INTERNATIONAL STANDARD

ISO 20415

First edition
2019-10

Trusted mobile e-document framework — Requirements, functionality and criteria for ensuring reliable and safe mobile e-business

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO 20415:2019
https://standards.iteh.ai/catalog/standards/sist/46fafecf-cfa0-4114-a7ed-22525bee6aa3/iso-20415-2019

Reference number
ISO 20415:2019(E)

© ISO 2019

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO 20415:2019
https://standards.iteh.ai/catalog/standards/sist/46fafecf-cfa0-4114-a7ed-22525bee6aa3/iso-20415-2019

COPYRIGHT PROTECTED DOCUMENT

© ISO 2019

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Fax: +41 22 749 09 47
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

© ISO 2019 – All rights reserved

Contents

Page

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO 20415:2019
https://standards.iteh.ai/catalog/standards/sist/46fafecf-cfa0-4114-a7ed-225f35bee0aa5/iso-20415-2019

© ISO 2019 – All rights reserved

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

This document was prepared by Technical Committee ISO/TC 154, *Processes, data elements and documents in commerce, industry and administration*.

ISO 20415:2019
https://standards.iteh.ai/catalog/standards/sist/46fafecf-cfa0-4114-a7ed-2353fb4d0e3d/iso-20415-2019

Any feedback or questions on this document shall be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

© ISO 2019 – All rights reserved

Introduction

Communication via mobile devices is essential in the modern world, so that most mobile devices are ever used as a passage for the connection of people, business and network. Electronic transactions, information processing and data transmission via the mobile device are common in business area. In addition, electronic documents utilized by mobile devices in the business world are rapidly increasing and its application area is growing also. Mobile electronic document exchange will be used in overall industrial areas including B2C and B2B; the effect will be enormous considering the characteristic of the mobile device.

However, communication using the mobile device always also involves a number of problems. First, the wireless channel could be disconnected unexpectedly even while transmitting data; in that case the data could be lost. This could be a fatal flaw in the transmission and reception of sensitive corporate data. Second, it is possible for anyone to steal easily the mobile device, causing data transmission by a fake user. Third, the mobile communication is relatively vulnerable compared with online communication in the respect of security and reliability. These problems have been an obstacle to the flow of electronic documents and electronic transactions diffusion through the mobile communication. Companies or individuals have increasing demand for data transmission to continue to be safe and reliable enough from the mobile communication. Thus, it is necessary to have a standard way to exchange data with the electronic document in a manner that is safe and reliable over a mobile device.

In the process to distribute electronic documents for electronic transactions using mobile networks, principles and standards different from those in the wired situation need to be suggested in order to maintain the reliability of distribution of electronic documents due to the negative characteristics of mobile network. As mobile networks give lower reliability generally and limit available computing resources, users of mobile electronic documents need to have wide range of options for ensuring the reliability in the distribution of mobile electronic documents. That is, a guide needs to be suggested to find out an appropriate way for distributing mobile electronic documents according to costs or the network environment.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO 20415:2019
https://standards.iteh.ai/catalog/standards/sist/46fafecf-cfa0-4114-a7ed-22525bee6aa3/iso-20415-2019

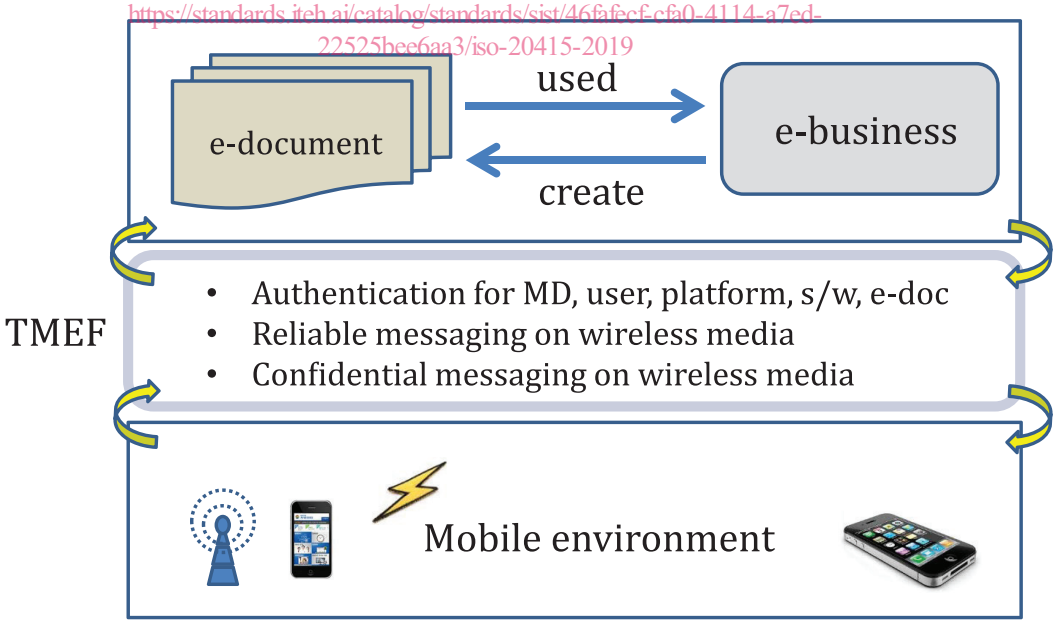


Figure 1 — Concept of a trusted mobile e-document framework (TMEF)

This document is intended to provide a framework standard for creating and transmitting electronic documents for B2B/B2C via a mobile device using a secure and trusted method in an unstable and unreliable mobile environment. The concept of TMEF is illustrated in Figure 1. Businesses or individuals are getting more dependent on mobile devices in terms of handling business as time passes by. Also, the situation is that the demand to handle important duties of businesses is increasing. Therefore, the

© ISO 2019 – All rights reserved

demand for safe and reliable processing of electronic documents under mobile environment is also rapidly increasing.

However, a mobile environment is unable to apply all methods for maintaining highest security and reliability due to the limitations of computing resources and the limitations of wireless network. Therefore, trusted factors necessary for performing safe electronic transactions under the mobile environment need to be derived to apply them in reality.

Wireless network and the mobile device (MD) are exposed to risks and easiest to get attacked under the mobile environment. It is very difficult to identify strictly the MD and the user who owns the MD due to its portable nature. Also, the wireless network causes many problems with reliability and safety while performing electronic transactions since it can often be cut off suddenly and also can be tapped by a random user very easily.

Accordingly, in order to process electronic documents in a safe and reliable way under a mobile environment, authentication on the MD in use, platforms on the MD, and the users who use the software and MD need to precede. Also, detection on the disconnection of wireless network and fast recovering the network are necessary. In addition, maintaining confidentiality is also absolutely required to be ready for tapping. In some cases, verification of integrity or confirmation of authenticity on a document prepared in an MD can be required. If a mobile device is assumed to provide partly some of these functions, it cannot be considered safe or reliable. So, it is necessary to establish an overall mobile framework which can cover completely the vulnerability of the mobile environment: safety and reliability.

This document presents a framework standard, called TMEF, necessary for using and transmitting electronic documents in a safe and reliable way under a mobile electronic transaction environment. TMEF presents functional requirements and criteria for practical use and management factors necessary for performing mobile transactions.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO 20415:2019
https://standards.iteh.ai/catalog/standards/sist/46fafecf-cfa0-4114-a7ed-22525bee6aa3/iso-20415-2019

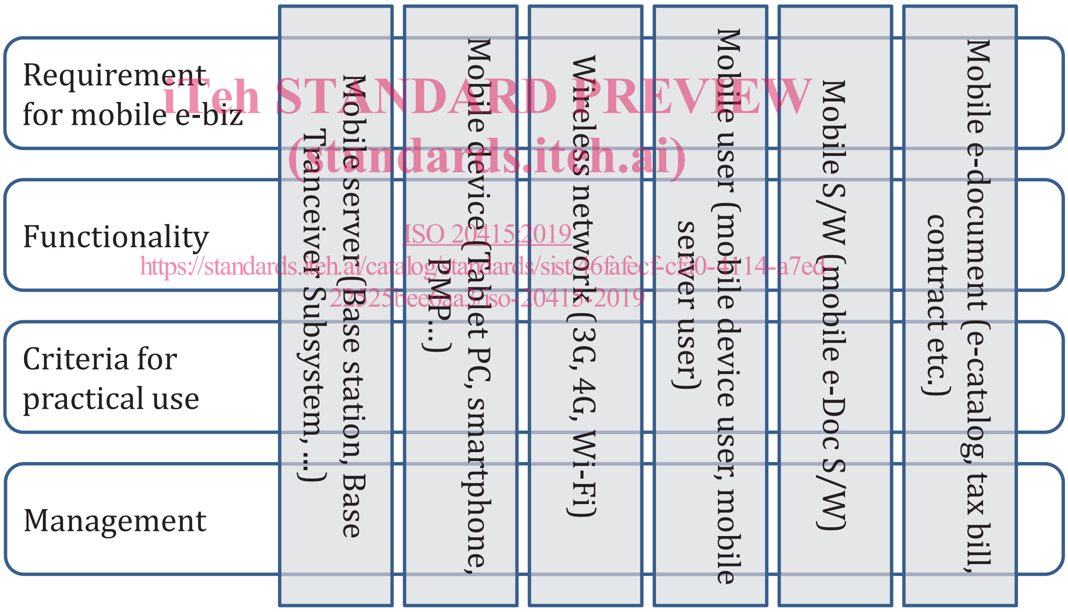
© ISO 2019 – All rights reserved

Trusted mobile e-document framework — Requirements, functionality and criteria for ensuring reliable and safe mobile e-business

1 Scope

This document provides a set of requirements, functionality and criteria for ensuring reliability and safety of mobile e-business.

The specification of this document covers overall use cases for mobile e-business including simple inquiry of electronic documents, exchange of electronic documents for general transaction and even exchange of contract and payment documents. This can be applied to the most wireless protocols such as 3G, 4G and Wi-Fi, etc. This could be also used in the general mobile e-business area such as logistics, electronic trades, financing, manufacturing and service, and can be referenced by system developers of electronic transaction using mobile devices, mobile network service providers and users. The scope of this document is shown in Figure 2.



iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO 20415:2019
https://standards.iteh.ai/catalog/standards/sist/26fafecf-c8f0-4114-a7ed-2b325beeb6aa/iso-20415-2019

Figure 2 — Scope of this document

This document is intended for:

— mobile-based electronic document system development, operation and certification organization;

— mobile electronic document software development organization;

— mobile electronic document third-party service provider organization.

2 Normative references

There are no normative references in this document.

© ISO 2019 – All rights reserved

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at http://www.electropedia.org/

3.1
acknowledgement
ACK
signal passed between communicating processes or *mobile devices* (3.9) to signify acknowledgement, or receipt of response, as part of a communications protocol

3.2
access point
AP
cellular base station, typically designed for use in communication business, which connects to the service provider's network via broadband

3.3
electronic document
digital representation of content that is stored and managed electronically

iTeh STANDARD PREVIEW

Note 1 to entry: Association of content, logical structure and display attributes, retrievable by a device capable of rendering a human-readable (or machine-readable) object. A document can be digitally born (creation) at source or converted from an analog document.

(standards.iteh.ai)

3.4
denial of service
DoS

ISO 20415:2019
https://standards.iteh.ai/catalog/standards/sist/46fafecf-cfa0-4114-a7ed-22525bee6aa3/iso-20415-2019

attempt to make a machine or network resource unavailable to its intended users, such as to temporarily or indefinitely interrupt or suspend services of a host connected to the mobile network

3.5
digital signature
data appended to, or cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and *integrity* (3.8) of the unit and protect against forgery by, for example, the recipient

3.6
electronic signature
data which, when appended to a digital document, enable the user of the document to authenticate its origin and *integrity* (3.8)

3.7
handover
ability which allows a *mobile device* (3.9) to continue the service offered by the previous cell even if it moves out of the cell to another cell

3.8
integrity
attribute of a document whose content is unimpaired

3.9
mobile device
MD
device for mobile e-business

EXAMPLE Smartphone, notepad, etc.

© ISO 2019 – All rights reserved

3.10
mobile server
MS
server which sends message or receives from *MD* (3.9) through *AP* (3.2) and authenticates MD, software (S/W)

3.11
mobile communication
data and *electronic document* (3.3) transmission through wireless network such as CDMA, WCDMA, Wi-Fi, Wibro, etc

3.12
negative acknowledgement
NACK
negative *acknowledgement* (3.1) for transmission control and confirmation

3.13
personal identification number
PIN
numeric password shared between a user and a system, which can be used to authenticate the user to the system

3.14
public key infrastructure
PKI
set of hardware, software, people, policies and procedures needed to create, manage, distribute, use, store and revoke digital certificates and manage public-key encryption

iTeh STANDARD PREVIEW
(standards.iteh.ai)

3.15
public key certificate
digitally-signed statement that binds the value of a public key to the identity of the person, device or service that holds the corresponding private key

ISO 20415:2019
https://standards.iteh.ai/catalog/standards/sist/46faaec1-efa0-4114-a7ed-22525bec6aa5/iso-20415-2019

3.16
short message service
SMS
text messaging service component of phone, Web, or *mobile communication* (3.11) systems which uses standardized communications protocols to allow fixed line or mobile phone devices to exchange short text messages

3.17
synchronous message
SYN
message packet for requesting session connection in TCP (transmission control protocol)

3.18
timestamp
sequence of characters denoting the date and/or time at which a certain event occurs

3.19
trusted mobile e-document framework
TMEF
electronic document (3.3) framework operating in the mobile environment which can overcome the difficulties of the authentication, the limited resources of a *mobile device* (3.9), unreliable data transmission channel and the instability of the data exposed

© ISO 2019 – All rights reserved

3.20
trusted communication
qualified electronic communication including secure and reliable transfer of *electronic documents* (3.3) and its provable custody for the purpose of dematerialization in the distributed open environments in achieving the certainty, the completeness and the confidentiality of communication

3.21
wired equivalent privacy
WEP
security algorithm for wireless networks introduced as part of IEEE 802.11 whose intention was to provide data confidentiality comparable to that of a traditional wired network

3.22
Wi-Fi protected access
WPA
security protocol and security certification program developed by the Wi-Fi Alliance to secure wireless computer networks

3.23
wireless public key infrastructure
WPKI
infrastructure for *PKI* (3.14) in mobile system

4 General requirements

iTeh STANDARD PREVIEW
(standards.iteh.ai)

4.1 General

The TMEF has the precondition that it is a kind of framework and the presented functions shall be executed in reality after being implemented. Therefore, there are general requirements which the TMEF shall possess considering the environment where the TMEF is executed, implemented technology and user aspect. This clause describes the general requirements of TMEF.

ISO 20415:2019
https://standards.iteh.ai/catalog/standards/sist/...

4.2 Capability of linkage with wired environment

Electronic documents created under a mobile environment may be used under a wired environment and a document created under a wired environment may be used in an MD on the contrary. Therefore, functions described in the TMEF shall consider linkage and interface with the wired environment. Although a protocol on the physical level or link level of the wireless network is not directly linked with a wired environment, a linkage on the session level or application level shall be adequately considered at all times. ISO/IEC 27033-3 specifies standards for wired network security threats, design techniques and control issues, and ISO/IEC 27000 provides information security management concepts and vocabularies. In general, communication interfaces of wireless network and wired network are implemented in a mobile server (MS). A kind of message communication software can be used without classifying it as wired or wireless. In such a case, the linkage of wired and wireless network is accomplished just by using the software. However, if communication software is used in exclusively wireless or wired network, it is necessary creating a protocol linkage interface in order to link between wired protocol and wireless protocol.

4.3 Generality of applying various wireless network

Types of wireless network are very diverse and its evolution speed is very fast. Mobile electronic transactions may be performed on all kinds of wireless network. Therefore, a TMEF shall possess generality so it may be applied to all kinds of wireless network. In other words, a TMEF shall not be based on a specific wireless network or a specific function which the specific wireless network possesses and shall be able to present protocol requirements or criteria for use to overcome the limitations of the wireless network based on the universal characteristics possessed by the specific wireless network.

© ISO 2019 – All rights reserved

4.4 Minimum protocol set

The TMEF gets executed in a mobile environment and it generally has the restrictions of computing resources and the limitations of a wireless network. Recently, the performance of the MD or the transmission speed of the wireless network is rapidly getting developed along with the development of technology; an MD still has the limitations of a portable device. Therefore, it possesses various types of problems such as battery capacity, small screen or coexistence of deteriorated mobile networks. Therefore, a set of functions that construct the TMEF shall become a minimum set which is light but can be executed quickly as the one that can be executed under various mobile network environments without putting the burden on the MD as much as possible.

4.5 Neutrality of technology

All contents described by the TMEF shall be technologically neutral. In other words, they shall not include the special functions that are dependent on a specific technology or protocol and shall become a form to describe by deriving a common denominator on universal and essential functional requirements of the protocols. The neutrality of a technology can be confirmed by whether the technology fully complies with international standards. For example, if a user authentication technology using biometric information fully accommodates the ISO/IEC JTC 1/SC 37 standard, it can be said that the technology guarantees the neutrality. Special technologies that became generalized or standardized already may be used at the position of being technologically neutral. The TMEF can become free from the problems that fall under a technology license when it is technologically neutral and based on the standard.

4.6 Feasibility of implementation

iTeh STANDARD PREVIEW
(standards.iteh.ai)

The TMEF shall be described using the functions or the protocols that are commercialized already or most widely used on the spot. In other words, it shall be written based on the currently released technologies and the development shall be possible for all users without any limitations on the technology by doing so. If a TMEF gets written based on a technology which is not released yet or will be released in the future, the possibility of implementing the TMEF will be lower.

ISO 20415:2019
https://standards.iteh.ai/catalog/standards/sist/46fafeefc-da04-4114-a7ed-22525bee6aa3/iso-20415-2019

5 TMEF environment and model

5.1 Physical environment

The TMEF physical model has major components enabling electronic document exchange, such as mobile devices, wireless communication networks, access points, the mobile service providers, electronic document systems, trusted communication systems and wired communication networks as shown in Figure 3. The following is a description of the physical model components:

— wireless communication network: a network that allows to send and receive electronic documents over the air such as CDMA, WCDMA, Wibro, Wi-Fi, Bluetooth, etc;

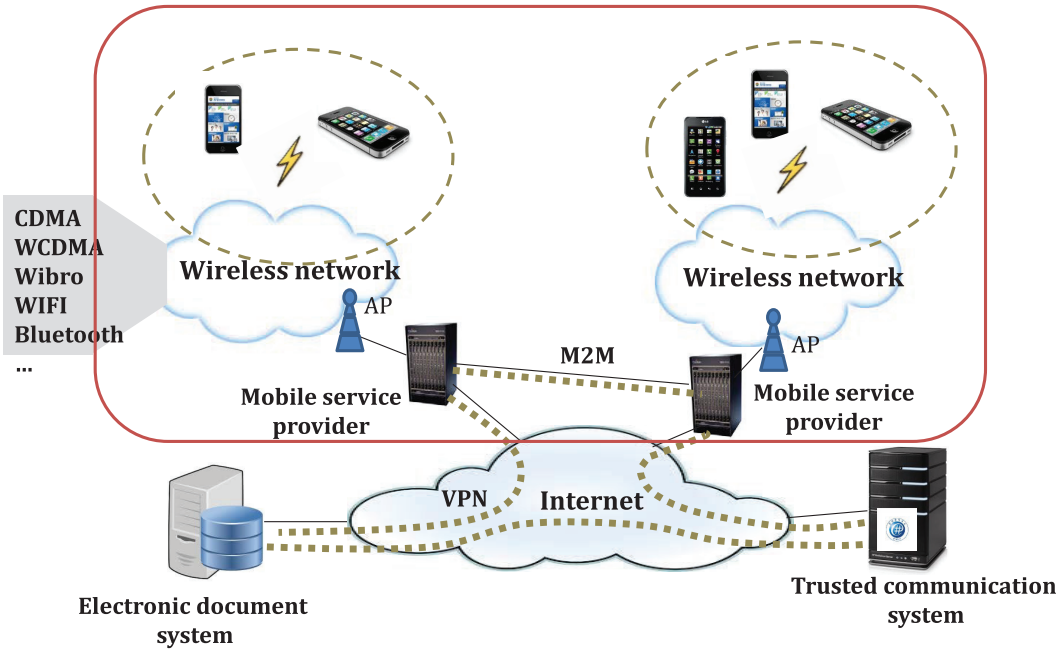
— mobile service provider: an organization which operates a wireless network for electronic data interchange and authenticates the mobile devices on the wireless network, the mobile application, and the mobile users;

— electronic document system: a system for managing and distributing the electronic documents which is connected to the mobile service provider for exchanging electronic documents;

— trusted communication system: a system which exchanges electronic documents in a reliable way and safely through a wired network and provides the legal evidence available;

— wired network: passage which distributes electronic documents by utilizing VPN or by securely encrypted messages.

© ISO 2019 – All rights reserved



Key

M2M mobile to mobile communication

Figure 3 — Physical environment for the TMEF

iTeh STANDARD PREVIEW
(standards.iteh.ai)

5.2 TMEF logical model

ISO 20415:2019

The TMEF logical model is composed of the requirement for mobile e-business, functionality and criteria for practical use and management as shown in Figure 4.

Safety and reliability are the main requirements in a mobile electronic transaction. Safety means whether an electronic document can be transmitted to a proper counterparty without exposing or damaging such an electronic document when a user uses an electronic document under a mobile environment. Reliability is whether the counterparty of mobile electronic transaction and the action of mobile electronic transaction can be trusted. A party of mobile electronic transaction shall be able to verify the identity of the transaction partner, effectiveness of the MD and even the operating system (OS) or S/W which the MD is equipped with. An action of electronic transaction includes all activities of sending or receiving the messages necessary for electronic transaction through wireless network and all activities to create or manage electronic documents using an MD.

Functions for implementing the requirements of mobile electronic transactions and the application standard for realistically utilizing such functions are required. Functions in a TMEF are composed of an authentication function for the authentication of the user and MD, a trusted messaging function and a safe messaging function in order to completely make up for the vulnerabilities of mobile electronic transaction. Since these functions are utilized under the mobile electronic transaction environment, they shall satisfy the requirements according to the environmental characteristics of the mobile system. The TMEF includes descriptions on the roles of each function, common and detailed functions, and the technologies that are realistically available.

The TMEF describes the functions which enable safe and reliable mobile electronic transactions, and a superset of detailed functions. Although it could be possible to make all functions described in the TMEF for implementing a mobile electronic transaction system, situations of having no choice but to select specific functions as the variables such as business situation, technical skill, cost or available mobile network are given. In such cases, the standards of conformity to select and combine the detailed functions are necessary considering realistic variables without creating problems on safety and reliability. In a TMEF, this is presented as an item called usage criteria.

 © ISO 2019 – All rights reserved