DFS VENDOR PLATFORM FEATURES

ITU-T FOCUS GROUP ON DIGITAL FINANCIAL SERVICES

International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

FG-DFS

(02/2017)

ITU-T Focus Group Digital Financial Services

DFS Vendor Platform Features

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.

DFS Vendor Platform Features

About this Report

This report has been prepared by Chenshan, Huawei Technologies and Rob Reeve, VimpelCom. The report has been reviewed by the Technology, Innovation and Competition working group.

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

Table of Contents

LIST OF FIGURES

Executive Summary

The report provides insights and concepts shared by vendors and customers of DFS platforms who participated in the ITU Focus Group Digital Financial Services. This report captures all the functions, features and access options required to deploy and manage a mobile money ecosystem. It defines how potential interoperability can be supported – both with third parties and other mobile money operators. It also provides a reference modular architecture that supports the creation of complex account structures and services.

All these items have been collated to provider the regulator an understanding of all the elements that may be deployed. Regulators can then focus their efforts on the services already adopted, give clear guidance for security and data controls, and also prepare for new services that may be deployed as the ecosystem matures. This will allow the regulator to promote the common and general features of the platform they wish to advance in their market, it will give any potential operator an insight into the best practices for the system functionality – using a common framework to remove any potential ambiguity and allow regulators to provide clear guidance on the controls and mechanisms required in the relevant data sets and access channels. A vendor can advance their platform with the confidence that it will meet developing market needs within a robust regulatory framework.

1 Scope

This report describes the vendor platform features expected of a typical digital financial service (DFS) deployment, which includes access options, cooperation with third party partners, mobile money operator (MMO), MMO interoperability, service function, and system features, in order to present the recommendation and suggestions for the study phase.

2 Logic functional diagram of DFS vendor platform

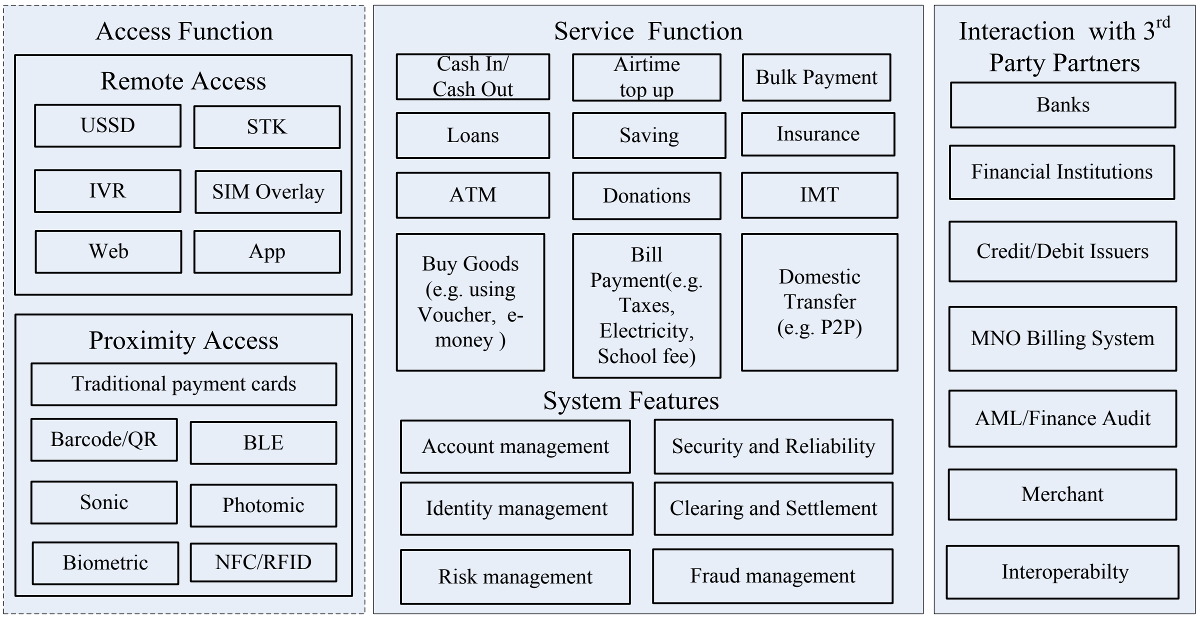

Figure 1: Functional diagram of DFS vendor platform

The following requirements would be beneficial to any DFS:

1. The solution could be built in modules with interfaces based on standard protocols that render each layer independently from any other layer in order to: Allow a distributed architecture; make it easier to integrate different provider modules; get a more secure topology (e.g. inserting firewalls between the front-end and back-end); and allow high availability (e.g. by means of load balancers).
2. The solution architecture could allow for different access channels including: User mobile and web applications; agent (e.g. shops and affiliated retailers acting as service branches) application to support customer-facing procedures; call centre (including interactive voice response (IVR)) access; point of sale (POS) for affiliated merchants (e.g. closed loop payments), etc.
3. The system can support connections to third parties. All financial transactions performed in the public domain should be transacted using a secured environment.
4. The solution architecture could allow third parties with the proper rights that are then duly authenticated to access a subset of system functionalities through an open application programming interface (API).

3 Access function

DFS in developed markets are making headlines because of their significant effort in virtualizing the physical wallet into one accessible via an electrical device, e.g. mobile phone or laptop. Whether for remote payments or proximity payments (often using radio frequency identification (RFID) or near field communication (NFC) technology), for consumers in developed markets (with ubiquitous mobile data available at ever lower costs and mobile broadband available at every corner coffee shop), it does not take a great leap of the imagination to envision a world of frictionless, cashless, and effortless mobile commerce. However, the story in developing markets is far different.

The section describes the multiple access options for the vendor platform to improve user experience.

3.1 Remote access

3.1.1 Unstructured supplementary service data (USSD)

USSD was built into the global system for mobile (GSM) specifications to support network operations. Later, a few operators began using it to interact with users for simple purposes like airtime top up and balance checks.

3.1.2 Subscriber identity module (SIM) toolkit (STK)

STK refers to the placement of a small application into the memory of a user's mobile phone SIM card. STKs are a popular user interface (UI) for MNO-provided DFS.

3.1.3 SIM overlay

SIM overlay (also known as thin SIM or skin-SIM) is a thin plastic cover or coating with an embedded chip that adheres to a SIM card, and effectively re-routes calls/short message service (SMS).

3.1.4 Interactive voice response (IVR)

IVR is an older, but tried-and-true technology, which is popular in call centres and allows a computer or other system to interact with humans. In the traditional set up, a customer receives a phone call on their mobile device and a pre-recorded message is played, which prompts the customer to use their mobile phone keypad to provide an input response (which leverages dual-tone multi-frequency (DTMF) signalling), which in turn is received by the computer system to record the response. Sometimes it is combined with a user-initiated SMS to a pre-defined phone number or short code (e.g., to initiate a peer-to-peer payment), which prompts an IVR phone call to the user.

3.1.5 Web access

For web access, the webpage is used to access the online payment platform e.g. PayPal, Amazon Payments, Google Wallet, Ali Payment, etc.

3.1.6 Application/in-app access

For application/in-app access are purchases made from within a mobile application. The purchasing process is completed directly from within the application and is seamless to the user, in most cases[1].

[1] Source: http://www.webopedia.com/TERM/I/in-app_purchase.html

3.2 Proximity access

3.2.1 Traditional payment cards

Plastic payment cards (e.g. Europay, MasterCard, and Visa (EMV) compliant 16-digit permanent account number (PAN)) are a popular and well understood method of payment, be it chip-and-PIN with an embedded chip (as is the norm in many parts of the world) or "swipe and sign" using a magnetic stripe (as in the U.S.). In developed markets, most customers carry several such cards, and many stores are equipped with POS machines to accept the traditional payment cards. Payment cards are durable, easy to carry, and, from the consumer perspective, an easy payment presentment method.

3.2.2 Radio-based NFC/RFID

NFC and RFID are mechanisms where devices enabled with NFC/RFID readers can "read" an NFC/RFID tag when they are in close proximity, usually within 10 centimetres. NFC is often thought of as requiring and leveraging a secure element; however, NFC/RFID can also be used on closed-loop contexts simply as a radio transmitter/identifier to convey transaction information. The RFID is significantly less expensive than NFC cards or tags containing a Secure Element. The popularization of NFC for DFS is only gradually taking off, and is especially popular in the context of a POS transaction, because information contained in NFC and RFID tags can be scanned very quickly, with minimal effort or input from the customer.

3.2.3 Barcode/QR code

A well-understood form of POS payment - and possible in developed market retail or supermarket locations - bar code readers use a laser reader or camera to "read" information stored on a barcode or QR code tag, often in the form of a sticker or presented on a mobile device.

3.2.4 Bluetooth low energy (BLE)

For Bluetooth-based POS payments, the terminal/mobile phone is paired with the POS via Bluetooth technology to transfer the transaction message. The payer should confirm the transaction on the screen of the terminal/mobile phone via a signature or password.

3.2.5 Sonic

A popular payment in automated vending machines, the sonic reader is integrated within the machine which "listens" for the appropriate payment information request from the application which is embedded within the sonic payment function feature. This is then transferred to a backend system for authentication and authorization.

3.2.6 Photonic payment

Photonic payment is a new mechanism using the flash lamp of a mobile phone. The photonic-based POS reads the information encoded in the light emissions from the mobile phone which integrates with the payment application.

3.2.7 Biometrics

Biometrics refers to metrics related to human characteristics and it is used in digital payment as a form of payer identification and access control. Examples of biometrics used in payment include, but are not limited to, fingerprint, face recognition, palm veins, etc.

4 Service function

4.1 Cash in

A customer can use an agent for cash in. The customer gives money to the agent requesting an e-Money account top up to a registered account. The agent receives the cash and sends the cash in request with the customer's identifier, e.g. mobile station international subscriber directory number (MSISDN) to the DFS Platform. The e-Money is transferred from the agent's account to the customer's account.

Note: A deposit voucher can be used to prevent the need for a customer's MSISDN being shared and is applicable to countries and regions with high requirements on privacy protection. The agent deposits money to the customer account using a deposit voucher without ever knowing the MSISDN.

4.2 Cash out

A registered customer can use an agent for cash out. The capital is transferred from the customer's account to the agent's account. There are different operational options present for the agent and customer.

4.2.1 Customer initiated

The customer asks the agent whether he or she has sufficient cash as well as the agent identifier. The customer will send the cash out request with the agent identifier, MSISDN, and appropriate authentication to the DFS Platform.

4.2.2 Agent initiated

The gent can initiate the cash out request instead of the customer, which the customer then accepts by providing their appropriate authentication.

Note: After obtaining a withdrawal voucher, a registered or unregistered customer can withdraw money using a voucher through an agent.

4.3 Savings

Savings are used to give the customer some interest in a given period. Dependent on the type of product, a customer may be able deposit/withdraw money to/from their savings account.

4.4 Loans

An organization can disburse funds for a loan. Funds are transferred from the financial institution, or group of individuals providing the loan directly to the applicant's individual account. A customer can request loans from the financial institutions and will also have the ability to repay these loans.

4.5 Insurance

A registered customer can make a request to buy insurance from the financial institution.

4.6 ATM

A registered customer, or a previously created voucher, can deposit/withdraw money to/from an e-Money account via an ATM.

4.7 Bill payment

A customer pays bills to organizations using e-Money in the DFS vendor platform. Through the DFS vendor platform, an individual customer can initiate a bill payment transaction for tax, water, tuition, electricity, gas, etc.

4.8 Airtime top-up

If a customer wants to recharge his or her airtime prepaid account, he or she can initiate a top-up request by self-service via a network device, over-the-counter (OTC), etc.

The DFS platform identifies the customer after receiving the request via a network device by self-service. After the identification is passed, his or her e-Money account balance will be deducted, and the DFS platform will work with the prepaid system, and recharge his or her prepaid account.

Via OTC, the DFS platform supports the top-up of registered and unregistered customers' prepaid accounts.

4.9 Buy goods

When a customer purchases goods at a merchant's store, they can pay using different methods, such as a traditional bank card (credit/debit card), QR code, voucher, etc.

4.10 Donations

Support donations to charitable organizations through the DFS platform. This works in the same method as a bill payment transaction.

4.11 Bulk payment（government to person (G2P) payment, salary distribution）

Allow organisations to issue an e-Money payment to their citizens or employees via a bulk file which they upload into the system. The system will process the bulk file and send the funds to the employee, including the ability to register an e-Money wallet.

4.12 Domestic remittance

4.12.1 P2P transfer (registered to registered)

A registered customer can initiate a money transfer from his or her e-Money account to another registered customer.

4.12.2 P2P transfer (registered to unregistered)

A registered customer can initiate a money transfer from her or his e-Money account to an unregistered customer. The DFS platform will identify the customer. After identification, the DFS platform will debit money from the registered customer's e-Money account, and then send a notification message to the unregistered customer. The message includes a voucher allowing the unregistered customer to withdraw the funds. The unregistered customer then needs to visit an agent, or appropriately configured ATM, to redeem the voucher. They may be asked to provide further identification and give cash in return for the e-money held in their account.

4.13 International remittance/international money transfer (IMT)

4.13.1 IMT sending

A registered customer can initiate a send money request through the DFS platform to debit the transfer amount form the customer's account held in the DFS platform to the users in a different or the same service provider system of different countries. The service provider system can be a DFS platform, bank, or any other kind of payment system.

An unregistered customer can also send money internationally via OTC.

4.13.2 IMT receiving

A customer can receive an international remittance via an IMT provider (or a specialist IMT broker who the service provider has partnered with), allowing e-Money to be credited into a customer's account from an international source.

5 System function

5.1 Security and reliability

The DFS vendor platform should ensure security from various aspects, such as applications, system, network, operation and maintenance, and privacy protection. Security features are provided based on security standardslocal laws and regulations.

5.2 Identity management

The DFS vendor platform should support the management of identity. Identity includes the end customer, business organization (e.g. agent or merchant), MMO, and service providers (e.g. vendors).

With the financial services regulatory requirements, the capture of customer data, its storage, and management requires robust and rigorous processes fully compliant with the required international standards (i.e. PA-DSS, etc. for card payments). With the separation of Identity Management function (rather than having it embedded in the accounts), governed with the appropriate information control, this function is expected to be the master record for the capturing and managing all information related to the costumer's identity, including:

- Processes for account registration and activation.
- Account data update.
- Account cancellation or blocking.
- Validation data capture and retrieval (physical or system capture).
- Validity management of data.
- Access to data for appropriately authorised users and systems.
- Performing the appropriate actions for registered services in case of any changes in the account status or data.
- If a PIN or password is used to securely identify the user, the life cycle must be managed: Issuing, reissuing, delivery, validation, blocking, unblocking, and deletion. Handling this securely is one of the hardest and more expensive parts of any payment system.

5.3 Account management

The DFS vendor platform should support the management of multiple accounts. Multi-account includes the internal account e.g. e-Money, bonus, points, or external accounts. The external account means the balance is not maintained in the vendor platform, but needs to reside in an external system, like online charging system (OCS)/ intelligent network (IN)/billing system or bank system.

Note: Regarding multi-currency, some countries are using more than one currency because of high inflation leading to their national currency being virtually unusable (for example, the hyperinflation in Zimbabwe) or other reasons. The DFS vendor platform should support more than one currency in the same system as different account holders might use different currencies, or the platform may be deployed to support more than one country at the same time.

5.4 Risk management

The DFS vendor platform should ensure that transactions are valid. The vendor platform collects service and transaction data to perform real-time or post-event analysis, tracing, and processing, implementing the automation of service monitoring and risk alarms, and conducting risk monitoring efficiently. The vendor platform provides the control and tracking of all risks relating to transactions. The rules management developed will depend on each country's regulations for each different service

5.5 Fraud management

Providing the control, tracking, and subsequent management of all fraud relating to transactions. The rules management developed will depend on each country's service regulations. This platform should be created by an independent team or external third party, to ensure the integrity of the fraud validation.

5.6 Clearing and settlement

The DFS vendor platform should support clearing and settlement. Based on different types of transactions, clearing can be classified by clearing in real-time (e.g. buy goods with immediate transfer of funds) and clearing at a deferred or regular time (e.g. bill payment). Settlement can be generated upon request.

5.7 Best practice for system function

To ensure maximum flexibility within the platform, the external and internal capability should be exposed via a service logic layer. The service logic layer will implement the service core logic as well as the necessary connectors to external third party systems. Service core logic should include the storage resources (e.g. user and tracking databases, system configuration database) and service functionality workflows (e.g. account management, money transfers, purchases, bill management, etc.) for any user profile (e.g. customer, agent, merchant, biller, etc.) and operations and maintenance (O&M) procedures (e.g. system administration, monitoring, tracing, etc.).

Since the core service features are based on the functionality provided by a set of financial capabilities, the platform must provide different modules implementing those capabilities, in order to:

- avoid a monolithic product;
- guarantee independence from a specific capability (to provide expansion and migration flexibility);
- allow other services to re-use those financial capabilities.

In addition, a business process modelling (BPM) tool will enable the company to implement end-to-end modelling of business processes as required to support rapid prototyping. Features could include:

- An intuitive design tool to capture business objectives;
- Automatic generation of application code (i.e. no need for programming by the service provider staff);
- Industry-specific solution frameworks such as those for banking BPM;
- Enterprise-level scalability;
- Standards-based user interfaces.

6 Reference architecture

The solution should be highly scalable, both instantiating new servers without adding any additional hardware (horizontal scalability) and upgrading platform components hardware with no loss of service (vertical scalability), being able to meet the needs of the current scenario (number of provisioned users), and rapidly scaling up to meet the needs of a more demanding one.

Each different software module and hardware component should be scalable independently from the rest of the modules and components, respectively.

The solution architecture should be comprised of standardized modules at different technology levels, enabling each individual component to evolve independently from the rest of the components.

The figure at Annex 3 represents a reference instance of an architecture for a DFS vendor platform to support a variety of services, which are covered in further detail in the remainder of this document.

This architecture should support:

- Modularity of logical components (for simple addition, removal or expansion);
- Components with configurable capability to support delivery in different regulatory markets;
- Separation of user experience, logic, and capability

6.1 Internal APIs

To facilitate the connectivity between all delivery elements, all communication should be exposed via well-documented open APIs.

The APIs have been structured into 3 key areas service, capability, and external.

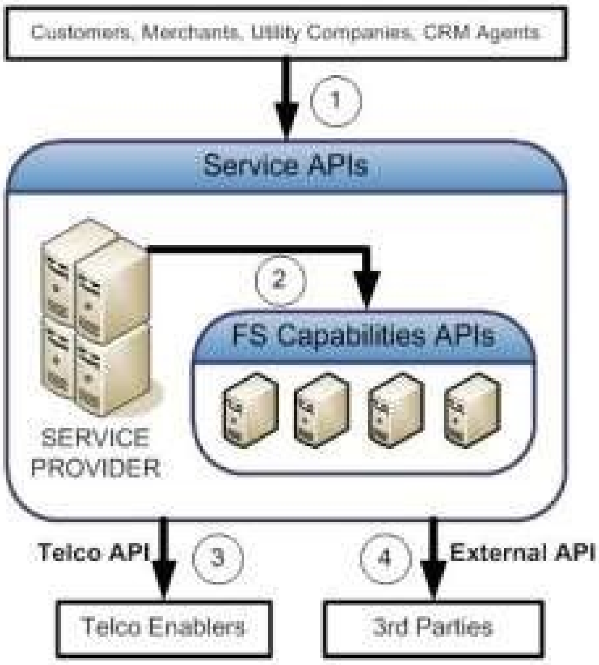

Figure 2: APIs of DFS vendor platform

Further information on each type is provided in the table below.

API type	**Description**
Service API	Service APIs are used to facilitate the delivery of user experience, irrespective of client platform. Services may be used directly with third parties for direct integration with their platforms, or integrated into web pages or mobile clients.
Capability API	All capability will be exposed via APIs to facilitate interaction with the service logic, or exposure as a service API.
External API	External APIs are used for integration with telco enablers and other third party capabilities.

Table 1: API types

7 Interaction with external third party partners

The ability to interact with other third party partners can help promote the development of the entire DFS ecosystem.

By extending the DFS ecosystem, the vendor platform can provide different methods in different scenarios to aggregate and interact with the peripheral partners. These include:

- Open API: Providing a set of APIs for third party partners to access the vendor platform and use DFS, i.e. banks, agents/distributors, remittance agents, payments, gateways, processors, etc. These interfaces are expected to be open standards, such as ISO 8583, or service-specific.
- Adapter: Providing adapters for the third party partners whose interface is already defined and stable.
- SDK: Providing SDKs to third party partners who use the vendor platform to deal with DFS transactions.

Note: In some countries the same DFS system is used for multiple banks via open API or adapter.

7.1 Open API

The vendor platform should integrate and interact with the third party partners by a set of APIs to facilitate DFS. Industry standardised – to ensure easier interaction with all parties in the eco-system in similar industries.

The vendor platform should provide two types of operations to the third party partners through API, transaction operation, and business operation.

- Transaction operation could include cash in, cash out, buy goods, bill payment, domestic transfer, etc.
- Business operation indicates management of system features, which includes account management, accounting, etc.

7.2 Adapter

The vendor platform provides adapters to the third party partners whose systems are stable or the interface is already well-defined. Adapters are used to convert the protocols of the partner’s system into protocols of the vendor platform, and vice versa.

The partner's system sends service requests to the vendor platform. After receiving service requests, the adapter parses the requests and matches elements in the requests with supported service elements in the vendor platform. After the requests are processed, the related processing results are returned through relevant responses.

The vendor platform generates transaction requests based on internal rules and sends service requests to the partner. After being converted into messages that the third party partners can identify through the adapter, transaction requests are sent to the third party partners.

7.3 SDK

An SDK provided by the vendor platform ensures the customer of the third party partners to pay with their e-Money account. The SDK is open to the third party partners (e.g. applications on Android or IOS platform), and should support platform services like purchasing goods, domestic remittance, bill payment, and so on. The SDK is integrated in application of the third party partners, and SDK is used to connect with the vendor platform.

8 Conclusion and recommendations

DFS platforms could leverage the features and functions from multiple vender platforms and could include multiple access options on the side of customers in different countries and for different electronic devices (e.g. computers, laptops, feature mobile phones, and smart mobile phones), the interaction with the third parties (e.g. banks, mobile operators, and interoperability) and the popular and normal service functions and system functions.

By identifying the common and general functions of the platform, regulators can focus their efforts on the services already adopted, give clear guidance for security and data controls, and also prepare for new services that may be deployed as the eco-system matures.

Promote the common and general features of vendor platform: This technical report cannot cover all of the features and functions for all vendor platforms. Only the common and general features and functions are present, such as USSD, NFC, and web apps from the view of remote and proximity access, the top services, such as cash in/out, remittance, and critical system functions, such as security and account management.

The vendor platform features expected of a typical DFS deployment should include access options, cooperation with third party partners, interoperability, key service functions, and system features. A reference instance of an architecture for a DFS vendor platform to support a variety of services is present within the report.

Using the best practice for the system function can make it easier for any operator to implement and deploy the vendor platform. The reference architecture will provide more details about how to potentially structure the vendor platform – with separation of functionality to ensure clear understanding of any regulatory requirements for an implementation. The specifics pertaining to capabilities and technologies are present for reference as a best practice, and supporting future extensions of the initial services, such as the BPM tool (to support prototyping) and the specific account and identity model.

Regulators need to consider the advancement of future services – many services will be combined to create new services. By providing clear guidance on the controls and mechanisms required in the relevant data sets and access channels, a vendor can advance their platform with confidence that the platform will meet developing market needs within a robust regulatory framework. A good example is identity capture – many current regulatory processes require the capture of physical paperwork, however digital techniques and processes can overcome the weaknesses in such a process.

Annex 1: Glossary

Term / Acronym	Description
ATM	Automatic teller machine
DFS	Digital financial service
G2P	Government to person
IMT	International money transfer
NFC	Near field communication
OTC	Over the counter A transaction taking place directly between a consumer and merchant. The merchant then facilitating the DFS transaction to the end recipient
POS	Point of sale
P2P	Person to person
RFID	Radio frequency identification
SDOs	Standards developing organizations
STK	SIM tool kit
Token or Tokenization	Something of low value representing something of high value (e.g., EMVCo. Specification for replacement of permanent account number (PAN) with one-time token). EMVCo exists to facilitate worldwide interoperability and acceptance of secure payment transactions.
USSD	Unstructured supplementary service data: A rudimentary mobile telecom-controlled technology that provides a text-based connection to many GSM mobile phones.

Annex 2: Platform capabilities captured in reference architecture

This section provides further insight into services that the platform may offer – it has been used to provide a benchmark/point of reference for provision of a full financial service eco-system; differing capabilities are required, depending on the maturity of the market.

1 Loan management

This capability could support the following functionalities:

- **Type of lending/credit -** such as revolving or refill credit, variable limits, variable loan periods, variable payment types, variable periods for repayments, variable amortisation types;
- **Credit amounts** - varying credit limit creation either at the customer or product level;
- **Physical documents** - the capture, storing, and retrieval of physical documents;
- **Disbursement to wallet or current account**;
- **Interest rates** - at a product or account level, this can be any combination of fixed and variable rates;
- **Loan refinancing or restructuring** - including identification of customers requiring this;
- **Loan renewal** - either automatically or based on customer changes;
- **Instalments** - various scenarios or extension of a grace period;
- **Late payment fees** - varying fees and support for applying the local taxes where relevant;
- **Calculation of interest or fees** - varying interest rates or fees and how they are applied depending on the local regulation;
- **Instalments payments hierarchy** - a hierarchy of payments which determines which items are paid off first such as: (1) Overdue fees (2) Overdue interest (3) Regular interest instalment portion (4) Main capital instalment portion;
- **Loans classification based on payments overdue**;
- **Advance payments**;
- **Customer statements** – either physical or digital;
- **Loan payments**;
- **Payment reminder and overdue alerts** – either automatically or at a predetermined time, with varying communication channels.

2 Credit scoring

The ability to set a customer credit score via a number of inputs such as: customer identification data; telco transactional data; inputs for external reference data (e.g. bureaus); social media data; and mobile financial services data.

3 Decision engine

The purpose of the decision engine is to ensure that any automated controls are captured and evidenced – to support any approval or rejections of a customer’s requests for any services. This capability could support as a minimum:

- **Data entry** - output data for a customer’s approval;
- **Digital storage** - with the capability to prove that any legal documentation signed or provided by the customer has not been tampered with – either physically or digitally.

4 Accounts structure

The following section provides further insight on how the accounts structure could be created to support complex relationships with a customer from the same DFS platform. The following are representative, and non-exhaustive, so a variety of different approaches may exist.

4.1 Any customer account could be hierarchically dependent on any other account.

Account hierarchy: Accounts that are different (with different User IDs), but are nested.

One account that could have one (or none) superior account.

One account that could have an unlimited number of subordinate accounts valid for any type of accounts (end users and companies).

Useful for hierarchical managing & reporting operations.

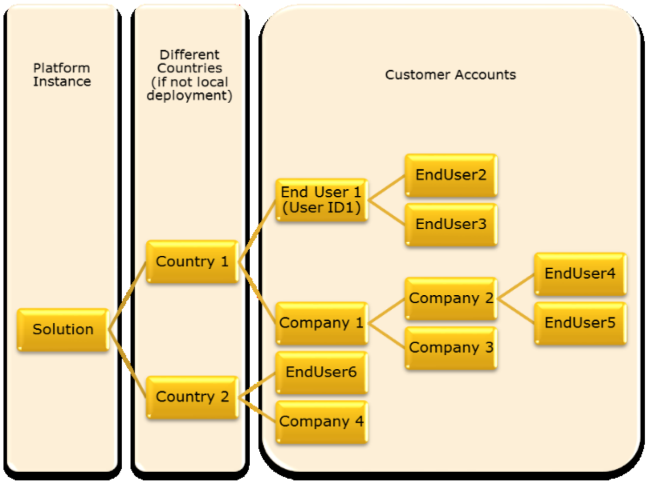

Figure 3: Possible account logic 1

4.2 Each customer account must have (at least) one stored value account (SVA)

The first SVA will be automatically generated within the account sign-up process. Additional SVAs could be associated with the same customer account later on. For KYC purposes, a SVA must not be associated with more than one customer account (user ID), however, the customer may provide access for other parties to use the account, i.e. family members or employees.

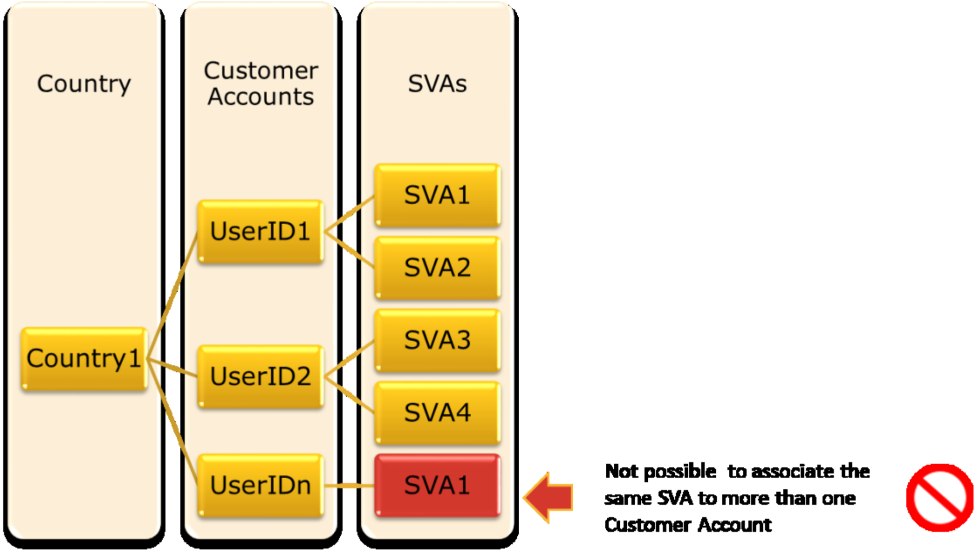

Figure 4: Possible account logic 2

a. Each SVA may also have a prepaid debit or companion card issued or linked to the account.

The prepaid card number being automatically generated within the SVA generation process, or once a companion card is issued.

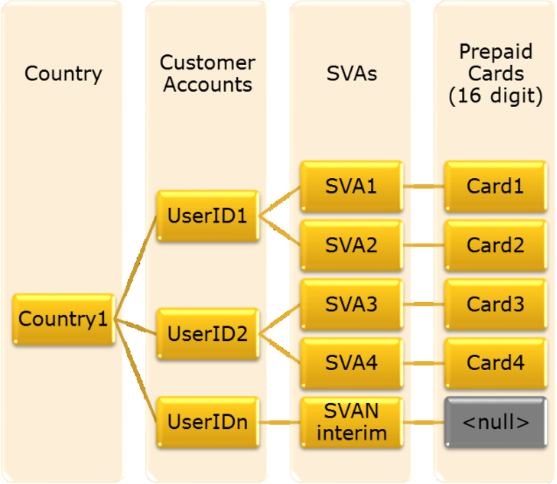

Figure 5: Possible account logic 3

b. Each SVA may also be associated with (at least) one MSISDN

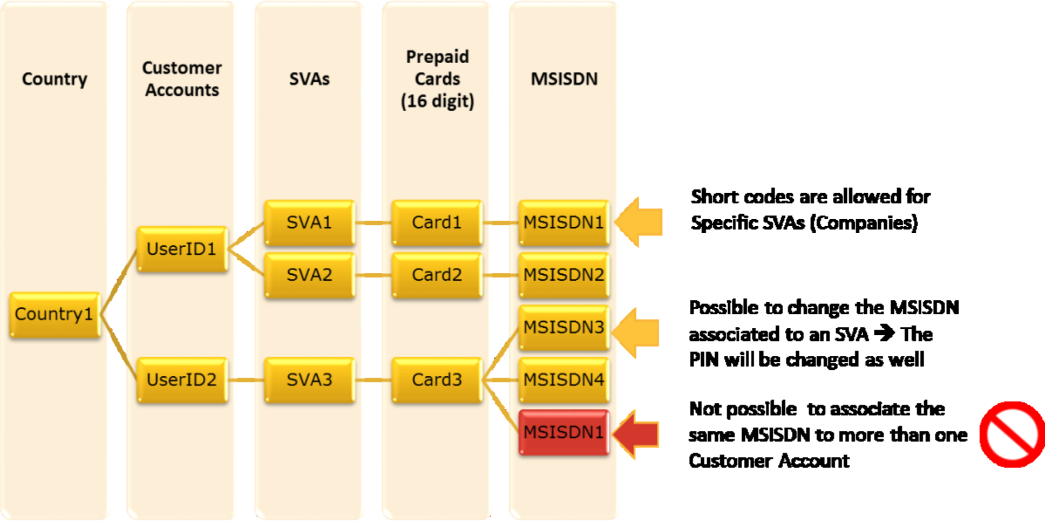
Country
Customer Accounts
SVAs
Prepaid Cards (16 digit)
MSISDN
Country1
UserID1
UserID2
SVA1
SVA2
SVA3
Card1
Card2
Card3
MSISDN1
MSISDN2
MSISDN3
MSISDN4
MSISDN1
Short codes are allowed for Specific SVAs (Companies)
Possible to change the MSISDN associated to an SVA → The PIN will be changed as well
Not possible to associate the same MSISDN to more than one Customer Account

Figure 6: Possible account logic 4

5 Credit account

A credit account will have the same transactional capability as the SVA, but also supports a negative balance being created, and managed appropriately. It could also support: The account permitted to go into credit; fees for a configurable period; charging of interest e.g. x.xx per cent for a configurable period; potentially multiple accounts per customer – each account with different parameters.

6 SVA

The SVA will provide a prepaid account issued by the service provider (or partner financial institutions). The movement of funds will be available through a variety of sources: cash in; money transfer; card loads; cash out.

The SVA capability will provide a master record of the customers' available funds, points, or other units of currency (including virtual) to allow them to transact. This capability will also deliver the required payments of money transfer authorisations, ledger balance updates, refunds and reversals, as well as settlement processes both with merchants when operating in a closed loop or with the external clearing houses when operating in open loop, applying adequate transactional rules, such as timing delays for specific merchants and providing dispute resolution tools.

When a transaction is performed, the SVA will identify the sender and receiver of funds, applying the appropriate risk and fraud rules associated with the service being facilitated.

The platform should support multiple separate accounts per customer – each account with different parameters.

7 Issuer processing

In association with the accounts, users could have a plastic or virtual prepaid card using the identification number of an established payment card network such as Visa, MasterCard, or any other international payment schemes (IPS). The issuer processing capability will pass authorisation and settlement requests on to the various accounts for processing. This number will identify the customer when performing an open loop transaction, applying appropriate risk and fraud rules and ledger balance updating. All of the required actions to guarantee transaction integrity must be performed to avoid data loss or duplicity. This capability must be able to handle the periodical clearing and settlement processes defined by the plastic or virtual card issuer.

To support the creation of physical and logical cards, in addition to the payment process, the DFS platform may also have all the systems and processes required for the creation of physical plastic, or an NFC enabled card (both physical and virtual) as needed.

8 Payment planning

Payment planning is the customer's ability to establish future payments which support the following scenarios:

- Upon receipt of an eInvoice;
- upon entry of specific data;
- with business and user configurable reminders being issued:
- to advise the transaction is due;
- to advise the transaction is due without sufficient funds;
- to advise the transaction has concluded.

9 Trigger management

The platform can also initiate specific tasks primarily in response to a time-based event. The platform supports at minimum: Modification of accounts based on a change in age (e.g. parent/child accounts upon reaching the age of 18); transaction flows initiated upon an account reaching various configurable funding levels (max and min, as well as multiple levels in between either as a percentage or a specific value) i.e. automatically top-up airtime if balance is below 2USD; transaction flows initiated at a specific date in month i.e. a date set in payment planning.

10 Payment instrument vault

A PCI-DSS compliant database capturing all the information for methods of payments a customer has registered (i.e. cards, direct debits, etc.). The database also includes all the information on the channels and methods a customer needs to manage the service.

11 Compliance management

This platform should support: Accurate compliance monitoring and reporting; surveillance, detection, and event correlation i.e. alerting if a server cabinet is accessed and creates a potential exposure for PCI DSS, but cross-referenced to an authorised repair incident; a consolidated repository of all compliance libraries – i.e. risk and controls mapping to processes captured in BPM tool; managing the full cycle of new and changing regulations; lower regulatory risk through cross-channel coverage.

12 Payment capability

Payment capability provides the logic to manage how a transaction needs to be processed – using either business rules to match payment instruments with accepted methods of payment, or issuing a request for the consumer to select from their available options - direct to bill, direct debit, eMoney ledger, or cards. Payment capability also facilitates one-off or subscription-based transactions.

Payment capability can also have the ability to split a transaction into multiple flows, i.e. split payment authorisation, associated offers and coupons, and fraud validation of the transaction. Then reconsolidate to provide an authorisation or rejection.

13 Limit management

The platform could allow for configuration of the following parameters on a per instance level: Minimum transferred amount per transaction; Maximum transferred amount per transaction; Minimum remaining balance after transaction including taxes and service fees (where applicable); Maximum number of transactions per day. There could be an option to set this limit for transfers from each type of balance (airtime, mobile wallet, linked bank account).

Maximum value of transactions per day (calculated as maximum transferred amount per transaction times the maximum number of transactions per day). There could be an option to set this limit for transfers from each type of balance (airtime, mobile wallet, linked bank account).

Maximum number of transactions per month. There could be an option to set this limit for transfers from each type of balance (airtime, mobile wallet, linked bank account).

Maximum value of transactions per month (calculated as maximum transferred amount per transaction times the maximum number of transactions per month). There could be an option to set this limit for transfers from each type of balance (airtime, mobile wallet, linked bank account).

Maximum number of unsuccessful transfer attempts per day. This is required to prevent distributed denial of service (DDoS) attacks on the platform, i.e. account is blocked until 00:00 the next day after three unsuccessful transfer attempts. Maximum number of reversal requests per day.

Maximum number of transactions per x period for a certain destination (particular merchant or transfer recipient).

14 Address management

The ability for a customer to enter multiple addresses that can be validated via external data sources, or when goods or products are issued to the address. There should be clear identification of the date entered, and all modifications or validations.

15 Blacklist/whitelist

The ability to identify addresses, names, and customer identification that should be flagged as either acceptable or to refused.

16 Remittance hub

A service to facilitate international remittance activity, where additional information may be required to support a normal flow, i.e. enhanced limits, FX (Foreign Exchange Rate) and KYC processes. However, this service will share the cash in, cash out service, as well as calling the SVA, payment instrument store, payment capability, and identity management services.

17 Payment gateway

The platform should be able to act as a full payment gateway where necessary, supporting: Integration with the IPS for onward processing; allowing transaction data to be sent directly from the customer's browser to the gateway, bypassing the merchant's systems without redirecting the customer away from the website; forwarding transaction information to the payment processor for authorisation (with support from multiple schemes, both traditional card-based and alternative wallets); onward validation or rejection to the merchant of the success of the transaction; clearing and settlement processes for the merchant back end both in real time and batch modes; clearly assignable liability management to support various authorisation models; implementing EMV level compliance of transaction handling.

18 Payment switch

The platform could also act as a full payment switch, supporting where necessary: Integration with the IPS for onward processing; integration with local issuers; integration with local payment gateways and payment processors; integration with local ATM capability; onward validation of requests for authorisation; onward validation or rejection to acquire functions of the success of the transaction; clearing and settlement processes for the issuer and acquirer's functions both in real time and batch modes; EMV level compliance of transaction handling.

19 User preferences

Providing the appropriate: Hierarchy; registering; secure ID management; blocking and unblocking; managing of specific business rules and fees associated with user activity and services.

20 Merchant preferences

Providing the appropriate: Hierarchy; registering; secure ID management; blocking and unblocking; managing of specific business rules and fees associated with merchant activity (including creation of merchant, stores, and employees).

21 Agent preferences

Providing the appropriate: Hierarchy; registering; secure ID management; blocking and unblocking; managing of specific business rules and fees associated with agent activity (including creation of super agents, agents, stores, and employees).

22 Receipting

The platform could support the creation of digital receipts for all transactions created that can be stored in a consumer's cloud account for subsequent warranty and returns claims - the data should be both searchable and retrievable for consumers and accessible by the consumer profiling services for data mining, and insurance products for simpler insurance creation.

23 eInvoicing

The platform could support the creation of electronic invoices (eInvoices) to provide electronic bill presentment where necessary: Merchant or utility companies; consumers marking an invoice as in dispute and appropriate remediation processes to bring to resolution; issuing a configurable set of reminders at set intervals to a consumer for eInvoices nearing or exceeding due date.; merchant monitoring and tracking of all outstanding or due invoices; configurable events to allow for chasing reminders to be sent, and, in worst case scenarios, onward processing to a debt collection agency; the payment capability supporting partial and full payments and reconciliation of any eInvoices.

24 Liability management

The platform could provide monitoring, tracking, and reporting of all liabilities for merchants and agents it should support, where necessary: Identifying amounts due to or owed by consumers, merchants, and agents with segregation of when such items become due; identifying amounts awaiting settlement or reconciliation.

25 Cash management

The platform should support reporting of cash floats available at merchants to ensure that there is sufficient liquidity in the ecosystem. It should also support reporting of the following: Liquidity management and risks; cash available or required at a specific location; cash available or required in a specific geographic region.

26 Financial reporting

The platform could have the ability to create regulatory compliant financial reports and accounting procedures, supporting its own internal general ledger.

27 Insurance

The platform should support the sales of, in-life management, and the reporting, monitoring, and management of all insurance services offered - including configurable levels of document retention management.

28 Customer relationship management (CRM) / customer support / back office case management

Providing the core platform for supporting and tracking any incidents related to financial services. Providing the ability to move incidents between appropriately structured queues allowing dedicated teams to respond. As some queues will monitor and respond to highly sensitive and confidential information, the appropriate controls and monitoring are implemented to ensure full compliance.

29 Business intelligence / data warehouse

The platform could provide a repository for all data, relating to the service for its subsequent analysis, reporting, and creation of statistics - including ID management and business data as transactions, operations, and methods of payment. This information is being used by customer support staff, for back office purposes, and, where appropriate, by agents and partners.

30 Acquirer processor

The platform could provide the services for acquirer processing, supporting where necessary: Integration with the IPS for onward processing; merchant acquisition and account management; dispute and resolution management; clearing and settlement processes with deferred payments for different merchant categories; clearing and settlement processes for the merchant back end - both in real time and batch modes; clearly assignable liability management to support various authorisation models implementing EMV level compliance of transaction handling.

31 POS service management

The platform could support the deployment of multiple POS terminals, with capabilities such as: Delivery and installation management of POS & mobile POS (mPOS); manufacturer warranty management; hardware break fix tracking and management; field force management.

32 Virtual POS (vPOS) management

The platform could support vPOS management to support the rapid deployment of new functionality to the POS terminals, either in the traditional POS or mPOS environment.

33 Consumer data storage

A storage capability to store digital receipts, photo images of receipts, and additional items, as required.

34 Merchant data storage

A storage capability to store digital images of products, contracts, and additional items, as required.

Annex 3: Reference architecture

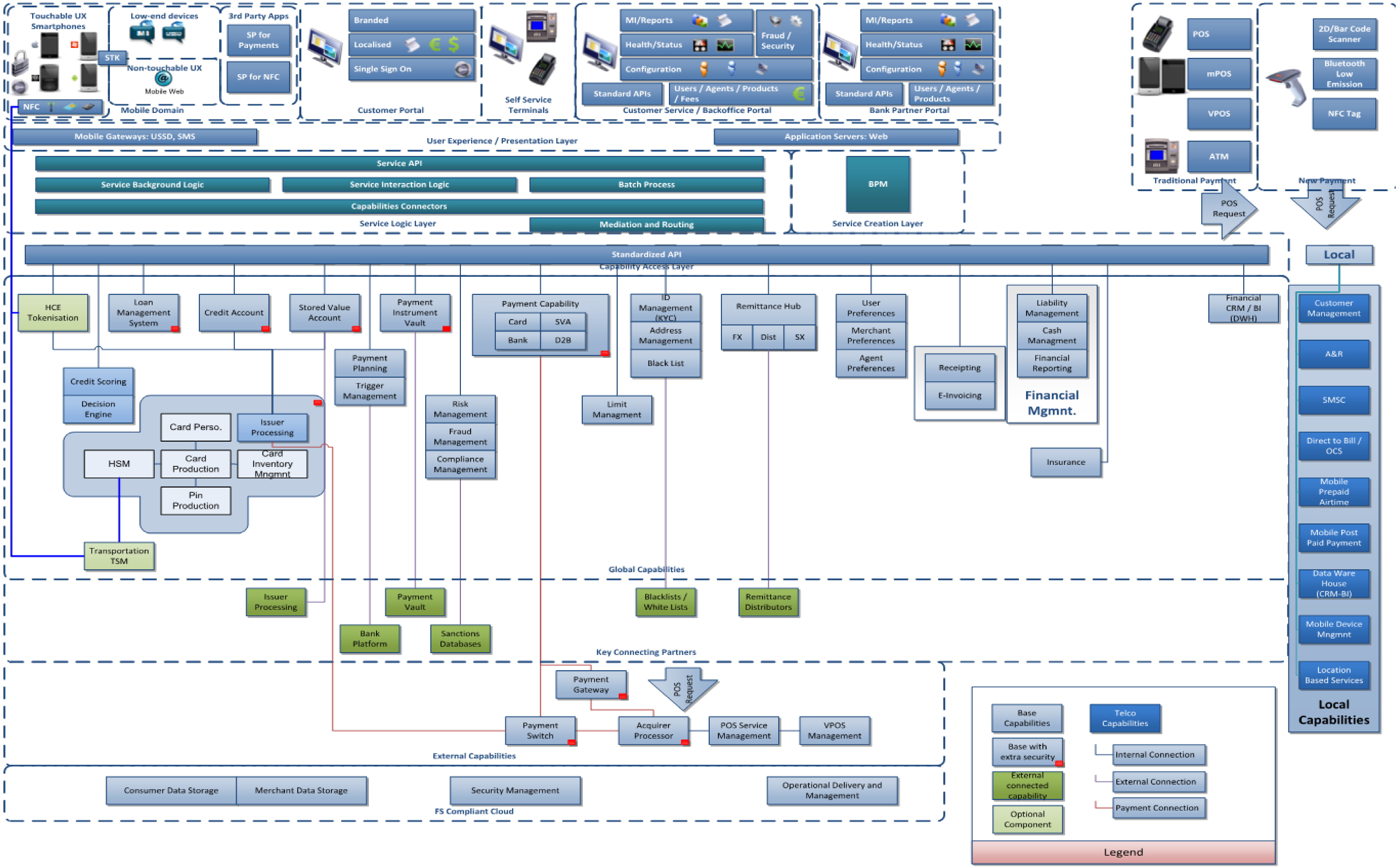

Figure 7: Reference architecture of DFS vendor platform

List of acronyms used in the different layers in the reference architecture in Figure 7

User Experience

- Touchable UX/Smartphones – mobile devices with a touchable user interface.
- STK – Sim Tool kit, an application residing on the SIM
- SP for Payments – Service provider for payments
- SP for NFC – Service Provider for other Near Field Communication services (i.e. transportation or access control)
- MI/Reports – Management Information and Reporting Modules
- API – Application Programming Interface
- POS – Point of sale device, dedicated terminal used to accept card payments
- mPOS – mobile Point of Sale terminal – additional hardware, once connected to a mobile device, creates a secure payment terminal
- VPOS –Virtual Point of Sale software – software that allows a PC or other internet device to act as a secure payment terminal
- ATM – automated teller machine

Service Logic

- BPM – Business Process Modelling

Financial Services Capability

- HCE Tokenisation – Host Card Emulation Tokenisation. Provision of security tokens to eliminate the need to send sensitive data (such as card information) to the mobile device. The token is instead converted into real card data at the time of transaction processing.
- Card Perso. – Card personalisation. Secure manufacturing process required to add relevant identifiers to physical card
- HSM – Hardware Security Module
- Transportation TSM – Transportation Trusted Service Manager – to facilitate transfer of relevant secure transportation data to a device
- SVA – Stored Value Account
- D2B – Direct to Bill – mechanism to use the mobile balance as the source of funds. Sometimes referred to as Direct Carrier Billing.
- KYC – Know Your Customer – process to capture and validate a customer’s identity
- Remittance FX – Foreign Exchange mechanism, to identify the current rate of foreign exchange
- Remittance Dist – database supporting the distribution mechanism for funds – i.e. merchants and agents involved in remittance flows
- Remittance SX – Settlement mechanisms and controls for settling remittance flows
- Financial CRM – dedicated Customer Relationship Management

- Financial BI – dedicated Business Intelligent Module

Telco Capability

- A&R – Access and Registration systems
- SMSC – Short Message Service Centre
- Direct to Bill/OCS – Online Charging Service

____