International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

P.1502
(01/2020)

SERIES P: TELEPHONE TRANSMISSION QUALITY, TELEPHONE INSTALLATIONS, LOCAL LINE NETWORKS

Methods for objective and subjective assessment of quality of services other than speech and video

---

Methodology for QoE testing of digital financial services

Recommendation ITU-T P.1502

ITU-T

ITU-T P-SERIES RECOMMENDATIONS

TELEPHONE TRANSMISSION QUALITY, TELEPHONE INSTALLATIONS, LOCAL LINE NETWORKS

Vocabulary and effects of transmission parameters on customer opinion of transmission quality	P.10–P.19
Voice terminal characteristics	P.30–P.39
Reference systems	P.40–P.49
Objective measuring apparatus	P.50–P.59
Objective electro-acoustical measurements	P.60–P.69
Measurements related to speech loudness	P.70–P.79
Methods for objective and subjective assessment of speech quality	P.80–P.89
Voice terminal characteristics	P.300–P.399
Objective measuring apparatus	P.500–P.599
Measurements related to speech loudness	P.700–P.709
Methods for objective and subjective assessment of speech and video quality	P.800–P.899
Audiovisual quality in multimedia services	P.900–P.999
Transmission performance and QoS aspects of IP end-points	P.1000–P.1099
Communications involving vehicles	P.1100–P.1199
Models and tools for quality assessment of streamed media	P.1200–P.1299
Telemeeting assessment	P.1300–P.1399
Statistical analysis, evaluation and reporting guidelines of quality measurements	P.1400–P.1499
Methods for objective and subjective assessment of quality of services other than speech and video	**P.1500–P.1599**

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T P.1502

Methodology for QoE testing of digital financial services

Summary

Recommendation ITU-T P.1502 is based on the end-to-end quality of service (QoS) key performance indicator (KPI) definitions first published in the ITU-T Focus Group Digital Financial Services Technical Report "QoS and QoE Aspects of Digital Financial Services" (see [b-DFS TR] in the bibliography). It details the methodology and connects to a field test using this methodology which has been conducted in Ghana in the first half of 2018.

Money transfer from end user devices to other devices or to other entities has become an important element of everyday life in many countries. This service, however, relies on the functionality of mobile networks. Therefore, a connection exists between the functioning, QoS and quality of experience (QoE) of money transfer services, and the QoS and proper functioning of those mobile networks, and respective quality metrics and testing methodologies need to be defined.

The main part of the present Recommendation describes the testing methodology.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T P.1502	2020-01-13	12	11.1002/1000/14160

Keywords

Digital financial services, QoE, QoS, quality of experience, quality of service.

* To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

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 World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Page

Introduction

Regulators of both the financial and the telecommunication sector are encouraged to collaborate in using the present report as an initial toolbox for the assessment of digital financial services (DFS) related aspects of QoS and as far as possible as QoE.

DFS applications preferred by customers will swiftly change in functionality, structure and thus also in complexity. These changes will differ by country or region, and international interoperability will add even more complexity.

There is not, and there will not be a particular QoS and QoE test suite that could be applied to all DFS applications. Therefore, the challenge for regulators of both sectors is to use the present document to define QoS and QoE test suites tailored to the needs in their country or region such that customers can rely on smoothly flowing DFS services which can be trusted as much as the many other utilities that keep an economy up and running. Regulators are encouraged to exchange their approaches towards QoS and QoE test suites with their counterparts in other countries or regions.

The present Recommendation is based on the end-to-end QoS KPI definitions first published in [b-DFS TR]. Furthermore, it follows the recommendations provided in [ITU-T G.1033]. The Recommendation details the methodology and connects to a field test using this methodology which was conducted in Ghana in the first half of 2018.

Money transfer from end user devices to other devices or to other entities has become an important element of everyday life in many countries. This service, however, relies on the functionality of mobile networks. Therefore, a connection exists between the functioning and the QoE of money transfer services, and the QoS and proper functioning of those mobile networks, and respective quality metrics and testing methodologies need to be defined.

The main part of the present Recommendation describes the testing methodology.

Annex A describes basic tests on a target service prior to setting up a testing campaign. Annex B describes check lists to be used in testing campaigns. Annex C provides an overview table of KPIs and related trigger points.

Furthermore, appendices provide specific information on the pilot testing campaign itself, which was performed in Ghana in the first part of 2018. Appendix I shows the device set-up for the Ghana pilot; Appendix II shows the naming rules, data structures and related processes used in the pilot project; Appendix III gives an overall description of the Ghana Pilot Campaign, and Appendix IV illustrates campaign log examples.

Recommendation ITU-T P.1502

Methodology for QoE testing of digital financial services

1 Scope

This Recommendation describes the QoE assessment methodology for the "Person-to-Person" (P2P) money transfer use case. The methodology is designed to be easily extended to other use cases in future revisions of this Recommendation.

It is important to understand that this Recommendation only covers the methodology for tests done from an individual user's (end-to-end) perspective, acting within a given DFS ecosystem under current load conditions.

NOTE – It may be desirable to extend the scope of testing to capacity tests, which would involve creation of defined load scenarios to a DFS ecosystem to determine the robustness of DFS functionality under these conditions. Such extensions can be easily created from the methodology described in this Recommendation. Their execution is mainly a matter of scale of required resources.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T G.1033] Recommendation ITU-T G.1033 (2019), *Quality of service and quality of experience aspects of digital financial services*.

3 Definitions

None.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

DCS Data Capture Sheets

DFS Digital Financial Services

DID Device Identifier

E2E End-to-end

FPx Feature Phone x

ID Identifier

IP Internet Protocol

KPI Key Performance Indicator

MOMO Mobile money

NSMS Notification SMS

OPx Observer Phone x

P2P	Person to Person
PCO	Point of Control and Observation
PFT	Pilot Field Test
PIN	Personal Identification Number
POO	Point of Observation
QoE	Quality of Experience
QoS	Quality of Service
RAT	Radio Access Technology
SIM	Subscriber Identification Module
SMS	Short Message Service (also used for a single text message transmitted by SMS)
SPx	Smartphone x
STK	SIM Application Toolkit
TA	Transaction
TPID	Trigger Point ID
XML	Extensible Markup Language

5 Conventions

The following terms are used in an interchangeable manner:

Working name or definition	Term/Alias
DFS (Digital Financial Services)	MoMo (Mobile Money)
A or B party, account (actually the representation of a user's account on a mobile device or another type of terminal equipment)	Digital wallet, wallet
PFT (pilot field test)	Only internal use to designate the pilot test campaign in Ghana
TA	Transaction
ObsTool	Observer Tool: User Equipment running software for active and passive network testing

It is important to note that digital financial services in most cases cannot be understood as "standardized services" like telephony or facsimile, but rather as applications having an internal functionality which is not known to the general public and may also change over time without prior notice.

6 Test scenario under consideration

In the following, the "Person-to-Person" (P2P) money transfer use case is described. The methodology is designed to be easily extended to other use cases in future projects.

6.1 Roles and entities

A Party and B Party	Formal roles for transfer, e.g., A (active role) transfers money to B (passive role).
SPx and FPx	Designation of device types used for a transfer, Smartphone x, Feature phone x.
Dx	More general indexed device description (e.g., D1, D2…)
OPx	Observer phone x
Px	Person x, designation of a tester/operator (independent of role)

NOTE 1 – The testing methodology corresponds to a round-trip transfer consisting of N transactions. Consequently, roles between devices and operators are switched after every transaction.

NOTE 2 – In order to optimize testing efficiency and to minimize the risk of errors during the test preparation, the assignment of devices to accounts should be fixed. Consequently, the assignment of roles is being switched between the devices in a cyclic manner (practical example: Smartphone placed to the left and feature phone placed to the right of a person during manual tests). This is to ensure that the manual cycle of tests is uniform to the transaction cycle as illustrated in Table 1.

6.2 Action Flows

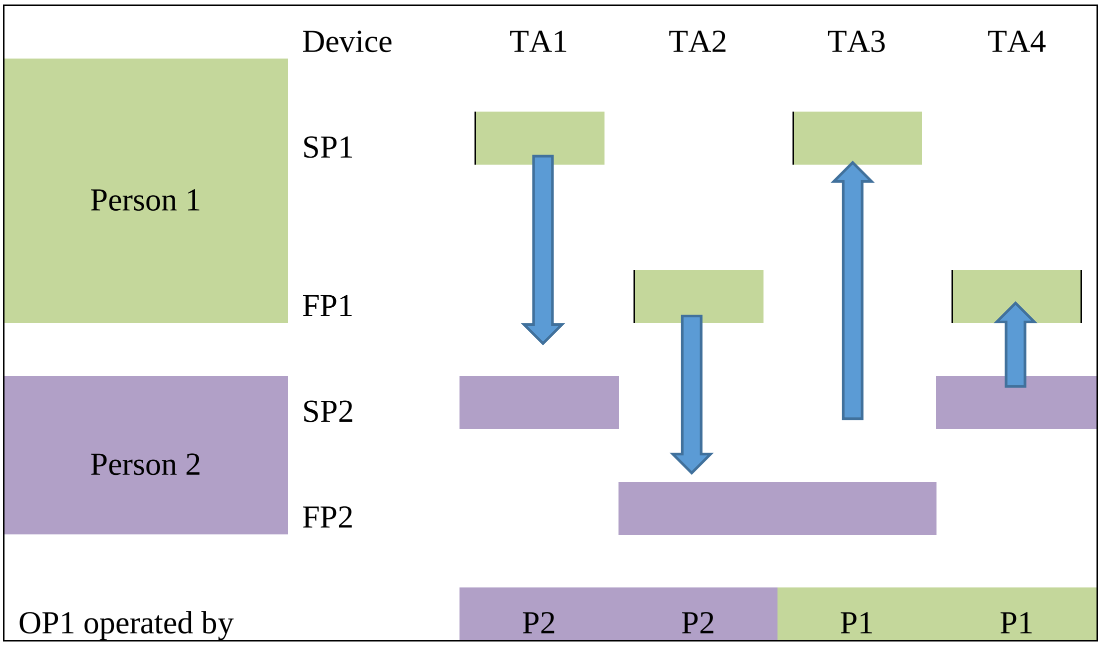
Test are typically conducted by a team of two persons, named P1 and P2. Alternative team sizes (e.g., five persons, where four persons are assigned to the testing phones and one person operates the observer phone) or the option to use more than one team per location are for further study. Based on experience made so far, it appears that any such solution should be accompanied by increased tool support (such as partly automated time-taking as described in clause 11). Doing uniform, repeated testing over a longer period of time is strenuous; tool support will therefore help to maintain high data quality.

A single transfer will be done by this team, acting in the roles of A and B party, respectively.

In parallel to the actual transfer action, the person designated as P2 also operates the observer phone (as P1, in the A party role, is engaged with performing the transfer while P2 in the B party role is mostly idle with respect to the money transfer).

A cycle of transfers consists of four (4) transactions, using all combinations of smartphones and feature phones assigned to the A and B party roles. After this cycle, the money transferred (less operator charges) is again available on SP1 and FP1, respectively.

Table 1 – Role and activity assignments during a 4-transaction cycle



6.3 Test parameterization and neutral starting state

A particular property of systematic service tests is a frequency of service usages which is significantly higher than the usage frequency created by a typical end user.

While a high testing frequency leads to a high yield of samples for computation of QoS KPIs, it is conceivable that the system has a certain "dead time" after each transaction, where the system would not accept a new transaction or create unexpected results of a transaction attempted within this period of time. It is advisable to be aware of this possibility and to obtain relevant information before the actual parameters of a test campaign are determined.

The testing frequency can be controlled by the pause between transactions, which also acts as a guard time to allow the service under test to reach its neutral state again. The respective considerations are in full analogy to the testing of e.g., telephony.

A testing campaign, therefore, should contain a pre-testing phase with systematic tests to make sure that usage frequencies typical for testing do not affect testing results with respect to the end-user perspective.

As the starting hypothesis for systematic testing, it is assumed that a guard time is typically in the range of 10 to 30 seconds.

When testing is done manually, the testing frequency is limited by the speed of manual operation, and adding a suitable guard time between transactions would be part of the instructions given to testers.

In fully automated testing, it would also be possible to use the high degree of repeatability of such control to determine the appropriate guard time by probing, i.e., by systematically varying the guard time and checking for respective effects.

There is a second category of effects that need to be considered, namely the possibility of a service-specific local memory (analogously to a browser's cache) that stores information related to previous transactions. The effect would be that in subsequent transactions, such information would be read from local memory instead of obtaining them by an over the air request to the service. This could then impact related measurement values or KPIs.

According to findings of the respective pre-tests, appropriate steps should be taken (such as clearing local memories). As long as effects are quantitative rather than qualitative, it may not be practicable, and it is not necessarily required, to exclude frequency-dependent effects entirely. However, the respective effects need to be recorded and documented carefully as part of the reporting in order to understand their impact on the testing conditions.

6.4 Re-initialization after unsuccessful transactions

If a transaction fails, in particular after a time-out condition has occurred, it shall be ensured that the service and the device or application are in the typical neutral starting state again, i.e., that no memory of previous error states remains in the system.

6.5 Disappeared money

It is possible that during a transaction, the amount of money deducted is not correct with respect to transferred amount and fees. This includes the case that the amount is correct but sent to a third party by an error in the system. From an end customer perspective, this is either a loss (if too much money is deducted), or an unjustified gain (if money is credited but not deducted on the other side of the transaction). For simplicity, the term "disappear" is used for both variants of this kind of effect.

NOTE 1 – In cases of disappeared money, insertion of fresh money will be necessary.

NOTE 2 – Retrieval of lost money should be treated as a second stream of activities

6.6 Automation of tests

The methodology in in this Recommendation describes testing in a generic way, i.e., service tests can be done manually as well as in an automated way. It is understood that automation of tests is desirable to achieve a greater degree of repeatability, and less variation in quantitative data values due to inaccuracy of e.g., manual time measurements. It is likewise understood that such automation requires a higher initial effort to ensure reliability of operation under unsupervised conditions or to cover a wider range of end-user devices.

7 Transaction model

7.1 Person to person (P2P) mobile money (MoMo) transfer

7.1.1 Transaction description

Abstract: Transfer of a known amount of M units of money from account A to account B.

Success definition: The **correct** amount plus applicable operator fees have been deducted from the A party account **and** the **correct** amount (net) has been credited to the B party account within the defined time window.

Examples for unsuccessful execution are cases:

- where the system sends – at any stage of the transfer – an explicit response indicating failure of the transfer;
- where the transfer has been done but the amount is wrong;
- a time-out occurs with a still pending TA.

NOTE 1 – The description does not explicitly refer to assignment of roles to devices or operators. For instance, if a particular device is assigned to represent a given account, the device may be operated as A Party or B Party. Related events occur, and related activities are performed, on the respective device.

NOTE 2 – Some service implementations may also offer a "tokenized" transfer which is in effect also a P2P transfer. In this case, the transfer done by the A party would create a token that can be transferred to a B party. This type of transfer is considered to be a special case and is not considered here.

7.1.2 Event and action flow

The core of a P2P MoMo transfer consists of instructing the DFS to transfer money from the A party's account to the B party's account.

To do so, the service requires information items such as the respective account IDs, information text for the transaction and the amount to be transferred. Also, the transfer will be authenticated by providing a respective token such as a PIN.

There are many conceivable ways the user interface may be designed. Most details are not relevant for modelling of a generic use case – such as the order in which required information items are gathered.

7.1.2.1 Involvement of the mobile network in the MoMo process

There is, however, an important exception which is highly relevant. This is the degree to which the mobile network is involved in the MoMo process. There are two general options:

All information is collected locally, and afterwards a single data block is sent to trigger the actual money transfer. This will be referred to as type A.

The information is collected item-wise, with exchange of data over the network after each step. This will be referred to as type B.

These options define the extremes of a *network involvement type* scale where an actual implementation is described by a value between those extremes (assigning them, eventually, type identifiers for easier reference). For instance, the local (A-party side) application may collect type and recipient of a payment, then validate the user exists; then it may request the amount to be transferred to check if it is within the limits of the A party's balance and contract, and finally request the remaining elements, including the A party's authorization, to validate the transfer.

NOTE – The differences belong, from a generic modelling perspective of a MoMo transaction, to the 'service set-up phase'. Collecting the information is prerequisite to conduct the transaction, but these steps do not provide any customer value by themselves. The customer value materializes in the actual performance of the money transfer which is the subsequent step.

Figures 1 and 2 illustrate the perspectives graphically.

Figure 1 shows a MoMo implementation where all information is collected locally in the A side DFS agent (e.g., an app, or a function implemented in the subscriber identification module (SIM) of the device) and is then transferred to the DFS. In this example, the DFS sends three data items in response:

The primary confirmation is sent to the A side's local agent.

A secondary confirmation may be sent also to the A party through another channel, such as SMS.

Also, a confirmation that money has been transferred is sent to the B side. As this is an unsolicited message (the B party is not actively participating in the transfer), an appropriate channel (such as short message service (SMS)) is used.

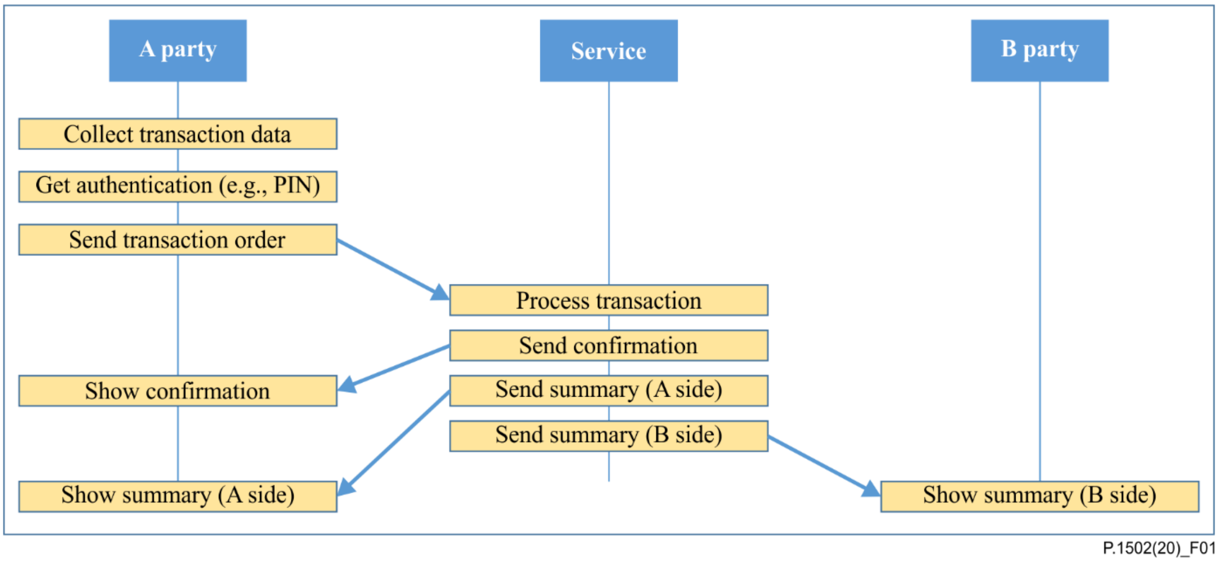


Figure 1 – Entities and event flow for a DFS implementation where required information is collected locally, and then transmitted to the service (Type A)

Figure 2 shows a MoMo implementation where the information required for a DFS transaction is collected successively by prompts from the server (intermediate variants are also possible, where some information is requested as a group).

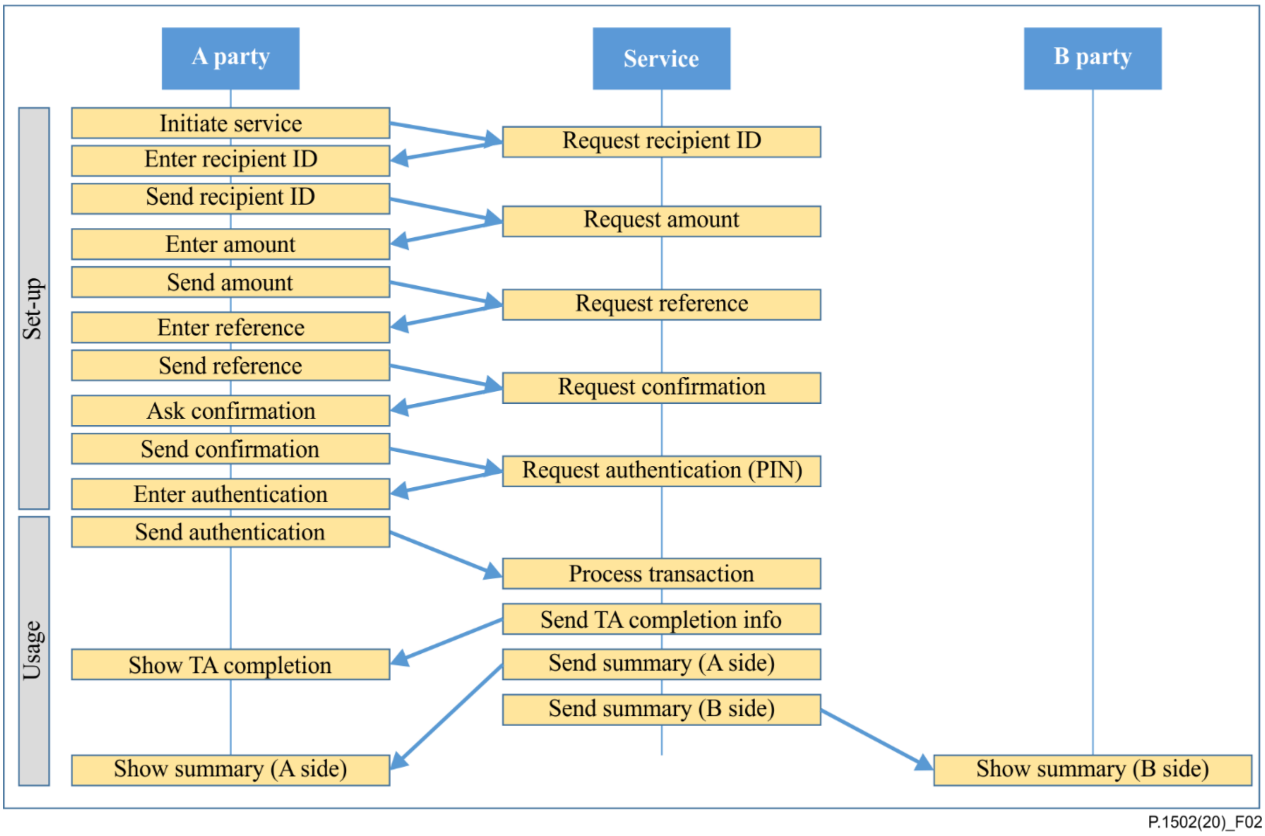


Figure 2 – Entities and event flow for a MoMo implementation where required information is collected element by element by the service (Type B)

Figures 1 and 2 also show a common element that is important for both modelling and methodology. There is an event "Show TA completion" on the A side. It represents a message from the service indicating that the transaction has been completed. It is therefore called the *primary completion* *indicator*. Completion is used here as the most general case for a distinctive message from the system which by itself only marks a defined end of the transaction, which can be a successful operation or an unsuccessful one. If the transaction has been performed successfully, this event is also called *primary success indicator*.

In real MoMo implementations there are additional messages generated by the MoMo service, e.g., a summary of the transaction (including, for the A side, information about fees charged). These messages are typically sent by a store and forward service such as SMS.

From a functional point of view, they can be considered as additional information which is, at least for the B side, important from the customer perspective but not critical or indicative for the DFS core transaction; debiting and crediting money has taken place already. Consequently, these events and information elements are considered to be secondary indicators; they are not crucial for the following considerations of type-variant dependent dynamics.

In the context of the current methodology, it is assumed that the SMSs containing summary information represent the final and correct information about the A and B side account balance. Technically, it is possible that these SMSs may contain erroneous content with respect to actual book-keeping. However, it is, for state-of-the-art systems, unlikely that such an essential element of a DFS implementation is faulty.

From a QoS perspective, and therefore also for network testing, the degree of network involvement is considered to be mission-critical.

First of all, the number of data exchanges through the network is much higher in type B than in type A. As the overall success of the MoMo transaction depends on the success of each of those steps, the MoMo success rate has a stronger dependency on network performance than in type A. Second, the collection of information items involves human interaction, i.e., typing. This extends considerably the time window in which the network needs to perform well, which, in particular, plays a crucial role in mobile scenarios.

On the other hand, Type B implementations enable collection of more information about the network performance as each step in the information-gathering phase provides an information source for the respective indicators. This topic will be discussed in detail in subsequent clauses. Briefly, the question is if it makes sense to define KPIs for every possible combination of events – which is technically possible but may obscure things rather than provide insights.

In this context, not only network quality should be considered but also terminal effects, like running out of battery power. Annex B provides an overview of elements for checking.

Of course, this discussion does not change the necessity of using the actual implementation of the service. From a QoE point of view, there is no choice – the whole transaction has to be taken into account if the test results are assumed to describe the customer perspective properly.

7.1.3 Phase definition

7.1.3.1 Top-level phases

Set-up: Preparations for the actual transfer:

- activation of service;
- input of required information, such as destination account, amount of money to be transferred, reference, credentials to enable the transfer (e.g., password or PIN).

Usage:

- performance of actual money transfer (including service-related transfer of information on A and B side).

NOTE – The set-up phase may or may not include access to functions within the service. Typically, the information required for a money transfer consists of several items of information. These items can be collected on the A party side and sent in one block of data, or can be sent one after another. From a diagnostic point of view, these variants will have different appearance and relation to properties of the transport network. However, from an end-to-end related functional view the actual mode is not relevant.

7.1.4 Failure information in top-level views

Depending on DFS implementation, collection of information needed to perform a DFS money transfer may involve data transfers through the network. In the hierarchical phase model, such steps are described by the corresponding sub-phases of the set-up phase.

While it is formally possible to define the respective KPI from these sub-phases, this may not be the best choice. It would increase considerably the number of KPIs. This may weaken the value of each KPI and obscure the function of a KPI as indicator of quality from the user's perspective. When benchmarking services, each contender can be the "test winner" in some category if there are enough KPIs in the portfolio. In the end, this decreases transparency instead of increasing it. Therefore, the set of KPIs should be as small as possible, with each KPI carrying a strong meaning with a clear relation to user perception.

Moreover, a KPI is essentially an isolated quantity. A phase consists of individual steps or sub-phases that occur in a given sequential order. With KPI for each sub-phase, information about this sequential order is not visible anymore. Therefore, a single KPI describing the overall success (or failure) rate of that phase, plus detail information about unsuccessful cases is more useful. Such detail information would then consist of information at which step of the sequence the failures have occurred. If required, statistics on such causes can be created or further processed to KPI-like indicators, i.e., this way is still open if required. The advantage as compared to the primary use of KPI to convey this information is that the information about failure causes is preserved on the transaction level and can be used to create additional diagnostic insight.

In the set of DFS KPI, the money transfer completion rate is a very good example for this approach. With the abstract model described in event and action flow (see clause 7.1.2), and the practical example shown in clause 7.2, this approach is demonstrated as follows.

The information required to perform a DFS transaction is prompted sequentially. After the user has entered a value, it is transmitted to the service, which in effect triggers the prompt for the next item of information. To make this happen, two data transfers are required. As seen from the A party's mobile device, these are:

- sending an item of information, via the transport network, to the service, and
- receiving the next item from the service.

As seen from the A party device, there are two ways this sequence can be interrupted:

a) sending an information item can fail, with a failure information; this can be a temporary failure when a retry takes place, or a permanent failure when e.g., the maximum number of retries or a time-out condition is reached;

b) the expected response may not occur. This essentially a matter of time-out condition. Without additional information, the A party cannot determine if the request – the data sent to the service – or the response of the service has been lost.

If there is, in a particular implementation of a test or the DF service, no sending failure information on the A side, case a) cannot be recognized technically and all interruptions appear to be of type b).

In any case, the A side has information of the last successful step, and the next one attempted. In case of failure, this information can be output together with the failure information and used in subsequent processing.

7.1.5 Time corrections for human interaction

If interactions require human input, time measurements will need adjustments. The top-level phase for set-up (see top-level phases in clause 7.1.3.1) consists, as shown in event and action flow (see clause 7.1.2), of a series of prompts for information items, and respective input by the user. Therefore, a time measurement for the whole set-up phase will contain elements that depend on the user's typing speed, which is clearly not useful for an objective measurement.

If time measurements are sufficiently fine-grained, it is possible to separate human interaction-related time spans from time spans caused by network or service response. For instance, if a prompt to enter data appears, the user needs some time to read the prompt, enter the requested information and send it to the service. The service then responds with the next prompt until all required steps are made.

When the DFS event flow is monitored and recorded manually, the granularity of time measurements, and their accuracy, is limited. Therefore, it may be difficult to separate service response times. Time measurements for larger groups of activity – such as the entire set-up phase as shown in Figure 2 – will inevitably contain human-interaction times. It can be expected that after some initial training, the time to enter data will be quite constant from transaction to transaction. However, time measurements should be expected to be of limited accuracy.

It is plausible to assume that service response times in the set-up phase are nevertheless of interest. A possible way to create respective data – at least on an averaged basis – is to record a number of interactions by e.g., video and determine a typical "typing time".

For a practical example, see the extended table in clause 7.2 and the definitions provided there.

7.2 Trigger point IDs

7.2.1 Trigger point ID basics

A trigger point ID is a short-form notation describing a specific action or event. The difference between action and event is somewhat arbitrary, and it also depends on the point of observation (POO). For a POO on the A party side of a use case implementation, *action* refers to an activity performed on the A side (by human action or some programmed activity) while *event* refers to something incoming (e.g., a message received via a mobile network).

NOTE – In older literature, the term PCO was used (Point of Control and Observation). The newer term POO reflects the fact that in most cases, respective data comes from sources which do not allow control anyway (e.g., IP layer traces); also in general it is better to not intermix control and data layers.

Trigger Point ID (TPID) = <Service and use case code> **_**<Type>**_**<Index> where

<Service and use case code>: in the present document, always DFSP2P

<Type> is either

a) AE event observable on the A side;

b) AA action to be performed by the user on the A side;

c) BE event observable on the B side;

c) BA (not used) Action to be performed on the B side.

<Index> is a continuous index, three digits, leading zeroes. Please note that numbering is not necessarily consecutive, i.e., choice of index does not carry meaning by itself.

For practical purposes in cases where the use case context is clearly defined, there is also a short-form TPID being used which omits the service and use case code and the related delimiter.

7.2.2 Trigger point IDs used

The following list of events has been derived from video analysis of an actual DFS P2P money transfer, for two variants:

- app based (this category also includes usage browser based web applications (typically such applications use https or other secure protocols);
- USSD based (typically used on feature phone based.

For further reference see also Event and action flow, clause 7.1.2.

Table 2 shows the trigger point ID for the MoMo P2P transaction model which has been derived from a practical implementation.

With respect to the considerations discussed in Time corrections for human interaction, and Special considerations for manual testing and time-taking, Table 2 also contains colour coding describing the nature of the phase between respective trigger points.

Table 2 – Trigger point IDs for the MoMo P2P model case

Triger point ID	Short TPID	Description (app)	Description (USSD)
DFS_P2P_AA_100	AA_100	Start DFS app	enter start USSD command
DFS_P2P_AE_104	AE_104	Prompt to select TA type	Prompt to select TA type
DFS_P2P_AA_108	AA_108	Select: Transfer	enter 1 to select "Transfer Money"
DFS_P2P_AE_112	AE_112	Prompt to select recipient type	Prompt to select recipient type
DFS_P2P_AA_116	AA_116	Select: To mobile user	enter 1 to select "to Mobile Money user"
DFS_P2P_AE_120	AE_120	n.a.	Prompt to select category of recipient
DFS_P2P_AA_124	AA_124	n.a.	enter 1 to select "to subscriber"
DFS_P2P_AE_128	AE_128	Prompt to select recipient ID	Prompt to select recipient ID
DFS_P2P_AA_132	AA_132	Enter B number and continue	Enter B number and continue
DFS_P2P_AE_136	AE_136	Prompt to select recipient ID again	Prompt to select recipient ID again
DFS_P2P_AA_140	AA_140	Enter B number again and continue	Enter B number again and continue
DFS_P2P_AE_144	AE_144	Prompt to enter amount	Prompt to enter amount
DFS_P2P_AA_148	AA_148	Enter amount and continue	Enter amount and continue
DFS_P2P_AE_152	AE_152	Prompt to enter reference	Prompt to enter reference
DFS_P2P_AA_156	AA_156	Enter reference and continue	Enter reference and continue
DFS_P2P_AE_160	AE_160	Request to confirm transaction appears	n.a.
DFS_P2P_AA_164	AA_164	Confirm	n.a.
DFS_P2P_AE_168	AE_168	Request for PIN appears	Request for PIN appears
DFS_P2P_AA_200	AA_200	Enter PIN and confirm	Enter PIN and confirm
DFS_P2P_AE_210	AE_210	Display TA in progress info	Display TA in progress info
DFS_P2P_AE_300	AE_300	Display payment confirmation	Display payment confirmation
DFS_P2P_AE_310	AE_310	Receive A side payment info	Receive A side payment info
DFS_P2P_BE_320	BE_320	Receive B side payment info	Receive B side payment info

The fields marked in blue identify parts of the event flow which relate to user activity. They are to be read in the following way: Beginning of the user activity is marked by the TPID preceding this element; the end of user activity is marked by the TPID assigned to the respective element.

Example – For the TPID AA_148 (Enter amount and continue), the user-activity starts with TPID AE-144 (Prompt to enter amount). At this point in time, the respective prompt appears on the user interface. The duration of this sub-phase is the time difference between these two trigger points, T (AA_144, AE_148); it includes the time the user needs to read and understand the prompt, to perform the action asked for (in this case, to type the amount, and to tap or press a button to confirm/send).

8 End-to-end DFS KPIs

8.1 KPI abbreviations and reference

Table 3 is a quick-reference index between KPI abbreviations, basic types, and the respective KPI definitions.

The abbreviation is given for easier reference; it also provides a way to add the actual test case type description in a similar way as in other KPI definitions. For ease of reading – because the present document only deals with the P2P MoMo case – the core abbreviation is used.

Full abbreviation: DFS-<Test case type>-<KPI abbreviation>

Table 3 – Example: DFS-P2P MoMo-MTCR

Abbreviation	Type	Reference
MTCR	Rate/Probability	Money Transfer completion rate
MTCT	Time	Money Transfer completion time
MTFPR	Rate/Probability	Money Transfer False Positive Rate
MTFNR	Rate/Probability	Money Transfer False Negative Rate
MTFTRR	Rate/Probability	Money Transfer Failed Transaction Resolution Rate
MTASSR	Rate/Probability	Money Transfer Account Stabilization Success Rate
MTAST	Time	Money Transfer Account Stabilization Time
MTLR	Rate/Probability	Money Transfer Loss Rate
MTDR	Rate/Probability	Money Transfer Duplication Rate

All definitions are using the event codes defined in clause 7.2.

8.2 Money Transfer completion rate, MTCR

8.2.1 Functional description

Probability that a money transfer can be completed successfully.

8.2.2 Formal definition

MTCR = *ratio between the number of successful instances of the use case, and all valid attempts to perform the use case.*

With AA_100 as indicator for a valid attempt (successful activation of the DFS function) and AE_300 as success indicator, the expression becomes

$$MTCR\ [\%] = 100 * \frac{Number\ of\ AE\_300\ events}{Number\ of\ AA\_100\ events}$$

8.2.3 Specific definition

Using the primary success definition, i.e., the summarizing SMS are not considered.

8.3 Money Transfer completion time, MTCT

8.3.1 Functional description

Time to complete a money transfer.

8.3.2 Formal definition

Using the primary success definition, i.e., the summarizing SMS are not considered.

This value is determined from the time between the activation of the used case until the completion of the transfer as indicated by the primary success indicator; it is therefore only valid for a successful transaction.

As the overall time contains human interaction, the technical definition excludes such times, but adds a typical time assumed to express the respective portion of the use case.

$$MTCT = T(AE\_104, AE\_300) - MTHI + TTHI$$

MTHI stands for the measured, and TTHI for the (assumed) typical time or all human interaction in this use case.

The meaning of this expression is "take the measured overall duration of the transaction, eliminate times caused by actual human interaction (which can vary from instance to instance) and replace them by a generalized (typical) value.

The special case TTHI=0 stands for the ideal (practically unreachable) case where data is entered so fast that the duration becomes negligible.

8.3.3 Specific definition

MHTI can be expressed in terms of trigger point timestamps as follows:

$$MHTI = T(AE_{t04}, AA_{108}) - T(AE_{112}, AE_{116}) - AE(120, AA_{124}) - T(AE_{128}, AA,_{132}) - T(AE\_136, AA\_140) - T(AE\_144, AA\_148) - T(AE\_152, AA\_156) - T(AE\_160, AA\_164)$$

By reference to Trigger Point IDs used, the terms of this equation are the sub-phases related to entering required information elements for the DFS transaction.

If a specific DFS implementation does not use and request a specific item, respective events and actions are not present, and associated T(x,y) are likewise not valid and are not used in the computation.

8.4 Money Transfer False Positive Rate, MTFPR

8.4.1 Functional description

Probability that a transaction is reported as successfully completed but has not actually been performed.

8.4.2 Formal definition

Using the event flow, receiving a primary or secondary success event without a corresponding attempt.

$$MTFPR\ [\%] = 100 * \frac{Number\ of\ success\ indicators\ received}{Number\ of\ all\ attempted\ transactions}$$

NOTE – Technically it is possible that this value is above 100% or even is undefined (denominator value zero). A service producing such results is however considered to be not suitable for field use – therefore, it is assumed that such cases are excluded.

8.4.3 Specific definition

For further study. In order to determine the actual account balance, either secondary information (e.g., A/B side summary information SMS), or an evaluation of an account record could be used.

8.5 Money Transfer False Negative Rate, MTFNR

8.5.1 Functional description

Probability that a money transfer is reported as unsuccessful but in fact has taken place (i.e., money has been transferred)

8.5.2 Formal definition

Computation of this KPI requires the existence of a corresponding information source. This can be a message (e.g., a secondary success criterion in the shape of a SMS, for A and B side, respectively) or a top-level check of account balances on A and B side by other means, e.g., transfer logs the service may provide on user request or on a regular basis. Data analysis will then use the reported account balances to determine the factual success of the transfer.

$$MTFNR\ [\%] = 100 * \frac{Number\ of\ transactions\ incorrectly\ reported\ as\ unsuccessful}{Number\ of\ all\ transactions}$$

8.5.3 Specific definition

For further study. In order to determine the actual account balance, either secondary information (e.g., A/B side summary information SMS), or an evaluation of an account record could be used.

8.6 Money Transfer Failed Transaction Resolution Rate, MTFTRR

8.6.1 Functional description

Probability that a failed transaction (by time-out through inaction or loss of network coverage) leads to a correct account balance

NOTE – This will be treated as out of context for the current project but should be subject of further study. Respective cases from the project can be used as input for failure assessment.

This is a secondary KPI which implies an error resolution process outside the scope of actual testing. It involves cases where initially money is lost (with respect to reported account balance), and where this lost money is retrieved though:

- an active process, e.g., by filing a claim to retrieve lost money, or
- some automated process in the realm of the DFS operator which restores lost money automatically.

8.6.2 Formal definition

Subject to further study.

8.6.3 Specific definition

Subject to further study.

8.7 Money Transfer Account Stabilization Success Rate, MTASSR

8.7.1 Functional description

Probability that a DFS transfer leads to a consistent account on both sides when all information is considered (i.e., primary status information on the A side, and summary information on A and B side.

For the current project it is assumed that the content of A and B side summary messages is correct. This KPI can then be computed as soon as both of these messages (e.g., SMS) have arrived.

8.7.2 Formal definition

Subject to further study. It needs to be defined how missing A or B side summary messages should be treated (e.g., ignoring them for KPI computation or not).

Furthermore, the computation for a consistently negative case needs to be defined (i.e., when a transaction fails, the expected result would be that the account balance is not changed). If this is not desired, respective definition of valid transactions is needed.

Preliminary definition:

$$MTASSR\ [\%] = 100 * \frac{\text{Number of transactions where information in summary messages is correct}}{\text{Total number of successful transactions (: AA\_200}\ \ valid, AE\_300\ valid)}$$

MTASSR = Ratio of transactions where the information is correct, to all valid and successful transactions (i.e., where AA_200 and AE_300 are valid).

8.7.3 Specific definition

Start/valid try when the MT is actually triggered, i.e., with last user confirmation. End after both the A and B side summary SMS (or equivalent data elements of a particular DFS implementation) have been received. Evaluation is made based on content of these elements.

See also the considerations in Event and action flow, clause 7.1.2.

If the actual DFS implementation does not provide respective information, this KPI cannot be computed.

8.8 Money Transfer Account Stabilization Time, MTAST

8.8.1 Functional description

Time (after the DFS money transfer has been triggered) until all status and account information is correct and consistent.

Start event: when the MT is actually triggered, i.e., with last user confirmation

With reference to Money Transfer Account Stabilization Success Rate MTASSR, the stop time is the time when the last of the A and B side summary messages e.g., by SMS have been received.

For the current project it is assumed that the content of these messages is correct.

NOTE – In order to validate the content of confirmation SMS against primary account reports may be a subject of further study.

8.8.2 Formal definition

$$MTAST\ =\ max(\ T(AA\_200, AE\_310), T(AA\_200, BE\_320)\ )$$

This definition takes into account that the A and B side confirmations (e.g., by SMS) do not necessarily have a fixed order.

8.8.3 Specific definition

Start time taken when the MT is actually triggered, i.e., with last user confirmation

8.9 Money Transfer Loss Rate, MTLR

8.9.1 Functional description

Probability that a money transfer ends in a loss, i.e., money is deducted on the A side but not credited on the B side.

For the current project it is assumed that the content of A and B side summary messages is correct. This KPI can then be computed as soon as both of these messages (e.g., SMS) have arrived.

8.9.2 Formal definition

Computation of this KPI needs further study to determine how unsuccessful transfers should be treated.

Preliminary definition:

$$MTLR\ [\%] = 100 * \frac{\text{Number of transactions where money is deducted on the A side but not credited on the B side}}{\text{Total number of successful transactions}}$$

8.9.3 Specific definition

This KPI requires a timeout which determines the time after it is assumed unlikely that the money sent by the A party will appear in the B party account. The timeout value should be determined based on the specific implementation of the service under test (see also Annex A for respective considerations).

8.10 Money Transfer Duplication Rate, MTDR

8.10.1 Functional description

Probability that a money transfer is credited to the B side but is not deducted from the A side account.

For the current project it is assumed that the content of A and B side summary messages is correct. This KPI can then be computed as soon as both of these messages (e.g., SMS) have arrived.

8.10.2 Formal definition

Computation of this KPI needs further study to determine how unsuccessful transfers should be treated.

Preliminary definition:

$$MTDR\ [\%] = 100 * \frac{\text{Number of transactions where money is credited on the B side but not deducted on the A side}}{\text{Total number of successful transactions}}$$

8.10.3 Specific definition

There are two possible cases to differentiate:

- TA is reported as unsuccessful, but money actually appears on B side (but is not debited to A side; the other case is treated in the MT false Negative Rate);
- TA is reported as successful, money is credited to B but not debited from A.

9 Acquisition of data on DFS transactions

9.1 Overview

To compute DFS KPI, the respective input data need to be collected.

The method used should be robust and provide a high level of data quality. Robustness means that the system should ensure security against loss of data. Data quality refers to aspects such as reproducibility and plausibility tests to detect wrong data.

Figure 3 is a graphical representation of measurement data flow and handling. Please note that this is a rather schematic and simplified view. Details given in the following sub clauses have precedence.

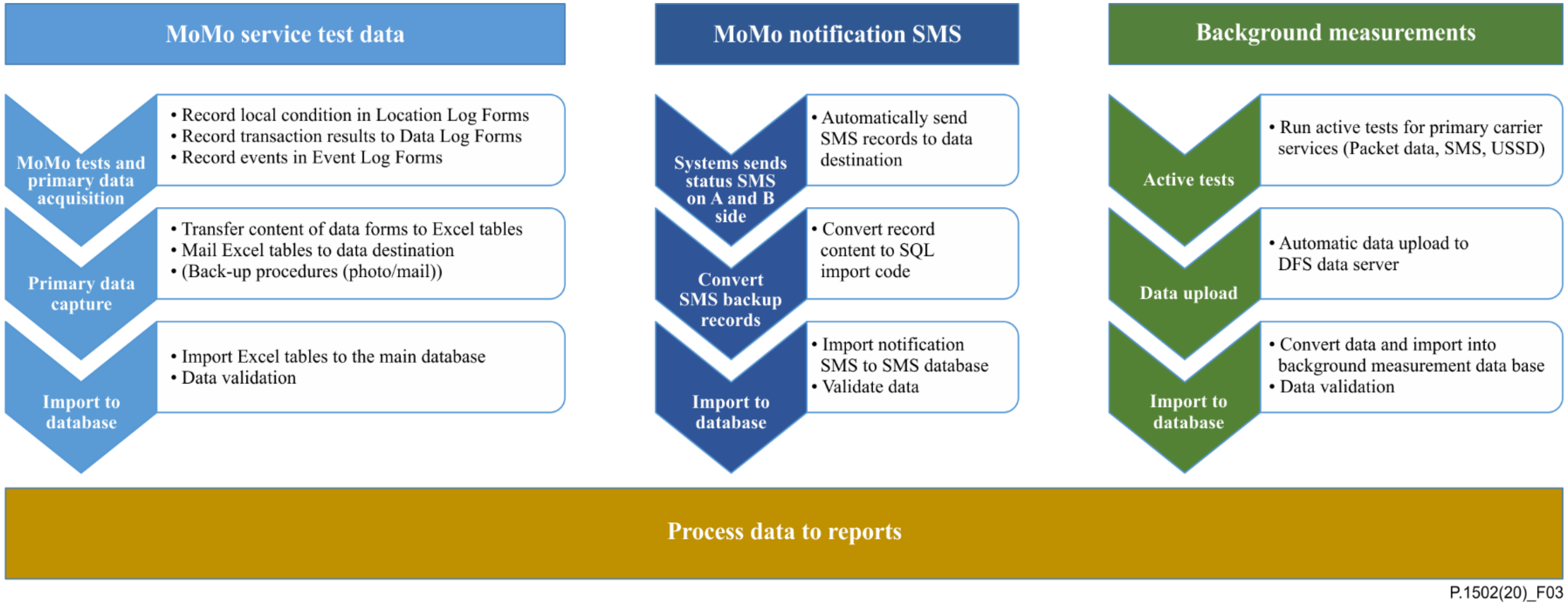


Figure 3 – Schematic overview of measurement data flow and handling

In a generic implementation of the methodology, a manual method is used to collect the primary information, i.e., timestamp data for events needed to compute KPI are noted manually by a member of the measurement team.

There is in addition, secondary information in the form of summary SMS sent by the system at the end of the transaction. These SMS can be read from the devices in a bulk fashion, and also transmitted to the data processing system.

For primary data collection on DFS transactions, there are basically two possible approaches:

- collection on paper and subsequent transfer into electronic forms (e.g., Excel®);
- direct entry to electronic forms (e.g., Excel® tables).

Both methods have their respective merits and will therefore be described subsequently.

Practical implementations of the methodology can use full or partial tool support, e.g., time-taking for events of a transaction by means of suitably designed apps which may also transmit collected data automatically to a server for post-processing.

9.2 Primary DFS data collection modes

9.2.1 General remarks

The procedures in the following are defined to provide operational robustness. They include steps which are intended to provide some redundancy and elements of data backup.

The term "uploading" is used in a functional way. Where smartphones are the platform (e.g., when taking a photo of a completed data log), it is assumed, unless otherwise mentioned, that this means sending respective data by e-mail.

As far as PCs are the platform, it is assumed that FTP or http upload will be used.

9.2.2 Collection on paper, deferred transfer

Paper printouts of respective tables are created. These printouts are called data capture sheets (DCS) from here on.

Each DCS shall carry some information to allow data consistency and completeness checking:

- identification of the team;
- date;
- location of test;
- running number of test in this specific location.

When a new location is used, a new DCS is used.

During testing, the team member enters data manually into the DCS.

The exact means of time-taking are not prescribed provided the required time resolution is given. However, the overall procedure must make sure that time and date settings are correct.

When a DCS is completed (all rows filled in), it is photographed and uploaded. Each such upload is logged in the general event log. Likewise, if the location of the test is changed, and at the end of a measurement day, the last DCS used is photographed and uploaded.

After the end of a measurement day, the data sheets of that day are entered into an electronic file (e.g., Excel spreadsheet) by a member of the team.

For the name of data files, see Data file naming, clause 9.3.

The data file is then uploaded. Also, a copy of the file is made to a suitable data medium (CD or USB memory stick, to be kept in a safe place). The file is also kept on the PC.

If an upload is not possible (if no connectivity for upload is available), attempts to upload the file shall be repeated in a reasonable time pattern, at latest at the following day.

All DCS originals are collected and kept in a safe place.

9.2.3 Direct entry into electronic form

During testing, the team member allocated for this task enters data directly into a data file. Respective procedures are the same as described in the previous clause.

Upload attempts for data files shall be made on the following occasions:

- the team changes the location;
- at the end of a measurement day;
- when a time of 4 hours after the last upload has elapsed.

9.3 Data file naming

9.3.1 General file naming

These generic file naming rules apply to files not specifically listed in clause 9.3.2.

Each electronic document (data table) is named in a consistent and unique way.

This information is also duplicated in the document itself. The information shall contain:

- a common text identifier (to be defined);
- identifier of the team;
- date and time of creation (time resolution: minutes, e.g., hh:mm).

Table 4 contains file/content types used, and their respective file naming rules.

9.3.2 Specific file names

Table 4 – File naming rules

File type	Naming definition
Scanned/photographed log files (per location)	TeamName_YYMMDD_LocationName.pdf Example: Team2_180618_Bubuashie.pdf YYMMDD should indicate the day to which the log file set refers (this implies that each file should only contain log files for one and the same day)
Electronic version of Data Log	DataLog_TeamName_YYMMDD_hhmm.xlsx YYMMDD should indicate the date of entries (implying that each log file should only contain data for one day). hhmm should indicate the earliest timestamp of content. With respect to the paper versions, this would be the "sheet started" time. If no paper version is used, the time should be the time of the first item of content.
Electronic version of Location Log	LocationLog_TeamName_YYMMDD_hhmm.xlsx For YYMMDD and hhmm, see above.
Electronic version of Event Log	EventLog_TeamName_YYMMDD_hhmm.xlsx For YYMMDD and hhmm, see above.

The naming of electronic log files is tentative and users of this specification are encouraged to reasonably adapt naming conventions to local circumstances.

NOTE – Data, location and event log files may contain information for different locations and therefore have no location name in the file name. Instead, they carry hhmm in case there are multiple files per day.

9.4 Campaign logs

Each team maintains a campaign log (paper or electronic form) where all relevant events are logged with date/time. Such events are:

- entering and leaving a given location;
- start, end and possible interrupts of background measurements;
- start and end of test activities;
- data logging and transfer related activities (depending on the mode selected);
- unusual events which occurred during measurement (e.g., power outages, planned or unplanned pauses).

The forms being used should at least include the following:

- location Log Sheet: Initial, intermediate and final checks on device set-up and status;
- Data Log Sheet (P2P Transfer): Acquisition of results for service tests;
- Event Log Sheet: capture of unusual conditions or events during tests.

An example of an actual campaign log used in the pilot campaign done in Ghana is shown in Appendix IV.

9.5 Handling of confirmation/information SMS (secondary information)

This data shall be retrieved from the device at least once per day, and transmitted/uploaded to a target destination (typically by email).

It is recommended to use an automated process to transfer SMS from the device to a storage location. For this purpose, there are several products available in the market. Which product is actually the best-suited for a particular testing campaign can be determined based on the actual requirements and process definitions of that campaign.

After the data has been successfully uploaded, it can be deleted on the device. The data file just uploaded can be moved to a backup storage location. Until then, the data shall be kept on the device as a back-up copy.

NOTE – If the devices are restricted in functionality (e.g., to act as "Feature phones", transfer via e-mail requires that these restrictions (e.g., "no mobile data") are removed for the transfer. It is important to re-establish the correct settings for DFS testing afterwards, or prior to a new set of tests.

10 Special considerations for manually operated testing and time-taking

The considerations described so far assume that time-taking provides a precision of time measurement which is sufficiently higher than typical times for respective phases of the event flow.

In case of fully automated data acquisition, typical time resolution is 1 ms while typical phase durations are at least a couple of 100 ms or longer.

The other extreme is entirely manual time-taking where time resolutions are much longer, typically 1 s or even more considering that times have to be read from a display which by itself may contain additional delay. Even in the case of semi-automatic data acquisition where some kind of stopwatch with high resolution is used, human reaction time and its jitter will result in an effective time resolution in the order of some 100 ms.

This means that a fine-grained time recording as indicated by Figure 2 will not be possible and use case modelling will have to be restricted to main phases. From a practical point of view, this will be the overall transaction time from invocation of the MoMo service to its completion (end-to-end duration), and the core transaction time, i.e., the time between triggering the transfer after all input information has been provided, and its completion.

Data acquisition may deliberately be done fully manual, or points of observation to obtain tripper point events may be limited. In such a situation, some of the generic KPI, as described in clause 8, are not applicable due to the reasons described. The following set of practical KPI can be used:

Table 5 – Simplified set of DFS KPI

Indicator	Abbreviation	Computation	Reference to formal KPI
Money Transfer Core Duration	MTCD	T3-T2	New KPI
Money Transfer Raw Completion Time	MTRCT	T3-T1	MTCT
Money Transfer completion rate	MTCR	T1 present, T3 present: success	MTCR
Money Transfer Full Completion Time	MTFCT	T7-T1	New KPI
Money Transfer A-side Completion Time	MTACT	T6-T1	New KPI

In all cases, a valid sample requires that all trigger points used in computation are valid, i.e., present. Indicators of type 'time' are therefore computed from transactions where respective phases have been completed successfully.

For the overall completion times, the E2E version using T1 was selected although it includes times for manual activity. Reasoning is as follows: A KPI, as an indicator expressing the end-user perspective, should provide a realistic estimate of a service's behaviour. Manual activity is an integral part of service usage and therefore it makes sense to include respective times into an indicator. Assuming that a testing team can be compared to an experienced user, times taken by such a team can be viewed as a valid estimation of manual components of service usage.

11 Measurements in the background

11.1 Overview and basic assumptions

The performance of Digital Financial Services over mobile networks is related to the properties of the network over which these services are provided.

It is important to keep in mind that the actual DFS is usually provided by some distinct ecosystem or functionality domain. A good mobile network alone does not guarantee a well-performing DFS as other components of such services also need to function well. A poorly performing mobile network can, however, degrade DFS performance massively.

Table 6 – Categorization of impact of mobile network and DFS infrastructure performance on end-to-end DFS QoE

	Well-performing DFS functionality	Poorly performing DFS functionality
Well-performing mobile network	High level of overall QoE, only vulnerable to local or temporal impairments of each component	Mobile network performance not relevant/not visible
Poorly performing mobile network	Overall DFS QoE strongly depends on mobile network performance	Low level of overall QoE, no clear dominance of each component

Table 6 shows the categorization of relative impacts of mobile network and DFS infrastructure performance, and conclusions with respect to field testing of DFS. With a poorly performing DFS functionality, effects of mobile networks are not or only weakly visible. In that case, field tests in different locations will most probably not be efficient, as the same results could be obtained by testing in fixed locations. If, on the other hand, if it is possible to ensure that mobile network performance is high, no field tests are required either. In the remaining cases, field tests will be needed to get a correct picture of overall DFS performance and QoE.

One of the goals of the methodology described in the present document is to provide guidance to regulators with respect to service performance levels of mobile networks in order to secure well-working digital financial services. While the present document describes KPI to express DFS QoE, it is desirable to provide insights about the connection between basic transport network QoS and their relation to DFS quality. Basic service KPI can then be used as proxies to create assessments on expected DFS quality. The methodology therefore also provides ways to link these KPI.

DFS can be implemented in various ways. Many implementations are based on the SIM Application Toolkit (STK) and access transport network services through functions provided by the STK.

With unmodified mobile devices it is not possible to access such services through STK, but this is considered to be not essential as these services can be accessed directly.

NOTE 1 – STK offers encryption of traffic which is not an intrinsic property of the generic services such as SMS or USSD. In the current context, this is considered to make no difference. Encryption may lead to additional delay and/or increased size of data content. It can however be assumed that this will not qualitatively affect the sensitivity to factors impairing service quality.

Using basic service as proxies to create assessments on expected DFS performance, and to provide guidance for e.g., regulators to set meaningful targets for network performance, has potential benefits; it is however also important to understand the limitations. A benefit is that the measurement of basic network services is technically easier than a full end-to-end measurement of DFS, not the least because the actual transfer of money is involved. It should be kept in mind, however, that the full DFS ecosphere also includes actors or parties beyond the mobile network infrastructure.

Figure 4 shows a generic model of the elements involved in the interaction between the A party (left side) and DFS system it uses.

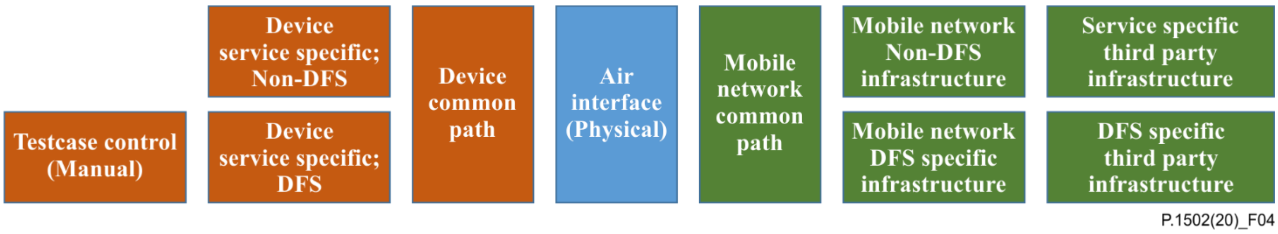


Figure 4 – Generic model of the elements involved in the interaction between the A party and the DFS system

Each component has a certain influence on the overall result, i.e., on the QoE of the DFS as perceived by the user of the service. If mobile network performance is the dominating element, there will be a distinctive correlation between the KPI of transport services used by the DFS implementation, and these service KPI can be seen as good proxies for actual DFS performance. If other elements dominate, e.g., the infrastructure which handles the money transfer, or elements between the mobile network and this infrastructure, respective correlation will be weak and transport service KPI will not be good proxies for DFS performance assessment or formulation of target value corridors.

If it is not clear which transport services are used in a particular case of testing DFS, the scenario should contain a wide spectrum of basic services tests. This allows to evaluate the correlation between

DFS and transport service KPI and therefore identify the most useful proxies for DFS quality assessment.

NOTE 2 – In general it is advisable to assume little or no knowledge of particular implementations. This may reduce measurement data yield with respect to test designs which exploit such knowledge, but it will also provide robustness against effects caused by changes in implementation which can lead to significant errors in the assessment of DFS performance if the testing process is over optimized in this respect.

11.2 Data acquired

During execution of the DFS use cases, the transport network is tested actively in parallel with a repeated sequence of test cases for different services. The purpose is to evaluate the general condition of the network. The intensity of these tests is however moderate in order to not stress the network too much.

Also, some basic network parameters as well as GPS information are taken continuously. However, the extent of these passive data is limited. On purpose, in this methodology only unmodified ("out of the box") mobile devices are used.

The following parameters are recorded:

- signal strength;
- type of network (Radio access technology (RAT));
- cell identity (as far as the device supports this);
- GPS position and speed.

If more information is desired, modifications to the phones are unavoidable. Such an extension of the methodology is for further study.

In the following clauses, considerations about the design of this sequence and the accompanying methodological considerations are described.

11.3 Test cases for transport network background testing

Scenarios for testing the transport network in the background have to be selected and defined on a country-by-country basis.

As an example, the following test cases can be used:

- SMS;
- USSD;
- web browsing (to a live and a reference page);
- http download and upload.

These test cases – with respective guard times and additional pauses to achieve the desired frequency of tests – are repeated cyclically.

Most of these use cases have parameters such as the amount of data transferred. Choice of parameters is made in a way to avoid overloading the transport network. This relates to pauses between test cases as well as use case specific parameters, e.g., data volume transferred in upload or download, and selection of the web sites used for testing.

11.4 Monitoring

Some baseline data should be collected for assessment of packet data performance. It is recommended to also run a monitoring device under good radio conditions (or via Wi-Fi connected to a fixed-line connection) which accesses the same server (for UL/DL) or web site respectively.

By analysing the performance, times where the server or web site itself is down (or its performance is degraded) can be easily identified.

12 Data validation and processing

12.1 Plausibility and validity checks

Tables 7, 8 and 9 in the following clauses are meant to be check list templates, e.g., validated items would receive respective check marks.

12.1.1 Tests on DFS data

See Table 7.

Table 7 – Tests on DFS data

☐	Are backup records (photos of filled-in sheets) complete?
☐	Check time spans for electronic data (Excel tables from primary data) vs. backup copies (range checks, i.e., first and last transaction on each data log sheet)
☐	Check timestamps of DFS data against respective location logs Does the timestamp range match the time window recorded for that location?
☐	Check timestamps of background measurement data against respective location logs Does the timestamp range match the time window recorded for that location?
☐	Decide on necessity to exclude time ranges Does the location log indicate special events and conditions, which set the need to exclude data from the set?
☐	Visualize timestamps of transactions: Are there any gaps or unusually dense transactions during a period of time? If yes, validate reasons
☐	*(further check items to be added)*

12.1.2 Tests on background test data

See Table 8.

Table 8 – Tests on background test data

☐	If GPS data are available, does the location indicated, and the GPS location match?
☐	Visualize timestamps of transactions: Are there any gaps or unusually dense transactions during a period of time? If yes, validate reasons
☐	*(further check items to be added)*

12.1.3 Cross tests between data (after import)

See Table 9.

Table 9 – Cross tests between data (after import)

☐	Validate time stamps of DFS and background data for consistency
☐	Validate consistency between network unavailability in DFS and background data. A possible consistency problem exists if background data indicate network unavailability but DFS transactions work during a given timespan. If such periods of time exist, mark them in the database and seek further clarification.
☐	*(further check items to be added)*

12.1.4 Additional processing

With respect to some KPI definitions, additional check procedures may be done.

Examples are:

- check consistency of accounts throughout a sequence of information SMS;
- check for "false negatives" (ref. Money Transfer False Negative Rate MTFNR, clause 8.5) by comparing account balance against transaction results.

Annex A

One-time tests

(This annex forms an integral part of this Recommendation.)

A.1 Introduction

This annex deals with tests that should be performed once per campaign to determine basic properties of the DF service under test.

A.1.1 Determine time-outs

Determine the time-outs for each step of a DFS use case (e.g., entering destination ID, amount, and reference). Make sure the time-outs do not cause failures with typical typing speed/time for entering values. Consider also typical reading times for information presented by the service, e.g., prompt texts.

Annex B

Check lists to be used in testing campaigns

(This annex forms an integral part of this Recommendation.)

B.1 Introduction

This annex contains elements of check lists for usage in measurement campaigns. The lists describe the points to be checked; the way to do so will have to be defined case by case.

Figure B.1 illustrates the use of the check list during a particular day of a test campaign.

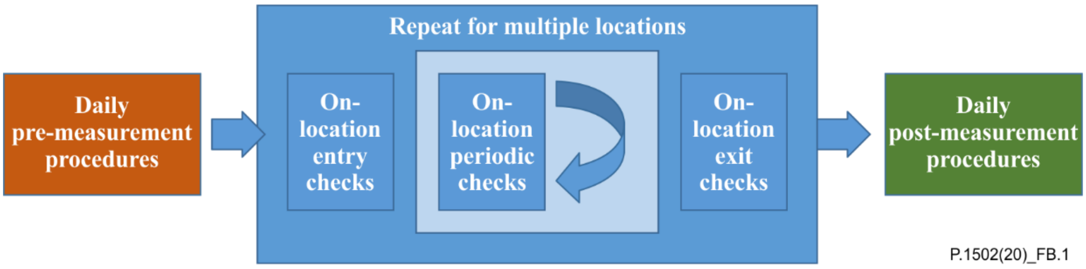


Figure B.1 – Measurement related checking procedures

B.1.1 Daily, prior to beginning of tests

- Make sure the time-taking device has correct time and date settings
- Make sure the device is set up to use network date/time (in case the network is providing this feature and information is assessed to be reliable)
- Make sure the devices have sufficient airtime/data volume credit to perform their respective actions (e.g., sufficient prepaid credit, or remaining data volume). Query and record respective information.

B.1.2 At each new testing location

Table B.1

Action	Frequency
Make sure the ObsTool UE is in the same cell as the DFS UE	Initially and periodically every ~ 2 hours
Make sure the UE used have sufficient battery charging level	Initially and periodically every ~ 2 hours
Make sure UE used for DFS testing do not run extensive background activities (e.g., download of new OS versions or apps requiring substantial system resources	Initially and periodically every ~2 hours

B.1.3 Daily after completion of tests

- Make sure the device is set up to use network date/time (in case the network is providing this feature and information is assessed to be reliable)
- Check that airtime/data volume credit is sufficient to perform their respective actions (e.g., sufficient prepaid credit, or remaining data volume). Query and record respective information. Re-charge if necessary.

NOTE – When respective action should be taken will depend on the actual testing situation (i.e., if it is better to do it in the evening for the following day, or in the morning of the next day). Choice should be made to give the best overall test team productivity under given circumstances.

Annex C

KPI/Trigger point lookup table

(This annex forms an integral part of this Recommendation.)

			MTCR	MTCT	MTFPR	MTFNR	MTFTRR	MTASSR	MTAST	MTLR	MTDR
			Rate/ Probability	Time	Rate/ Probability	Rate/ Probability	Rate/ Probability	Rate/ Probability	Time	Rate/ Probability	Rate/ Probability
TP ID	Type: Application	Basic (e.g., USSD)	Money Transfer completion rate	Money Transfer completion time	Money Transfer False Positive Rate	Money Transfer False Negative Rate	Money Transfer Failed Transaction Resolution Rate	Money Transfer Account Stabilization Success Rate	Money Transfer Account Stabilization Time	Money Transfer Loss Rate	Money Transfer Duplication Rate
DFS_P2P_AA_100	Start DFS app	enter start USSD command									
DFS_P2P_AE_104	Prompt to select TA type	Prompt to select TA type	Start	Start	Start		Start				
DFS_P2P_AA_108	Select: Transfer	enter 1 to select "Transfer Money"	X (2)	X (3)							
DFS_P2P_AE_112	Prompt to select recipient type	Prompt to select recipient type	X (2)	X (3)							
DFS_P2P_AA_116	Select: To mobile user	enter 1 to select "to Mobile Money user"	X (2)	X (3)							
DFS_P2P_AE_120		Prompt to select category of recipient	X (2)	X (3)							
DFS_P2P_AA_124		enter 1 to select "to subscriber"	X (2)	X (3)							
DFS_P2P_AE_128	Prompt to select recipient ID	Prompt to select recipient ID	X (2)	X (3)							
DFS_P2P_AA_132	Enter B number and continue	Enter B number and continue	X (2)	X (3)							
DFS_P2P_AE_136	Prompt to select recipient ID again	Prompt to select recipient ID again	X (2)	X (3)							

			MTCR	MTCT	MTFPR	MTFNR	MTFTRR	MTASSR	MTAST	MTLR	MTDR
DFS_P2P_AA_140	Enter B number again and continue	Enter B number again and continue	X (2)	X (3)							
DFS_P2P_AE_144	Prompt to enter amount	Prompt to enter amount	X (2)	X (3)							
DFS_P2P_AA_148	Enter amount and continue	Enter amount and continue	X (2)	X (3)							
DFS_P2P_AE_152	Prompt to enter reference	Prompt to enter reference	X (2)	X (3)							
DFS_P2P_AA_156	Enter reference and continue	Enter reference and continue	X (2)	X (3)							
DFS_P2P_AE_160	Request to confirm transaction appears		X (2)	X (3)							
DFS_P2P_AA_164	Confirm		X (2)	X (3)							
DFS_P2P_AE_168	Request for PIN appears	Request for PIN appears	X (2)	X (3)							
DFS_P2P_AA_200	Enter PIN and confirm	Enter PIN and confirm	X (2)	X (3)		Start		Start	Start	Start	Sta rt
DFS_P2P_AE_210	Display TA in progress info	Display TA in progress info	X (2)	X (3)							
DFS_P2P_AE_300	Display payment confirmatio n	Display payment confirmatio n	Success	End (1)	Success (use for validity check)						
DFS_P2P_AE_310	Receive A side payment info	Receive A side payment info			use content for validation						
DFS_P2P_BE_320	Receive B side payment info	Receive B side payment info			use content for validation						

NOTE 1 – For a time value, all sub-phases where human interaction is involved need to be eliminated, and, eventually, a normalized/typical time value has to be used instead

NOTE 2 – Used to create detail information in case of failure (identify sub-phase where failure occurred)

NOTE 3 – Use all available elements to calculate eligible time intervals (only use the times which do not contain human action, e.g., time from confirmation of an info item to appearance of the next prompt)

Appendix I

Device set-up for the Ghana pilot

(This appendix does not form an integral part of this Recommendation.)

I.1 General

Figure I.1 shows the device set-up schematically. Please note that this diagram is shown for convenience and overview. Explicit textual descriptions have precedence.

The software installed on the Observer Phone, labelled "dfs observer app", is a concrete example for an application doing QoS tests of transport network services. Basically, every suitable product available in the market can be used according to the guidelines described in the main part of this Recommendation.

For the task of transferring received confirmation SMS for further processing, the software selected for this pilot was "SMS Backup & Restore"; basically any product providing the necessary functionality as defined in the main part of this Recommendation can be used.

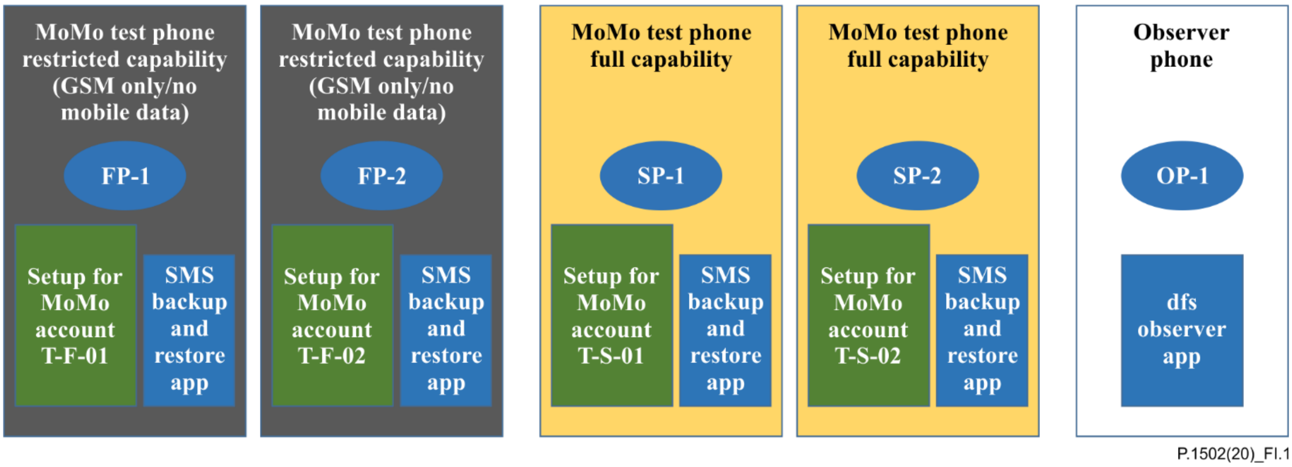


Figure I.1 – Device set-up for the Ghana pilot (per team)

All settings and selections made during the set-up process shall be recorded and stored electronically (e.g., in an Excel table file) to facilitate overview and reproduction in case of need.

I.2 Basic device set-up

All devices are set-up following the usual procedure for Android.

In particular, the Google user account and associated mail address shall be recorded to be able to identify mails sent from this device, and facilitate emergency remote access to this device over respective Google services.

Set-up of optional services and features for the MoMo test phones shall be made in a way assuming a typical user (i.e., accepting default settings suggested by the set-up process).

In case of the observer phone, set-up shall be made in a way which results in minimally possible background data traffic.

All devices should be set up to use network date/time to ensure time stamp consistency. This set-up should also be verified periodically, at least once per day at the beginning of measurements.

I.3 Setup for MoMo account

The accounts on each MoMo test phones should be set up in the way deemed typical for a subscriber of the respective service.

I.4 SMS Backup & restore app

The app was installed using the standard Android app installation process and parameterized using the product's guided set-up process. The app was set to transfer copies of the SMS on the device every 24 hours. In addition, a transfer was triggered manually after every measurement session.

I.5 Application for active network testing

I.5.1 General

In this particular case, a product called DFS Observer, a configurable QoS test suite for mobile networks manufactured by the German specialist company Focus Infocom GmbH has been used. This product comes as an Android app which is installed using the standard procedure for such apps.

Please note that the SMS test case needs customization of the scenario for each individual device to use the correct destination phone number.

I.5.2 Scenario used for the pilot

The scenario used combines various data tests, an SMS test and two different USSD tests (order of testing may differ)

- Google start page
- ETSI [b-ETSI TR 102 505] SP reference page on two different servers (fixed-time mode)
- ETSI [b-ETSI TR 102 505] Full reference page in fixed-time mode, on two different servers
- Download 100 KiB, fixed-time mode, on two different servers
- Upload 100 KiB, fixed-time mode
- SMS to self
- USSD: *156# (show own number)
- USSD: *151# (unknown code, see remark below)

NOTE – Deliberately using an invalid USSD code is a means to get a kind of "ping" to the USSD subsystem. There is, however, the risk that the network negatively reacts to repeated sending of invalid codes after some time. The data shall be monitored in order to detect indications of such reactions and the scenario may be changed respectively.

I.6 Additional software

To make remote support easier, it is recommended to install an application for remote support on each device. Examples for such products (list is not comprehensive and order does not indicate preferences) are TeamViewer, VNC Connect, UltraVNC, Chrome Remote Desktop or WebEx Meetings.

NOTE – When selecting an app, it is necessary to make sure that the terms of use for the chosen app allow the intended usage. Respective terms need to be monitored and checked against the mode of usage. In case of conflicts, a resolution by e.g., purchase of required license or selection of another app needs to be considered.

Appendix II

Naming rules, data structures and related processes used in the pilot project

(This appendix does not form an integral part of this Recommendation.)

II.1 Naming

II.1.1 General

Element names shown in bold face are functional names which shall be used consistently throughout all relevant documents. They may also have abbreviations used for brevity but only in the current clause of this document.

II.1.2 Teams

Each team shall be given a unique **Team ID** (TID), made of alphanumeric characters. The TN can be freely chosen but it shall not be changed over time.

II.1.3 Devices

The ***Device ID*** (DID) is composed of the device's role and index (e.g., SP1, FP2, and OP), underscore ('_') and the last 6 digits of the device's IMEI.

On log sheets, an abbreviated name using only the device's role is used. The full DID can be looked up by the respective entry in the device/team assignment data (see below).

The IMEI is the identifier displayed if the code *#06# is entered in the Phone Dial window.

In case of dual-SIM devices, they may have 2 IMEI. In that case, the IMEI for the first SIM position is used for the DID. Usually this is the first IMEI displayed for *#06# (to be verified).

Example for a full DID: SP1_123456

On log sheets, Device Role Aliases can be used instead of the short role names. The following aliases are defined:

SP	Full Capability
FP	Low Capability

II.2 Team and device assignment list

A list is kept which records the assignment of devices to teams. As this assignment may change over time, the respective time window is also recorded.

The list has the following elements:

Element	Type
Team ID	Varchar(128)
Device ID	Varchar(64)
Start time and date of assignment	datetime
End time and date of assignment	datetime

The end time can be NULL to indicate that the last assignment is still valid.

II.3 Notification SMS

II.3.1 Transfer and data handling process

The ***Notification SMS*** (NSMS) (sent to the A and B party) contain information about the DFS transaction. This information is used to complement the overall information.

The steps of this process are:

- NSMS arrive at respective devices;
- the SMS backup process (see SMS Backup & restore app, clause I.4) sends, when invoked, an e-mail with an XML file attachment to a specific location. This XML file contains a copy of all SMS which were stored on the device at the time of invocation;
- the attachment is processed by importing it into the project data base.

The NSMS do not contain information about the devices involved. This information must therefore be added during the overall process of NSMS collection.

This is done using the following definition and process:

- the set-up of SMS backup allows to configure the Subject. This Subject shall contain the DID of the respective device;
- for import, the DID shall be added to the respective data items;
- as each backup file is a snapshot of all SMS on the device, subsequent executions will produce duplicates of NSMS. The data structure/import process must have provisions to handle these duplicates.

II.3.2 Notification SMS Data table structure

Element	Type
Device ID	Varchar(64)
Import date and time	Datetime
SMS content	Mirroring of XML structure

II.3.3 Assignment of primary test data and SMS

Each successful DFS transaction is assumed to produce a set of primary data (timestamp information according to the definitions elsewhere in the present document) and two confirmation SMS on the A and B device, respectively.

By processing SMS back-up copies uploaded to the data base, these SMS are assigned. There are two basic types (A side and B side SMS). There can be other SMS on the device. Therefore, the classification and assignment process has the following stages:

1) Identify if a SMS is of type A-side, B-side or other
2) If A-side, attempt to find the matching B side SMS from another device
3) If B-side, attempt to find the matching A-side SMS (actually steps 2 and 3 are symmetrical)
4) Attempt to find the matching primary transaction for the A-side and B-side SMS, respectively, using device/team allocation and timestamp

Ideally, the process assigns all A-side and B-side SMS. It is expected that "orphans" exist which do not have a counterpart. For such orphans, the first step is to check if SMS exist on devices which have not been covered by the backup process. If this check finds previously missing SMS, they shall be processed.

The remaining orphans are again sorted into categories:

- A or B side SMS which have matching DFS transactions. This indicates transactions where such SMS are missing and shall be notified along accordingly.
- A or B side SMS which have no matching DFS transaction. An investigation shall be conducted to clarify the circumstances.

II.3.4 Storage and deletion aspects of SMS on devices

The process of SMS back-up is based on periodic copies of all SMS on a particular device.

In the course of the test campaign, locally stored SMSD will accumulate unless they are deleted. Deletion procedures carry the risk of unwanted deletion of meaningful data. A hard cause to delete SMS would be capacity issue. Unless this is given, it is assumed to be better to handle SMS duplicates – which is technically quite simple in data processing than to run a deletion process.

In case a deletion process is required after all, it is performed along the following process:

1) There are regular device maintenance cycles (e.g., once per week) where all devices used in the test campaign are participating.
2) From processing of previously uploaded data, a reference point in time for DFS confirmation SMS is calculated (SMS-RP, type time/date). It is assumed that up to this RT, all uploaded SMS are checked and assigned (see Assignment of primary test data and SMS, clause II.3.3) and that any hints on missing SMS (detected as missing in uploaded data, to be checked for on devices) are clarified.
3) In the maintenance process, all locally stored SMS older than the SMS-RP are deleted.

Appendix III

Description of the Ghana pilot campaign

(This appendix does not form an integral part of this Recommendation.)

III.1 Data collection method

For the Ghana pilot project, full manual acquisition of data, i.e., method a) as defined in clause 6.2, has been selected as it is the most generic one.

III.2 Event definition

Events have to be recorded with their respective timestamps. Manual recording of those events requires a certain amount of time. This should not delay the DFS process under test. This sets practical limits to the granularity or number of events per DFS use case. Therefore, the extent of data will be limited to the following set. See also clause 7 for related practical KPI.

Table III.1 – Timestamps used in the Ghana pilot project

Symbol		Description
T1		Start of transaction (activation of the DFS function/application on the device)
T2		All necessary input data has been entered and the actual money transfer is triggered.
One of	T3	Reception of the primary success criterion (information about the successful completion of the transaction), **or**
	T4	Reception of an information stating that the transaction has failed
	T5	Time-out limit reached without a positive or negative reaction from the service
T6		Reception of the summary SMS in the A-side mobile device
T7		Reception of the summary SMS in the B-side mobile device

The decision about the time-out condition needs actually to be made by a member of the observer team. This requires special element in the toolset used, e.g., an alarm timer started with T1.

NOTE – It is assumed that T6 and T7 can also be derived from captured SMS on respective phones later. It is however desirable to record these events in the data logs, too.

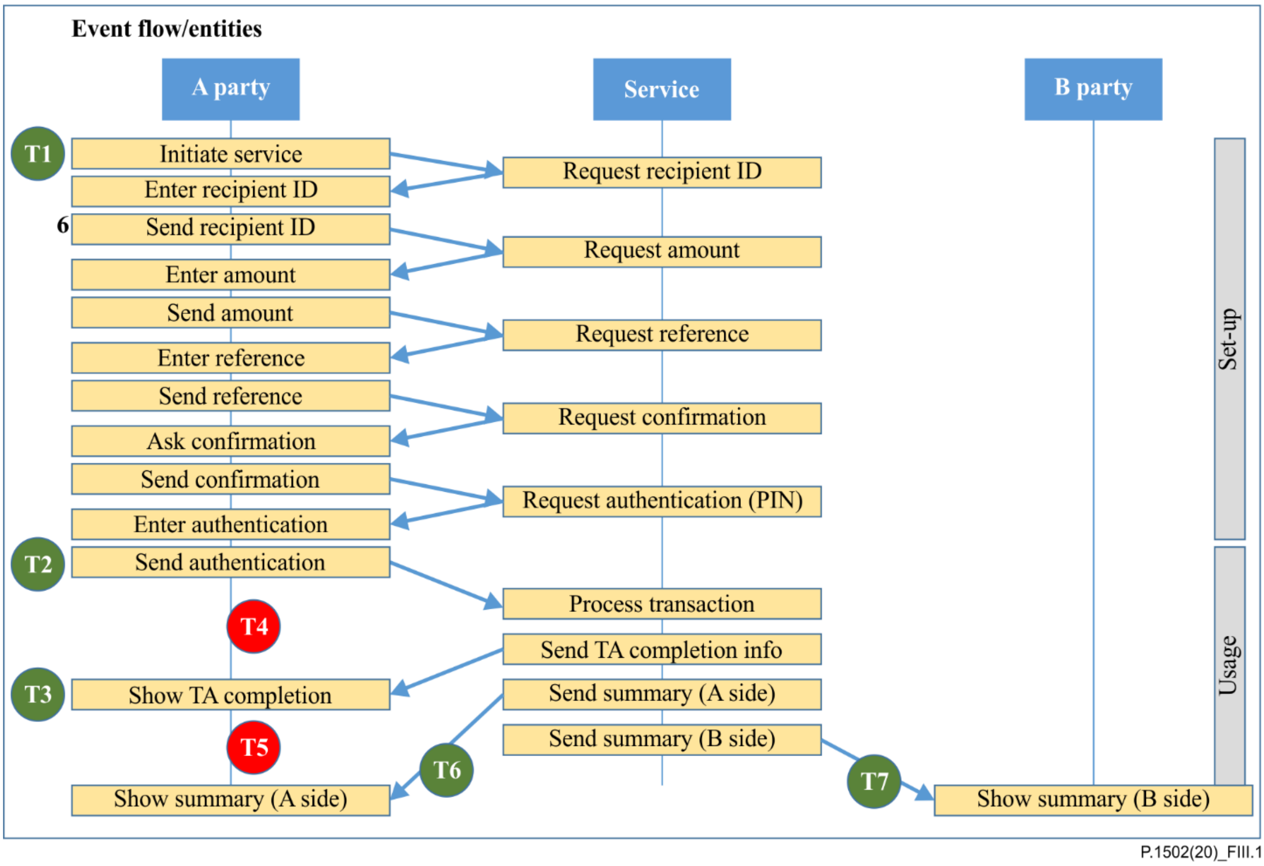


Figure III.1 – DFS event flow with recording points for manual time measurement

Figure III.1 (based on Figure 2) shows the event flow with the recording points T1 to T7 for manual time measurement. Events which belong to the positive result case are shown with green background colour; negative events (indicating failure or time-out) have red background colour.

III.3 Mapping of acquired data to formal trigger points

By comparison to the full trigger point list shown in Table 2, the timestamps used in the Ghana pilot campaign, as shown in Table III.1, are a subset (see the full discussion of consequences of manual execution of tests in clause 7). Consequently, a mapping of timer flags to formal trigger points needs to be done and is shown in Table III.2.

Table III.2 – Reference table: Ghana campaign timestamps to formal trigger points

Timestamp	Formal trigger point	Remarks
T1	AA_100	Start of test case execution
T2	AA_200	Start of core transaction
T3	AE_300	Successful completion of transaction
T4		Used as failure indicator
T5		Used as timeout indicator
T6	AE_310	Reception of information SMS on A side
T7	BE_320	Reception of information SMS on B side

Please note that there are no format trigger points for T4 and T5 as they are not linked to events from the activity flow in a DFS implementation. In case of T4, it will be set from a failure indication given by the DFS implementation which cannot be provoked directly from A or B side, but needs to be interpreted as part of human or automated monitoring of the test. In case of T5, it is set by a time-out condition determined by some external time-keeping process.

III.4 Background testing of the transport network

For SMS testing, sending SMS to the same device is used to simplify data capture.

For USSD testing, a code (or multiple codes) should not make permanent changes to the state of the subscription, or to the mobile device. For the tests, the USSD code *135# has been chosen which queries the own telephone number. Also, using a code which relates directly to DFS should not be used, as this may bring the DFS system into undesired states. Suitable USSD codes would serve as suitable proxies for the functioning of the USSD subsystem in the network under test, without having undesired side effects.

For the choice of web sites, small sites were selected, i.e., the Google search engine start page, and the ETSI Kepler for Smartphones page[1] hosted on a reference server.

Even though the DFS implementation in Ghana uses USSD and SMS as its principal carrier services, packet data related test cases have been added to collect some potentially useful additional information.

After some validation tests, it has been determined that using a data server hosted by the testing app's manufacturer in Germany provides the best operational value also with respect to maintenance. During the pre-pilot phase, a second server (at Strato, a large German web hosting system) has been tested and verified to work. This was done to make sure a fallback solution is available in case of server problems during the campaign.

1 http://docbox.etsi.org/STQ/Open/Kepler/Kepler_for_Smartphones.zip

Appendix IV

Campaign log examples

(This appendix does not form an integral part of this Recommendation.)

Data Log Sheet P2P transfer

Team ID	
Team Leader	
Location name	
Date	

	(Date/Time)
Sheet started	*Point in time when the sheet is started to be used*
Sheet completed	*Point in time when the sheet is full/completed*
Sheet photographed	*After completion, the sheet shall be photographed and the photo uploaded (e-mailed) to a given location*
Sheet Photo uploaded	*Checked after the sheet has been successfully e-mailed*

AMOUNT OF MONEY ON ACCOUNTS, BY TEST DEVICE

Device ID	at sheet start	at sheet end

Field description

Device ID	Unique ID of the device
Sender ID	Device ID of the device used to send money (A party)
Receiver ID	Device ID of the device used to receive money (B party)

TEST DATA LOG

Amount	Sender ID	Receiver ID	T1	T2	T3	T4	T5	T6	T7
			Start of TA	Trigger transfer	Success	Failure	Time-out	A side SMS	B side SMS

Event Log Sheet

Team ID	
Team Leader	
Location name	
Date	

	(Date/Time)
Sheet started	*Point in time when the sheet is started to be used*
Sheet completed	*Point in time when the sheet is full/completed*
Sheet photographed	*After completion, the sheet shall be photographed and the photo uploaded (e-mailed) to a given location*
Sheet Photo uploaded	*Checked after the sheet has been successfully e-mailed*

Time	Description of event

Examples of events to be logged:

- Changes of power supply (battery/charger operation, power outage,...)
- Changes of network coverage (loss of coverage/return of coverage)
- Stopping or resuming the test measurement (pause/end of pause, external events,...)
- Any unusual events which occured during the test

Bibliography

[b-ETSI TR 102 505] ETSI TR 102 505 V1.3.1 (2012), *Speech and multimedia Transmission Quality (STQ); Development of a Reference Web page*.

[b-DFS TR] ITU-T Focus Group Digital Financial Services: Technical Report "QoS and QoE Aspects of Digital Financial Services" (05/2016)
FG DFS QoS Report

[b-FIGI-1] Financial Inclusion Global Initiative (FIGI), *Security, Infrastructure and Trust Working Group (SIT WG) (03/2019), Methodology for measurement of QoS KPIs for DFS*
Methodology for measurement of QoS KPIs for DFS

[b-FIGI-2] Financial Inclusion Global Initiative (FIGI), *Security, Infrastructure and Trust Working Group (SIT WG) (03/2019), Report on the DFS pilot measurement campaign conducted in Ghana*
Pilot measurement of QoS KPIs for DFS in Ghana

[b-FIGI-3] Financial Inclusion Global Initiative (FIGI), *Security, Infrastructure and Trust Working Group (SIT WG) (2019), DFS Consumer Competency Framework.*

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	Tariff and accounting principles and international telecommunication/ICT economic and policy issues
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Environment and ICTs, climate change, e-waste, energy efficiency; construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	**Telephone transmission quality, telephone installations, local line networks**
Series Q	Switching and signalling, and associated measurements and tests
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks, open system communications and security
Series Y	Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2020