks that use expensive and very slow, time-based CSD to access data.[25] GPRS allows subscribers to stay connected to data on the Internet and to be billed per data unit (in megabytes or gigabytes). [26]

EDGE, and later EDGE+,[27] are software-based enhancements to 2.5G GSM/GPRS, providing slightly higher mobile data speeds. They are, however, still much slower than the data speeds offered by 3G/4G mobile data network.

The majority of phones – usually feature phones – used in emerging markets for DFS access use EDGE/EDGE+ for mobile data access.[28]

[23] Security concerns relating to SS7 also transpose to SMS.

[24] Poor mobile signals and substandard antennas in some mobile phones may cause USSD session initiation and sustainability issues.

[25] CSD data access is billed per minute compared to always-on systems like GPRS, EDGE, and 3G or 4G which charge according to how much data is transferred.

[26] GPRS and the other data facilities are billed in data units like megabytes or gigabytes of use by the MNO.

[27] This is known also as enhanced GPRS (EGPRS).

[28] Perlman (2016b) *ibid*; Perlman (2017) *ibid*

3.5.2 High-speed data networks

3.5.2.1 3G technologies

Third generation (3G) mobile networks – also known as universal mobile telecommunications service (UMTS) – provide higher speed data. The fastest 3G incarnation is high speed packet access (HSPA+). 3G requires new MNO base stations and new frequency allocations, both of which can involve high capital cost outlays for MNOs.

3G allows bandwidth-heavy DFS smartphone apps to utilize the full spectrum of facilities these apps offer, for example, agent mapping services.

3.5.2.2 4G technologies

Long term evolution (LTE) is a 4G data standard. It increases the capacity and speed over HSPA by using a different radio interface together with core network improvements. LTE advanced (LTE-A) is a major enhancement of LTE and includes voice over LTE (VoLTE).[29]

4 Mobile phone types used in DFS

4.1 Overview

The predominant types of mobile handsets in DFS markets that serve those at the BOP are what are now known as 'basic' phones and 'feature' phones, with some DFS markets showing increases in smartphone penetration. [30]

Mobile phone evolution over the past few years has, to some extent, rendered distinctions between these device categorizations somewhat fuzzy, as they can share some, but not all, of the same or similar features and capabilities.

4.2 Phone types

Basic phones, also called 'low-end' or 'dumb phones', have limited feature sets, limited or no factory-installed, or user-installable value-added third-party applications, and no or very limited data connectivity. They can, however, for the most part, access DFS platforms through the use of basic USSD and STK capabilities.

Feature phones are the dominant type of phones in DFS.[31] They have more functions than basic phones, but limited functionality and proprietary operating systems (OS). They include most of the features of basic phones, augmented in many cases by features such as Bluetooth and MMS, which are mostly narrowband data connectivity options. They also include wireless application protocol (WAP) capabilities, and, in some cases, 3G capabilities.

Market surveys and projections[32] indicate that smartphone penetration is increasing in many DFS markets worldwide. These devices have touchscreens, offer a better UI than the USSD and STK UIs used on basic and feature phones, as well as providing increased bouquets of service offerings. Entry-

[29] Note that 5G mobile network technology is still in development.

[30] The 'basic'- or 'low-end' - appellation is a throwback to the early days of the emergence of GSM mobile technology, where only basic functionality - such as call functions, SMS, USSD v1 functionality, and a phonebook - were needed (and available) to communicate. However, some basic devices could receive VAS, such as ringtones, via OTA installation.

[31] GSMA (2015) *From Feature Phones To Smartphones, The Road Ahead,* available at https://www.gsmaintelligence.com/research/2015/01/from-feature-phones-to-smartphones-the-road-ahead/456/

[32] See for example GSMA (2016a) *ibid.*

level smartphones being sold in emerging markets are at feature phone-level pricing of around USD 30,[33] although many are of relatively low-specification and of relatively shorter device longevity.

5 Mobile phone OSs

A key feature of mobile handsets in DFS has been their ability to operate ubiquitously and reliably across mobile networks without any modification, using relatively simple, if not bland, text-based UIs on basic and feature phones.[34]

In the past few years, with the evolution generally of mobile-based services and DFS specifically, the demand for increased functionality and better UIs has given rise to more sophisticated handsets that use specialized interfaces or OSs. It is thought that Better OS design may make the user's experience of accessing DFS far easier than using 2G-type phones that primarily employ text-based USSD and SMS for DFS access.[35]

With feature phones, not all support third-party software, but if they do,[36] they usually run on Java or similar or are made for the proprietary OSs of the device's core chipset in the phone such as those from Mediatek (S30+ and MAUI runtime environment (MRE)) and Nokia (Symbian).[37]

Smartphone OSs include those from Apple (Apple OS), Google (Android OS), Microsoft (Windows Phone, Windows Mobile), and Blackberry (Blackberry OS).[38]

6 Stores of value and billing systems

As noted above, DFS builds on the innovations developed in the mid-1990s for micropayments for VAS.[39] Payments for VAS[40] began using the prepaid-type[41] mobile airtime-based SoV accounts acting as a virtual currency created and provided by an MNO for semi-closed loop digital transactions.[42]
The unit of account[43] in the airtime-based SoV may be that of the national fiat currency, or some other unit, such as airtime minutes. The airtime value is usually bought at a retail outlet, on the Internet, via WAP, or via a bank automated teller machine (ATM) linked directly to the MNO airtime billing system.

Use of this MNO airtime-based stored value account has evolved into the venerated DFS stored value account, such that MNOs – and other non-banks, where allowed by regulation – can provide

[33] See Perlman (2016b) *ibid*; and Perlman (2017) *ibid* Prices for phones and access may however be affected by the increased tendency by some regulators to tax mobile phone imports and mobile phone airtime.

[34] For further details on mobile phone OSs and the relation to mobile phone chipsets, see Perlman (2016b) *ibid.*

[35] This, however, is market dependent, as many users do not necessarily have the technical literacy to navigate the new, more sophisticated UIs that the new OSs provide.

[36] These are usually standalone applications that do not necessarily integrate with other features of the phone.

[37] Nokia's Symbian mobile phone OS, once the world's most popular, is now in rapid decline.

[38] The Java application platform is the only system that is cross-platform and cross-OS so long as a Java engine/emulator is available on the phone to execute the Java applet.

[39] See for example, WASPA, at waspa.org.za. It is an industry association representing vendors of these digital goods and services.

[40] The airtime SoV is limited to digital goods and services. See below.

[41] A MNO usually has two methods of charging for access to its network and for the use of basic and VAS prepaid and post-paid. Prepaid is by far the most prevalent means of access around the world across all mobile technologies, and dominates in developing countries. Users will only be able to access services and do transfers if they have sufficient value in their mobile airtime accounts.

[42] The ecosystem is a semi-closed loop since some external purchase and value transfers may be possible.

[43] For example, Indian Rupees or Malawian Kwacha.

redeemable and non-redeemable wallets to users.[44] Stored value accounts with redeemable value, the core of the DFS concept, are based on the unit of account, SoV, and means of payment (money) of the local national currency and said to be fiat-backed. The value is usually stored by entities licensed or authorized by central banks. MNOs can offer both the airtime-based and fiat-backed SoVs simultaneously, in separate accounts.

If the DFS system is operated by a non-bank DFS SP such as an MNO, regulations from the central bank will usually provide that any fiat money received from users[45] must be placed by these entities in special bank accounts.[46] Through normative regulations usually issued by a central bank, the fiat money then becomes an electronic SoV for use in DFS stored value accounts hosted by the SP and which is often termed electronic money (eMoney) or mobile money (m-money).[47] The e/m-money is backed by the fiat money stored in the bank account(s) on a 1:1 basis.[48]

Comparatively then, use of a fiat unit of account for the airtime-based value does not make it e/m-Money *per se*[49]*,* as the former is usually characterized by a different regulatory regime to e/m-Money used in DFS. Regulation of this SoV is usually the domain of the telecommunications regulator rather than the central bank.[50] For most jurisdictions, the value received by the MNO for airtime wallet purposes is not ring-fenced nor regulated by the same regulations as e/m-Money. Value bought for airtime purposes, once placed in the airtime based stored value account housed at the MNO is (with a few exceptions) non-redeemable to cash.[51] The inability to cash-out of the airtime-based stored value reduces somewhat the risk profile in terms of anti-money laundering (AML) of the airtime-based store of value compared to use of fiat-backed eMoney used in DFS. Cash-in and cash-out (CICO) by users for fiat-backed DFS stored value accounts is allowed, but within regulated limits.

There are usually no limitations on the type of services the DFS user can obtain and use with the e/m-Money stored value. For example, the value can be used to make merchant payments for both physical and digital goods and services, as well as to do P2P payments within regulated know your customer (KYC) limits.
Indeed, a critical distinction between the airtime stored value account wallet and the fiat-based stored value wallet is the fiat value a MNOs receives when the airtime is purchased by users may also be used for operational expenses by the MNO.

---

[44] Other SPs – where allowed by regulation – may provide other types of 'virtual currency' wallets, for example the blockchain-powered Bitcoin or Ethers.

[45] Or initially provided by these entities themselves.

[46] The cumulative value received by the entity from users is stored in one or more special bank accounts, and the accounts are ring-fenced in so far as the bank cannot use these funds for intermediation. The entity cannot use the funds for any operational expenses or riskier activities. The special bank accounts may be called trust accounts where the jurisdiction has a trust regime.

[47] The terms eMoney 'creation' and eMoney 'issuance' are often used in this context – and often interchangeably in the literature – to describe e-money creation or distribution. Depending on the regulatory regime, the entity may be allowed to 'issue' (distribute) e-Money 'created' by the central bank, or create and also issue the eMoney itself. The effect is the same though: eMoney is made available to users as a usable SoV.

[48] That is, every e/m-Money is backed at par with the value stored by the entity in banks.

[49] This airtime-based virtual currency is in most cases not the same as eMoney, the latter usually coming into being through laws, directives, or regulations issued by central banks or parliaments.

[50] In some jurisdictions, such as South Africa, both the telecommunications regulator and the central bank have oversight over the use of the airtime wallet.

[51] An exception to the cash-out restriction for airtime wallets appears to be in Russia where cash-out from the airtime wallet is reportedly allowed.

At the non-bank SP level however, there may be limitations on use of the fiat money received for fractional banking purposes: That is, for providing credit or similar types of riskier services.

7 Mobile phone UIs used in DFS

7.1 Overview

While the explosion of new types of phones and OSs has provided reliable communications and services to users, there is an equally critical need to find effective UIs for the simpler devices used for accessing DFS products. Many potential users of DFS however, have limited technical literacy beyond the procedures used for making basic phone calls and using the mobile phone to input a code from a prepaid airtime voucher using USSD or IVR.[52]

Depending on the type of service and region a combination of the following may be offered by SPs as the primary interface to DFS products:

Sound-based:
- Voice channel – IVR
- Voice channel – NSDT

Text-based:
- SMS – cleartext (unencrypted)
- SMS – encrypted via STK
- USSD – mobile originated USSD (MO-USSD)
- USSD – network initiated USSD (NI-USSD)

Graphical interfaces:
- SMS – via Java-based applets
- IP-based OTT mobile phone applications
- IP-based WAP

7.2 Voice channel

The three main methods of interaction for DFS services using the GSM voice channel are via caller line identity (CLI), IVR, and NSDT.

7.2.1 CLI

The CLI method allows a user to simply dial a specific number, and the system captures the number and bills the user at a rate associated with that called number. This was first demonstrated by MTN South Africa in 1995 with its remote interactive voice response (RIVR) service[53], but is very seldom in use today.

7.2.2 IVR

IVR is a technology that allows a user to interact with system inputs via the handsets keypad. In most IVR incarnations, users are prompted by a recorded voice to input specific numbers on the keypad that then allows access to data or services. They are usually associated with customer care calls and for access to certain VAS, but at premium rates.

[52] See for example Grameen Foundation (2013) *ibid.*

[53] See Perlman (2003) *ibid;* Perlman (2010) ibid; and Perlman (2012) *ibid*.

The new Airtel India Payments Bank also uses IVR for primary DFS access for its customers.[54] ABSA bank in South Africa allows its customers to access the terms of conditions of its DFS banking offering through IVR. Users can also choose from multiple official languages.

7.2.3 NSDT

NSDT is a method of connecting a merchant with a customer for payment using handsets and merchant point of sale (POS) exchanging payment credentials with encrypted but silent data.[55]

7.3 Text-based

7.3.1 SMS and short codes

SMS is used in DFS primarily as an authentication and verification mechanism for fiat-backed DFS account transactions, as well as the initiation mechanism for purchasing VAS using the mobile airtime-based stored value account. The person-2-machine (P2M) SMS sent by the user may act as a payment to the VAS provider. The special number which the user sends the P2M SMS as payment is known as a 'short code' and is usually 5 digits long and common to all MNOs in a country. P2M SMSs are the mobile progenitors for the development of fiat-backed DFS mobile transactional platforms.

7.3.2 STK

STK - also referred to as SIM toolkit - is a SMS-based remote access and UI GSM technology used to provide DFS and related services to markets where basic and feature phones are the plurality. As with USSD, STK is especially prevalent in developing countries where entry-level basic and feature phones are mostly used. STK is currently one of the most extensively and globally used mobile interfaces in DFS other than USSD.

A specialized SIM to host the STK application and STK-compatible phone is required. STK technology is embedded on the SIM card, allowing special applications for DFS and banking services to be accessed by the subscriber using custom menus stored on the SIM card.[56] The STK will usually use SMS as a bearer for communication with a host,[57] usually encrypting the cleartext SMS to/from the handset and STK server.

On a 'basic' phone, the STK menu may appear as an additional phone menu item when scrolling through basic menus to access the phone's features. On a feature phone or smartphone,[58] the STK will usually manifest as a specific application icon that appears on the device's home screen.

If updates for functionality or security need to be made to the application on the SIM, a series of 'over the air' (OTA), binary SMSs are sent over the MNO's network to the phone, which when joined together, will update the STK application on the user's SIM. This may be costly for many non-MNO DFS SPs who have to pay for all the SMS to do a full update of the STK menu on the phone and is one of the primary reasons USSD is proffered by non-MNO SPs.

---

[54] Airtel (2016) *India's first Payments Bank goes LIVE*, available at http://www.airtel.in/about-bharti/media-centre/bharti-airtel-news/corporate/india++first+payments+bank+goes+live-airtel+payments+bank+starts+pilot+services+in+rajasthan

[55] See Section 7.2.3 on NSDT.

[56] These commands are standard for all mobile equipment and defined by European Telecommunications Standards Institute (ETSI) and Third Generation Partnership Project (3GPP) specifications.

[57] While STK can use USSD as a bearer, in practice, SMS is mostly used as the STK bearer in DFS implementations.

[58] Most of the newer versions of the Android OS do not support STK.

7.3.3 USSD

USSD is both a GSM bearer technology and a DFS UI usable on all GSM and 3G/4G mobile networks, does not require any additional installations by customers, nor does it require an IP-based data access connection by users.[59] As a result, USSD has been termed 'the third universal app.'[60]

It has been used as payment instrument and UI since the mid-1990s as the primary mechanism for loading mobile airtime value into a user's airtime stored value account when the first prepaid airtime systems were launched around the world in 1996. Unlike SMS, no data sent or received during the USSD session is stored on the mobile handset which – except for the glaring security issues identified in SS7 – makes USSD useful for the transmission and receipt of passwords in DFS sessions.

While the USSD specification allows a USSD session of up to 600 seconds, typical allowance by MNOs for DFS and other third-party services is up to 180 seconds, with 120 seconds being the typical maximum time allowed for the entire USSD session by MNOs.

There is also push USSD – also known as Network Initiated USSD – which is used mostly for 2-factor authentication in DFS.[61]

7.4 Graphical interfaces

7.4.1 Overview

While text-based UIs currently predominate in DFS, the past few years have seen the emergence of graphical and hyperlinked interfaces that provide icon-based navigation to users. The first DFS graphical UIs were introduced in 1999 with WAP-based interfaces using time-based CSD as bearers.

7.4.2 WAP

WAP is a type of mini-Internet experience designed for small mobile phone screens. It is used for transmission of simple web pages in primarily 2G/2.5G networks and may contain links and icons formatted especially to be usable and visible on the small screen of the mobile phone. While it first appeared in 1999 using CSD, WAP gained more prominence around 2001 when the first always-on IP-based GPRS networks appeared. However, the use of WAP as a UI for DFS access has largely dissipated in favor of STK, Java apps, USSD, and smartphone applications.

7.4.3 Java-based feature phone applications

In 2012 the first Java DFS apps for feature phones were launched and are now being used in a number of DFS implementations around the world.[62] The icon-based menus make it easier for illiterate and semi-literate users to navigate DFS options presented in the UI.

Technically, small Java 'applets' are installed on compatible phones either via Bluetooth or OTA using WAP. This method is similar in principle to a smartphone app, but running on a less sophisticated type of handset OS.

Generally, although they use encrypted SMS, Java-based DFS apps are more efficient and cheaper to operate than STK access to DFS since multiple SMSs for facilitating transactions are usually not required. Java applets mostly use bank-grade encryption for SMSs.

---

[59] Security concerns relating to SS7 also transpose to USSD.

[60] Perrier, T *et al* (2015) *USSD: The Third Universal App*, available at http://bderenzi.com/Papers/perrier-dev2015.pdf

[61] The caveats noted above around SS7 security are also relevant here, although push USSD is conceptually harder to intercept when a USSD session is initiated by an SP.

[62] Java is a programming language and computing platform first released by Sun Microsystems in 1995. It is the underlying technology that powers state-of-the-art programs including utilities, games, and business applications

7.4.4 Smartphone-based interfaces

The first smartphone-based OTT apps for DFS in developing markets emerged around 2010[63] and have grown in use as cheaper smartphones emerge.

Compared to WAP, USSD, STK, and even Java apps, these apps provide a rich-media user experience (UX) that utilize smartphone device features which include large color screens, touch access, faster access through 3G, as well as more context-sensitive access to DFS services, including NFC-based merchant payments. Most run on Google's Android OS. There are, however, security issues relating to some DFS-based apps.[64] To a large extent, the interface is also dependent on sufficient (high-speed) bandwidth, which is largely lacking in rural areas of emerging markets.

8 Digital value chain technologies and transactions

8.1 Overview

As noted above, the mobile phone has been used as a semi-closed-loop basic payment instrument since the mid-1990s when MNOs allowed their airtime-based stored value accounts to be used to purchase digital goods and services using the GSM voice channel. This was followed by the use of SMS-based short codes, USSD-based menus, then Java applets, and smartphone-based applications.

In most cases, transactions using airtime as the store of value are limited by regulation to digital goods and services than can and must be consumed on the handset. Users then – depending on regulations – have been able to: Make calls; send SMSs; access the internet; do P2P airtime transfers to users on the same MNO or other MNOs; to purchase digital goods and services, such as infotainment and gaming services; or purchase micro-insurance. They access and pay for these digital goods and services in a semi-closed-loop ecosystem by either dialing into special premium-rated IVR numbers, sending a SMS to special premium rated shortcodes, or navigating USSD menus via premium rated USSD shortcodes. The most predominant billing types for VAS have been the *à la carte* or once-off, and the periodic billing. These are still very popular today.

The fiat-backed store of value account characteristic of DFS is – where allowed by regulation – available from MNOs, banks, and service providers (SPs) offering DFS. These accounts are now being used in a wide range of digital transactions that may involve: The purchase of physical and digital goods and services; bill and government payments; P2P transfers; for and receipt of social welfare benefits.

Some DFS SPs also support companion magnetic-stripe and Europay, MasterCard & Visa (EMV)-based general purpose reloadable (GPR) payment cards, as well as contactless payment tools such as NFC which allow users to make payments to merchants at distances of a few centimeters to a few meters.[65] The contactless payment tools are linked to fiat-backed DFS stored value accounts.

Digital value chain payment technologies are described below[66].

---

[63]Times of India (2010) *Transfer Funds To Any Bank A/C Via Mobile App*, available at http://timesofindia.indiatimes.com/business/india-business/Transfer-funds-to-any-bank-a/c-via-mobile-app/articleshow/6973360.cms. See also GMA (2012) *Globe To Launch GCash Mobile App for iPhone, Blackberry*, available at http://www.gmanetwork.com/news/story/249879/scitech/technology/globe-to-launch-gcash-mobile-app-for-iphone-blackberry

[64] See Butler, K *et al* (2015) *Mo(bile) Money, Mo(bile) Problems: Analysis of Branchless Banking Applications in the Developing World*, available at https://cise.ufl.edu/~butler/pubs/sec15a.pdf ; and ITU Focus Group on Digital Financial Services report: *Security aspects of DFS* (2017)

[65] Some systems, like NFC and RFID, allow cheaper NFC chip-enabled stickers to be placed on the device instead of embedding a more expensive NFC chip inside. The sticker version of NFC does not have the same level of functionality as the embedded version.

[66] There is also Radio Frequency Identity Magnetic Secure Transmission, and Bluetooth Low Energy (BLE), but these are seldom – to date – found in DFS implementations in developing markets. They may gain traction in certain markets over time.

8.2 Sound-based

8.2.1 IVR

The early providers of VAS in the 1990s used IVR to facilitate payments. As noted above, IVR is also being used in some DFS implementations for primary service access,[67] although this is very rare nowadays.

8.2.2 Acoustic-based access

Acoustic-based access technology – also known as sound-based, or NSDT[68] – allows the microphone of any basic phone, feature phone, or smartphone to be used for data capture, with the standard MNO voice channel acting as the data transporter. Transaction data is encrypted through the phone's audio channel using a 'cryptosound.'[69] In a merchant/agent environment, the merchant or agent enters the amount on the POS terminal device. The customer then enters their phone number and personal identification number (PIN). On the terminal, the acoustic platform dials the customer's phone. The customer then answers the call and places the phone next to the terminal or agent's handset. A one-time encrypted password is exchanged via the cryptosound between the two devices and the transaction is complete.[70]

8.3 SMS and short codes

In a VAS environment, SMSs may be sent by a mobile user from their mobile phone – as a MO-SMS – via special shortcodes to systems run by third-party vendors of VAS-type digital goods and services such as mobile jokes, sports alerts, and phone ringtones. SMS shortcodes are being used in DFS through STK access and for customer care services.[71]

SMS-based STK is used as the secure UI to DFS in a number of implementations. Unencrypted (cleartext) SMS messages are also used for 2-factor verification purposes in DFS: A bank or SP will send a one-time password (OTP) to a user's phone via SMS, which the user must input into a challenge menu or screen to validate their identity and/or to confirm a large payment transaction. However, interception of OTP SMSs is prevalent through phishing attacks and interception of SMSs via IMSI Catchers – devices which can undertake man in the middle attacks on user handsets to illegally capture data – and attacks on the SS7 network layers.[72]

8.4 USSD

As noted above, USSD has been used as the payment instrument, UI, and technology bearer for both VAS and DFS transactions.

As an SP's service bouquet expands, menu tree structures can be created in real time by the USSD server at the MNO or aggregator at very little cost. This means that any calculations for DFS transaction costs can be dynamically generated per transaction, for example if the transaction cost is

---

[67] Airtel (2016) *India's First Payments Bank Goes LIVE-Airtel Payments Bank Starts Pilot Services In Rajasthan*, available at http://www.airtel.in/about-bharti/media-centre/bharti-airtel-news/corporate/india++first+payments+bank+goes+live-airtel+payments+bank+starts+pilot+services+in+rajasthan

[68] NSDT is the trade name for the acoustic access service offered by Tagpay. See www.tagpay.fr

[69] Zhang, B (2013) *PriWhisper: Enabling Keyless Secure Acoustic Communication for Smartphones*, available at https://eprint.iacr.org/2013/581.pdf

[70] The technology is used by Yes Bank (India), Pepele Mobile (DRC); Netcash (Zimbabwe); MoboMoney (India); UltraCash (India); and Alipay (China).

[71] DFS users send a SMS to a shortcode and will be called back by the DFS SP's customer care desk. This saves time as they do not need to be on hold.

[72] See further Perlman (2015b) *ibid* and Perlman (2016a) *ibid*

a percentage of the total transaction value. Other DFS interface methods such STK or Java applets may not necessarily have those real-time capabilities built in.

8.5 NFC

NFC is popular contactless payment system.[73] A device with an integrated NFC chip and antenna, or a NFC tag/sticker is required to facilitate payment.[74] This eliminates the need to carry all credit or debit cards in a physical wallet.

To facilitate a payment transaction at a merchant using an NFC-enabled phone, the phone is held against a merchant POS device. Since the majority of phones in use today in all classes do not have NFC, an alternative is to retrofit NFC through the use of NFC 'stickers' stuck on the back of a phone.

8.6 Quick response (QR) codes

QR codes have emerged as a DFS payment mechanism in a number of countries. In a typical payment environment, the QR code will uniquely identify the user and the payment, and a POS scanner or QR-enabled phone will read the data and process the payment.

8.7 Magstripe and chip card readers

MNOs and DFS SPs are now providing companion GPR Visa/MasterCard/Unionpay-branded cards, following a big push by card associations to provide GPR cards to augment the card-less DFS systems. Some may be magstripe only, with an increasing number of cards with EMV chips embedded for added security.[75] These cards are aspirational products for those who have never had a Visa or Mastercard product. Most GPR cards are debit-based magstripe cards, with some linking to DFS accounts. However, this may raise consumer protection concerns as loss or theft of the card may give bad actors full access to the full value in a DFS account. Fault for loss of the value through card loss or theft, and subsequent use by bad actors usually fastens fully on the customer.

An increasing number of merchants use simple, plug in magstripe and EMV card readers plugged into the audio jack of smartphones.[76] Transaction data is sent to a processing switch, which may withdraw funds from a DFS wallet or a bank account, depending on the configuration.

9 Thin SIM technology in DFS

9.1 Overview

Thin SIM – also called sticky SIM – is a relatively new technology being used in DFS markets to address technology access issues in DFS. It is used to facilitate secure transactions, as well as to provide access to DFS where MNO coverage is not available.

The thin SIM is a paper-thin plastic sheet embedded with a number of contact points and a chip that is stuck on top of a standard SIM card.[77] Once in use, the thin SIM essentially converts any handset

[73] NFC complements many popular consumer level wireless technologies, by utilizing the key elements in existing standards for contactless card technology. See NFC Forum (2016) *About the Technology*, available at http://nfc-forum.org/what-is-nfc/about-the-technology

[74] Google and its partners have devised an alternative mechanism called Host Card Emulation that replaces for the most part the internal phone processes NFC uses.

[75] EMV is a technical standard for smart payment cards and for payment terminals and ATMs that can accept them. Europay, MasterCard, and Visa, are the three entities that originally created the standard. The standard is now managed by EMVCo, a consortium with control split equally among Visa, MasterCard, JCB, American Express, China UnionPay, and Discover.

[76] Card readers have been popularized by, amongst others, Square, and allow almost any smartphone to accept payment cards. The readers usually plug into the audio jack of the smartphone.

[77] The technology was developed in China in 2005, primarily designed to avoid roaming fees.

into a dual-SIM phone. Users can then access services on both networks and have two SIM cards in one slot of the device. The solution is device and MNO agnostic.

The Global System for Mobile Communications Association (GSMA) undertook a study on thin SIMs after concerns were raised by some MNOs that there may be security and privacy implications in using the technology. In essence, he GSMA report said that interception risks were negligible if thin SIM technology was properly implemented.[78]

9.2 Uses of thin SIMs

Kenyan mobile virtual network operator (MVNO) Equitel – the telecommunications arm of Equity Bank – uses its thin SIM technology offered to its customers to use cheaper USSD and STK bearer services from MNO Airtel.[79] Use of the shortcode *247# will divert the session to use the Airtel network.

Similarly, India's Yes Bank launched its own thin SIM payments solution for feature phones.[80] The sticker installs a STK-based app linked to a prepaid store of value.[81]

Thin SIM technology is also being offered for use in DFS DigiTally to compensate for lack of MNO coverage by providing an offline alternative for doing P2P transactions.[82]

10 Identity verification in DFS accounts and transactions[83]

10.1 Overview

As DFS grows in developing countries, regulators have imposed KYC rules that require SPs to identify users on their systems. With a few exceptions, some type of identity must be provided by the user for account openings and CICO services.[84] The KYC rules are derived from standards established by the G7's Financial Action Task Force on standards in financial services aimed at AML initiatives.[85]

The progenitor for these verification systems, however, has been at the mobile phone SIM card level, where regulators have for a number of years mandated the registration of prepaid SIM card users.

---

[78] GSMA (2014) *Generic Overlay SIM Security Assessment*, available at http://www.gsma.com/publicpolicy/wp-content/uploads/2014/08/GSMA-Security-Group-Overlay_SIM_Security_Assessment_August_18_2014.pdf

[79] See Equitel (2016) *Get Activated*, available at http://www.equitel.com/my-phone/get-activated

[80] ETCIO (2016) *Yes Bank To Launch SIM Sleeve Payments Solution For Feature Phones*, available at http://cio.economictimes.indiatimes.com/news/mobility/yes-bank-to-launch-sim-sleeve-payments-solution-for-feature-phones/51780748

[81] The transactions currently offered P2P fund transfers, person-to-account (P2A) fund transfers using NEFT and IMPS, balance checking, payments to merchants for small and large value purchases and payment of bills, top-ups, and recharges.

[82] DigiTally achieves this via a STK or as a smartphone app, or in thin SIMs for basic phones. To transfer money from one phone to another, a user exchanges cash for DigiTally credit via an agent, provided as a unique code. When the phones next connect to the network, their transaction history is uploaded to the servers of the DFS system.

[83] Identity designs and platforms are covered in a separate ITU DFS FG study and hence will not be covered in great depth in this study.

[84] See also, McGowan, K (2015) *Know Your Customer is the Secret to MNO Negotiations*, available at http://technologysalon.org/know-customer-secret-mno-negotiations/ and Gidvani, L (2015) T*he Promise of Biometric KYC and Remote Account Opening for Branchless Banking in Pakistan*, available at http://www.gsma.com/mobilefordevelopment/programme/mobile-money/the-promise-of-biometric-kyc-and-remote-account-opening-for-branchless-banking-in-pakistan

[85] See www.fatf-gafi.org

Prepaid SIM registration is currently mandated in around 90 countries.[86] While SIM registration is often not sufficient KYC to open a DFS account, some jurisdictions where there is registration allow a DFS account linked to each SIM card under registration to be opened. SIM registration may sometimes be sufficient to open a DFS account that does not allow cash-out, with additional KYC information and verification required for full account functionality.

In some countries, the number of DFS accounts one person may have may be limited. In Jordan, for example, a user may only have two DFS accounts, even though they may have multiple mobile numbers and SIMs.

10.2 Technologies used

The lack of a verifiable address or similar document for onboarding and assisting in verifying identity for transaction purposes has been a handicap to these efforts. In addition, most of these onboarding and verification procedures have involved manual processes involving fragile documents.

With more countries insisting on identifying verification for SIM and DFS registrations and transacting, biometric-based onboarding and verification systems have emerged.[87] Initial implementations have involved capturing fingerprint data, with evolving implementations using Iris capture, bolstered by drops in costs for this technology.

In India, for example, Unique Identification Authority of India's national identity verification system uses a sequence of biometric capture devices to collect the biometric and demographic data of residents, store them in a centralized database, and issue a 12-digit unique identity number called Aadhaar to each resident.[88] It is considered the world's largest national identification number project.

Iris is becoming the preferred biometric capture method in DFS countries. This is set to increase with emergence of application programming interfaces (APIs) for Iris capture and phones with Iris scanners.

11 DFS payment infrastructure

11.1 Overview

Access to and integration with existing payments infrastructure for non-bank payment SPs is an evolving technical enhancement to DFS, especially as services between SPs become interoperable, some integrate into national payment switches, and some are given access to Real Time Gross Settlement Systems run by central banks. And, as stored value account holders are given companion GPR cards, DFS SP integration into card switches is also emerging.

A number of international technical standards ensure seamless technical implementation into payments infrastructure across the integration types.

---

[86] See further GSMA (2016b) *Mandatory 'Real Name' Registration By Prepaid Sim Card Users: Considerations For Policymakers*, available at http://www.gsma.com/newsroom/blog/mandatory-real-name-registration-prepaid-sim-card-users-considerations-policymakers/

[87] See, for example, Pakistan, where the Pakistan Telecommunications Authority mandated verification of all active SIM cards using biometric verification where every SIM owner was required to visit an operator outlet where their MSISDN and Computerized National Identity Card were confirmed or updated in the existing ownership database and fingerprints were matched with the National Database and Registration Authority. Gidvani (2015) *ibid*.

[88] See https://uidai.gov.in

11.2 Technical standards

Most payment infrastructures utilize a suite of standardized protocols for payment data messaging formats and security. These include: Device and infrastructure standards such as EMV standards; account numbering standards such as IBAN; data security standards such as Payment Card Industry Data Security Standard (PCI DSS), [89] and SSL; data formats such as Simple Object Access Protocol (SOAP);[90] IS0[91] 20022, [92] ISO 15022[93], and ISO 8583[94]; and SWIFT Messaging Standards;[95] and ISO 12812.

11.3 Technical implementations

At a technical or infrastructure level, the options for connecting non-bank SPs to each other are via a direct (bilateral) connection between the entities, or an indirect connection via an intermediary that sits between the entities. The latter may be a central processor, indirect connection to a switch, and direct connection to a national switch.

Bilateral **c**onnectivity could take the form of APIs that may include standard financial messaging such as ISO 8583 or ISO20022 and security protocols, or combined with proprietary APIs developed by platform vendors contracted to each party.[96]

In the central processor model, participants may form a consortium to build and possibly also operate a single transaction processing hub that will provide clearing and possibly also settlement. The technical specifications will be for their purposes and/or to fulfill any regulatory mandates where applicable. These specifications may include processing time, messaging formats, and security protocols.

As an example, the Central Bank of Egypt (CBE), the Egyptian Banks Company, and MasterCard in 2013 partnered to interconnect bank and non-bank DFS providers through a new central processing platform provided by Mastercard. Each DFS stored value account is associated with a real or virtual card in the wallet management and tokenization system. DFS transactions are tokenized and converted to card transactions, and from that point onwards use the existing payment card infrastructure to transfer the mobile stored value account-originated transactions among the banks like any other card transaction.

---

[89] The major credit card issuers created PCI compliance standards to protect personal information and ensure security when transactions are processed using a payment card. The standards include including PCI DSS, Payment Application Data Security Standard (PA-DSS), and PIN transaction security (PTS) requirements.

[90] SOAP is an acronym for Simple Object Access Protocol, a specification for exchanging structured information in the implementation of web-based services.

[91] An ISO standard is an international harmonized standard, agreed by consensus. Governments can adopt an ISO standard as a National Standard or may reference it in technical regulations. Businesses can use standards to promote interoperability and increase markets, reduce risk, and build customer confidence.

[92] ISO 20022 is an ISO standard for electronic data interchange between financial institutions. It describes a metadata repository containing descriptions of messages and business processes, and a maintenance process for the repository content. The repository contains a huge amount of financial services metadata that has been shared and standardized across the payments industry.

[93] ISO 15022 is the standard for the format of electronic message exchange as used in banking and commerce.

[94] ISO 8583 specifies a common interface by which financial transaction card originated messages may be interchanged between acquirers and card issuers. It specifies message structure, format and content, data elements and values for data elements.

[95] See for example, SWIFT MT message implementation guidelines available at http://www.swift.com/solutions/factsheet_downloads/SWIFT_Trade_Extract_Standards_Messages_Implementation_Guidelines_200811.pdf

[96] Tigo Tanzania, for example, uses the ISO 8583 standard and variants for its interoperability.

In Mexico, non-banks such as mobile payment providers are allowed by the Bank of Mexico to have direct access to SPEI, the country's Real-time Gross Settlement System. Similar integrated centralized payment switch models are implemented *inter alia* in Nigeria, Peru, Brazil, and Jordan.

12 Conclusion

- USSD is the dominant access and interface mechanism for DFS access, followed by STK and Java applets.
- User preferences have shifted from basic phones to feature phones, with a number of smartphones evolving, all driven by a swathe of new manufactures taking advantage of massive improvements in fabrication.
- Access channels could use evolving Internet-based mobile access methods such as WAP and application-based access mechanisms, both of which take advantage of the emergence of new feature phone and smartphones.
- Smartphones provide an enhanced interface and user experience for customers, offering access to a range of external DFS services not available for the text-based SMS, USSD and STK.
- Java applets providing DFS on feature phones are gaining in popularity.
- Merchant services in DFS are growing, with merchants implementing NFC-based and magnetic stripe-based POS devices to accept payments.
- While NFC-based payment facilities are growing, they are still smartphone-centric. NFC sticker technology can retrofit all phones with NFC capabilities.
- Sound-based access to DFS services is growing, but still in limited use.
- The thin SIM is an innovative technology being implemented to obtain alternative network access, and to secure DFS transactions.
- Iris is becoming the preferred biometric capture method in DFS countries. This is set to increase with emergence of APIs for Iris capture and phones with Iris scanners.
- There is an increasing trend towards the integration of DFS accounts with payment switches linked to magstripe and EMV debit cards.