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

Reference number
ISO 20415:2019(E)

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

Contents

Page

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.

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

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.

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.

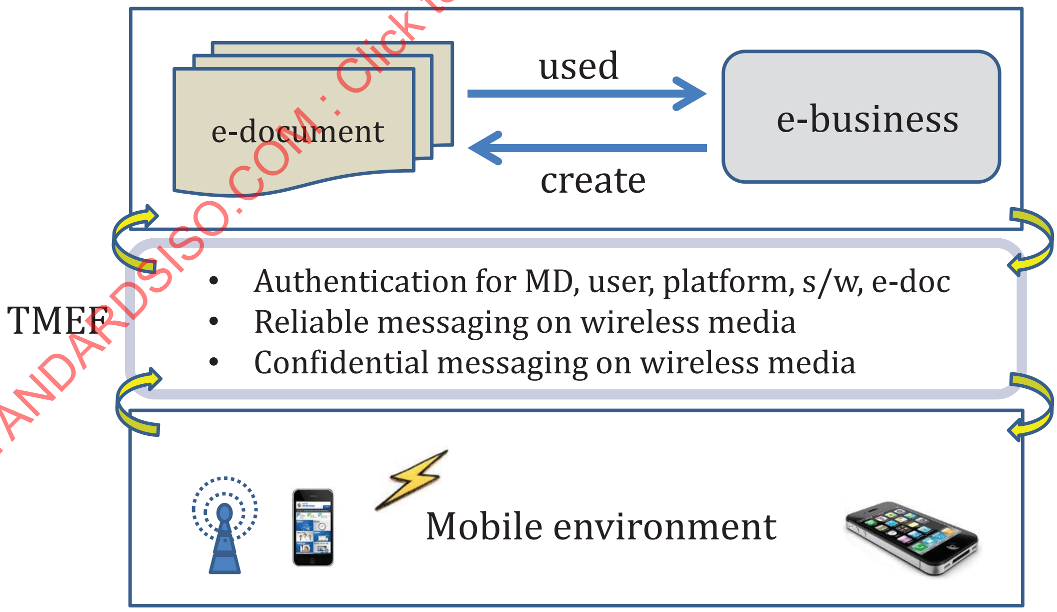

e-document
used
create
e-business
TMEF
Authentication for MD, user, platform, s/w, e-doc
Reliable messaging on wireless media
Confidential messaging on wireless media
Mobile environment

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 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.

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.

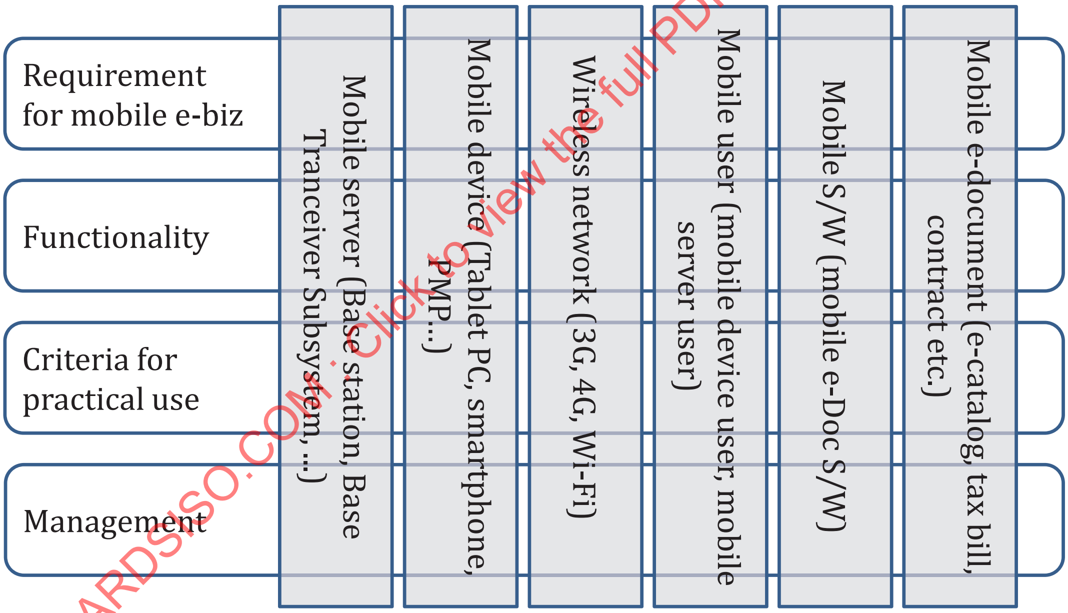

Requirement for mobile e-biz
Functionality
Criteria for practical use
Management
Mobile server (Base station, Base Tranceiver Subsystem, ...)
Mobile device (Tablet PC, smartphone, PMP...)
Wireless network (3G, 4G, Wi-Fi)
Mobile user (mobile device user, mobile server user)
Mobile S/W (mobile e-Doc S/W)
Mobile e-document (e-catalog, tax bill, contract etc.)

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.

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

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.

3.4
denial of service
DoS
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.

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

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

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

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

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.

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.

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

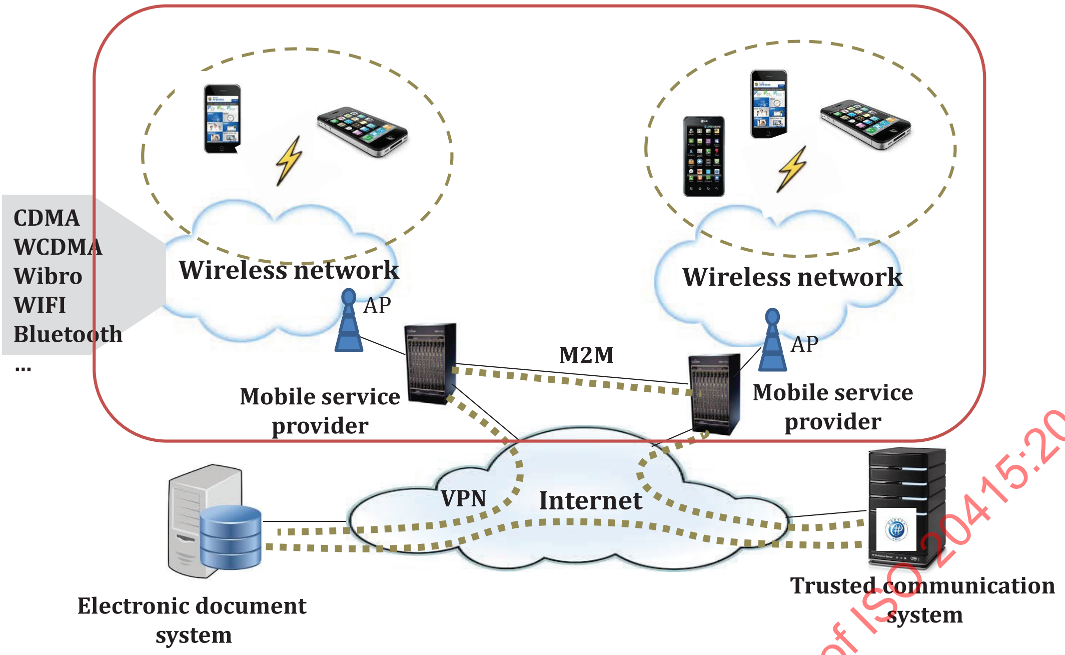
The TMEF shall be described using the functions or the protocols that are commercialized already or most widely used on the spot. In other words, it shall be written based on the currently released technologies and the development shall be possible for all users without any limitations on the technology 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.

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.



Key

M2M mobile to mobile communication

Figure 3 — Physical environment for the TMEF

5.2 TMEF logical model

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.

Once a TMEF is implemented, and an electronic transaction is performed because a safe and reliable mobile electronic transaction environment is formed, each function which construct the framework or MD, MS and wireless network shall be managed and monitored according to a standard that can guarantee safety and reliability. For this, subjects of management and criteria for management on mobile electronic transactions shall be presented.

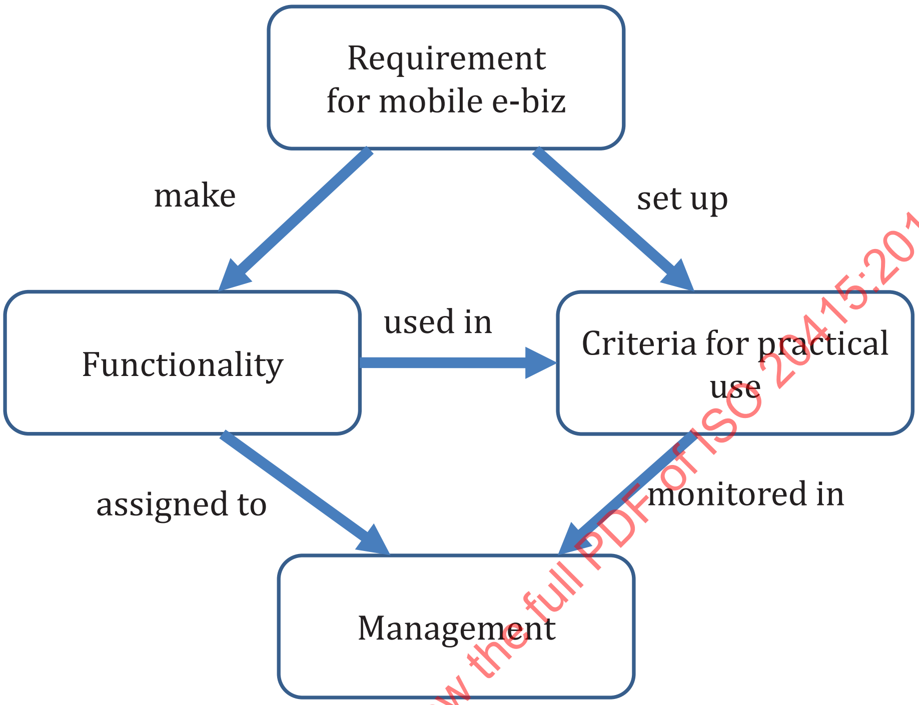


Figure 4 — TMEF logical model

6 TMEF functionality

6.1 General

This clause suggests the functionality for implementing reliable transmission/reception of electronic documents for electronic transaction in the mobile environment from an aspect of authentication, security and reliable transmission.

TMEF functions are composed of essential items in order to transmit e-business electronic document messages through the mobile channels safely and reliably. This clause describes requirements for each function, processes, considerations for implementation and preconditions. Figure 5 shows the functions, subfunctions and functional requirements of the TMEF.

	Requirement	Sub-functionality
Mobile authentication	• Simple • Reliable • Secured	• User authentication • MD & OS platform authentication • E-doc & S/W authentication
Mobile confidentiality	• Usable performance • Robustness • Agility	• Confidentiality for wireless channel • Confidentiality for electronic document • Confidentiality for MD
Mobile reliable messaging	• Recoverability • Continuity • Robustness	• Wireless session detection • Wireless session recovery • Transmission guarantee • Sequential transmission • Mobile e-doc handover • Mobile transaction
Mobile env. management	• Sustainability • Reliability • Availability	• User management • MD management • Wireless channel management • AP & mobile server management

Figure 5 — Overview of the TMEF functionality

6.2 Mobile authentication

6.2.1 Requirements

Mobile authentication is the starting point to use the electronic document reliably in the MD. The mobile authentication functionality shall be simple, reliable and secured.

Mobile authentication includes the authentication process for mobile users, MD and applications. As each authenticating process requires each data transmission, it shall not require too much data transmission/reception, and the data transmission shall be easy to use. An extensible and integrated authentication protocol is required for simple encapsulation which can access any type of authentication link and can use various authentication methods. It may play a role in transmitting various types of authentication methods and enhancing the convenience of authentication.

Mobile authentication shall be reliable in any cases. Despite the fact that the MD has an original risk factor in reliability, if the mobile user and MD is authenticated through a reliable authentication process, the result shall be reliable. Not only the MDs, but the authentication process of MD users and MD platforms shall be trusted by all mobile users. To make this possible, this shall be based on a reliable and safe mobile transmission protocol.

Data used during the mobile authentication process shall be kept confidential. Data transmitted/received during the mobile authentication process shall be encrypted, and key values used for encryption shall be stored safely. Even when the MD is physically robbed or lost, information for authentication shall not be exposed.

6.2.2 Authentication process

In order to transmit/receive electronic documents safely and reliably through the mobile devices, it is necessary to perform authentication on users, electronic document-related applications, mobile OS platforms and the mobile devices in authentication process as shown in Figure 6.

— User: performs identification of a user who has the right to use the mobile device and electronic document software installed in the device.

- — Electronic document and application: means to authenticate the validity of the electronic document application, which performs the authentication using the number authorized according to the authentication process when installing the app. Also, an electronic signature may be attached using an individual key and time stamp information of the MD owner on the electronic documents created within an application and may be used for verifying the integrity or confirming the authenticity of the electronic document.
- — Mobile OS platform and mobile device: authenticates that a mobile device maintains the same integrity and data protection as it was released without any mobile OS platform falsification by a random user and is used without reproduction, wiretapping or insertion of malicious codes.

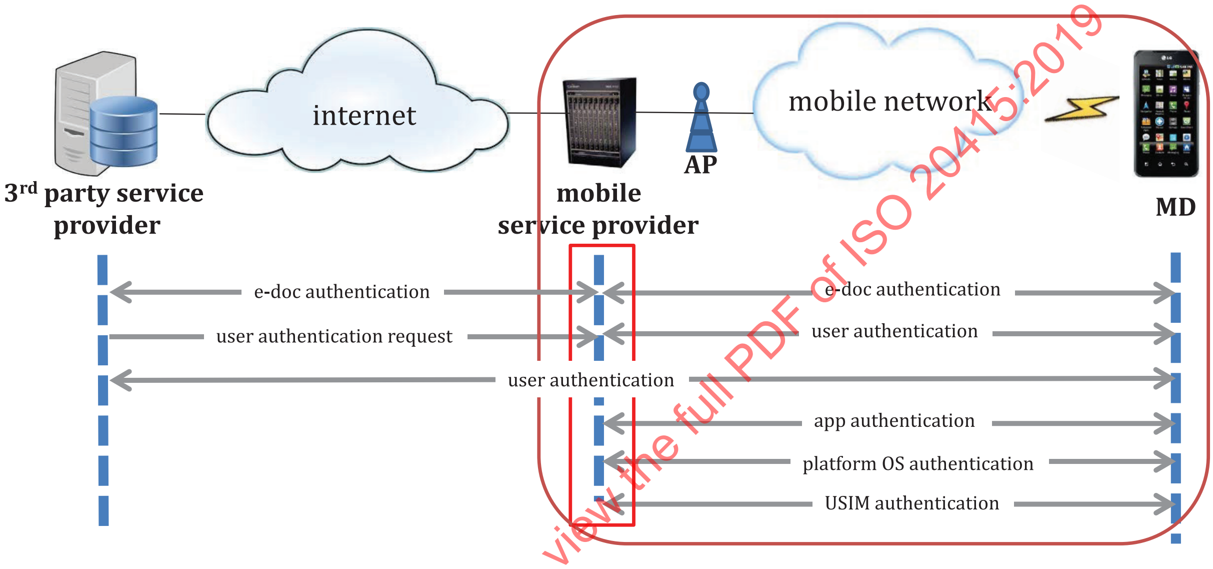


Figure 6 — Authentication process in the TMEF

Authentication on MDs and OS platforms shall be performed by a mobile service provider in advance before using the electronic document S/W. This is a precondition for using electronic documents by utilizing an MD. Therefore, it precedes the authentication on other subjects of authentication.

Authentication on electronic document S/W is performed by a mobile service provider. When a S/W producer writes a S/W and registers this to a mobile app market, a registration number gets assigned after the verification on the S/W. S/W authentication gets performed through this registration number before using the S/W.

Authentication on an electronic document gets performed through an electronic document S/W when required by the user. If there is an electronic document authentication request, a digital signature on the electronic document shall be created to be attached on the electronic document S/W and the authentication of integrity on the electronic document shall be possible through the created digital signature on the electronic document S/W.

Authentication on the user shall be classified into two types of cases according to the subject of authentication. First, if the subject demanding authentication is a third-party electronic document service business, authentication on the service user is absolutely required and the user authentication may be performed directly based on the ID/password of the user retained by the company. Second, there are also cases where the subject of authentication becomes a mobile service provider. They're cases where a third-party service business or an app developer consigns the user authentication duties to a mobile service provider, or cases of using by selecting the optional service of user authentication provided by a mobile service provider.

The mobile service provider shall be held responsible when a problem occurs due to an error of the electronic document S/W, mobile OS platform or MD authentication. The user shall be held responsible in case of electronic document authentication errors due to a user's error or blunder. In case of an authentication error due to the problem of S/W itself, the S/W producer and the mobile service provider that has authenticated such S/W shall be held responsible together. In case of user authentication errors, a third-party service provider shall be held responsible if the third-party service provider authenticated the user and a mobile service provider shall be held responsible followed by the authentication error if a mobile service provider performed user authentication duties by consignment.

6.2.3 Functionality for authentication

User authentication means to identify a user who has the right to use mobile devices and electronic documents installed in them. Even if a user does not have the right to use the mobile device, the user can easily attain or temporarily use it. The use of mobile electronic document software by a user who does not have the right shall be able to be prevented, and this can be done through the mobile user authentication. Currently, the most typical user authentication technologies being implemented by MDs or mobile service providers are as follows.

- One-time password is an authentication method where a user with a one-time password generator enters a password randomly created by the one-time password generator and identifies the user when the user wants to use mobile electronic document software. Users can receive the one-time password generator from a communications company or install one-time password-generating software in mobile devices.
- Using WEP protocol, possibility of mobile network access may be identified by checking the password which a user entered from the AP of the network when the user connects to a certain mobile network.
- User authentication may be performed using a PKI or WPKI (Wireless PKI) based accredited certificate.
- SMS authentication is a method where a user registers the user information on the mobile server of the communications company in advance, and when the user wants to get authentication, the user enters the user information. Then, if the information matches the predefined information, the mobile server sends a one-time password to MD.
- Authentication using PIN is a method where a user gets authentication from a communications company by entering his or her information and PIN number, and uses the PIN information for user authentication when it is required.
- Mobile accredited certification authenticates mobile users by utilizing a mobile accredited certificate saved in a mobile device. A user can get certification by entering the password of the mobile accredited certificate whenever the user uses the mobile software.
- User biometric information could be used for user authentication. The user biometric information includes iris, fingerprint, face and vein shape, which can be stored in the user's MD. User authentication can be performed by using the biometric information at the start of the MD or the use of the software.
- User authentication methods with even higher safety are also increasingly used by combining two or more types out of the methods above. For example, safety of authentication is drastically increased by combining the OTP (one-time password) and the user’s bio information to perform user authentication.

Confidentiality of the information received from an MS shall be maintained for the user authentication. Also, confidentiality shall be maintained through an encryption function even when registering the information necessary for user authentication to the MS. For this, an encrypted wireless channel shall be used. When registering information for the initial user authentication, there shall be a method to verify the identity of the user. Reliability of user authentication may be increased using the information which the user entered at the time of user authentication and the MD information at the same time by registering the verified user information and the MD information of that user at the same time. In case of not using the application for a fixed period of time after the user authentication, in other words after a fixed idle time passes by, the effect of user authentication shall be cancelled so that the use of application by a fake user may be prevented. When using the mobile accredited certificate, the biggest strength is that it can be integrated with the wired PKI system, and it is easy to apply under the integrated Internet environment. The PKI system shall verify various aspects of signature included in the certificate including whether a certificate authority has signed it or not, the appropriateness of the signature by the certificate authority, the usage of the certificate, and the expiration period of the certificate, in order to verify users' certificate. WPKI (wireless PKI) may perform the verification of certificate expiration period in an easier way or trust to the third party in order to reduce computing loads for verifying the certificate by mobile devices.

Authentication using WEP is dependent on the one-way authentication mechanism which authenticates a user in AP. Such a one-way authentication is not safe and may cause damages due to clone AP (AP configured by cloning a normal AP with the same configuration for malicious purpose) operated for a malicious purpose. The reason why such an attack is possible is that the mobile network service user does not get authentication on the AP which provides the mobile network service. That is, as WEP is one-way authentication, which may cause damages due to unauthorized AP or clone AP, users who use WEP shall take good care when using a mobile network service. Another weakness of WEP is that institutions which use mobile network use one fixed shared key as the WEP key value. As they use the same key values in all equipment using the mobile network, that is, AP and user devices, exposure of WEP key values may cause many security problems. As an institution using mobile network performs user authentication using one WEP key, when the WEP key is exposed externally, it is very dangerous. This is because an attacker can try to access the network using the acquired WEP key. If the WEP key is known to sub-contracting company's employees or visitors, the WEP key shall be changed regularly in order to reduce such a risk. As described above, when applying WEP, it typically uses a fixed shared key value, which causes several kinds of problems in security. To solve such problems, dynamic WEP shall be applied. An authentication server carries out authentication when a user tries to access and performs management works such as setting and renewal of WEP used in the institution.

Mobile user authentication using biometric information is increasingly utilized in mobile devices due to security and convenience. The user-specific uniqueness of biometric information suggests a reliable method for user identification. However, the possibility of theft or loss of the mobile device always opens the possibility of leakage of the user's biometric information. Leakage of biometric information can lead to problems such as leakage of important business documents such as contracts, leakage of user's personal information, or privacy invasion. Therefore, the user shall pay particular attention to the security of the biometric information stored in the mobile device.

MD authentication is to assure that MD maintains the level of data integrity and protection since it was produced without any changes in mobile OS platforms by a random user, and that MD is used without any copying, tapping or installing malware. For MD authentication, unique ID of each MD shall be authenticated first. Currently, MD user's information entered into a chip is used as an MD identifier, and the chip is called a USIM (universal subscriber identifier module) chip. Communications companies authenticate MD by using the identifier information contained in the USIM chip.

Authentication shall be done on the unique OS platforms, main platform data and major key values saved in MD. It shall verify whether mobile platform and main data are not changed or faked illegally by a random user. Main platform data and key values used in a mobile device are safely stored using a software system or hardware system. Software system encodes and stores main data of a mobile device which shall not be changed in the MD registry, and when MD authentication is required, it performs MD authentication by figuring out whether there is any change in main data based on such information.

Authentication of electronic document software is to verify the validity of electronic document software. MD can use only authenticated electronic document software, and for this, it requires an authentication process. As an electronic document software manufacturing company has issued software authentication numbers, these numbers are used for authentication.

Authentication on an electronic document created within an MD application shall be performed by verification of integrity or confirmation of originality. Electronic signature made by an individual key of a user stored inside an MD may be attached at the time of completing the preparation of an electronic document to be used for the verification of integrity which identifies the forgery status of electronic documents at the time of using the electronic document afterwards. Also, even verification on the originality of electronic documents is possible in case of creating electronic documents by including even the timestamp information of the time when the preparation of electronic document was completed to attach this on the electronic document.

Time stamp is the time indicated in a certain location in order to verify that data existed at some point, and a service technology which verifies that the electronic document has not been modified from a certain preparation time (originality) by storing the hash value of the electronic document with the standard time issued by the time stamp authority (TSA).

A time stamp is generally issued and authenticated through the accredited certification authority, the trusted third party (TTP) for its reliability of issuance and verification, but in some cases, it can be issued and authenticated independently by using a time stamp solution. A time stamp which uses the TTP is called as an official time stamp, while an unofficial time stamp is issued and authenticated independently.

The major function of the time stamp is to guarantee the existence time and the originality of electronic documents. When requesting application of time stamp to an electronic document, the TSA, a TTP issues time information based on the hash value of that electronic document as of the requested time, ensuring the existence time, and after some period of time, it warrants that the electronic document has not been modified since the time stamp was issued.

The service which provides the above function is called the time stamp service (TSS). When a user transmits the hash value, characteristic information of an electronic document to be issued with the time stamp to the TSA, the TSA gives and transmits the time information to the corresponding hash value. Then, for verifying the forgery of the electronic document, the user can compare the hash value of the electronic document with the hash value stored in the TSA.

Digital signature is a specific type of digital information attached to electronic documents in order to identify who signed the electronic documents and to determine whether the signed electronic document was not falsified or not, like a paper-written signature or seal.

The functions of digital signature include ‘identification’, ‘guarantee of the electronic document’s integrity’, ‘non-repudiation’ and ‘protection of personal information.’ ‘Identification’ means a function to verify and authenticate whether a person who sent a message is an actual party to a transaction through network. ‘Guarantee of the electronic document’s integrity’ is a function to verify that the electronic document being transmitted or received is prepared based on the signer’s declaration of will and there is no fabrication (forgery and falsification) during distribution or storage. ‘Non-repudiation’ is a function which can be utilized as an evidence for dispute in the future as well as to prevent repudiation of transaction by authenticating the transaction electronically. ‘Protection of personal information’ is a function which prevents anyone other than transmitters and receivers from confirming information (transaction, personal information and etc.) exposed due to Internet openness based on the PKI technology.

Digital signature is what converts (encrypts) the hash value of electronic documents into an individual key (digital signature-generating information) through the PKI, and the verification of digital signature is to invert the generating process. That is, when converting the digital signature into the signer’s public key (digital signature verifying information) and comparing it with the hash value of the target document, if the two values are the same, the digital signature is right, and if they are different from each other or there is an error, the signature is wrong. Like this, when attaching digital signatures to electronic documents, it is possible to assume that there is no modification in the document before and after the signature. Through this, the digital signature can be used as a means to confirm that the electronic document has not been forged or falsified during the distribution or storage process (integrity).

The confirmation of integrity of electronic documents by the digital signature is primarily for identification of the person who prepares it, and in order to maintain the originality, it shall be linked to the time confirming authentication (time stamp) technology. Also, due to the limits in expiration date (1 year) of the digital signature certificate, a digital signature for long-term verification linked to time confirming authentication shall be applied to electronic documents which require to be stored for a long time, and this kind of digital signature for a long-term verification is designated by ISO 14533-1.

6.2.4 Usage criteria for authentication

6.2.4.1 General

For the reliable and safe electronic transaction, one may just perform authentication using the safest authentication method on all authentication subjects mentioned in 6.2.2. However, requiring the best authentication method on all authentication subjects at all times may cause a problem with the possibility of implementation because of the limitations of computing resources that a mobile environment has. Therefore, a way to adjust the authentication subject or method flexibly according to business conditions, legal effect status of the electronic document and possibility of forgery within the extent of not harming reliability and safety of mobile electronic transaction is necessary. Thus, the items that have an effect on selecting authentication subjects or methods within the extent of not harming reliability and safety of mobile electronic transaction are called usage criteria.

6.2.4.2 User authentication

If the current mobile electronic transaction partner is positively identified by context information or situation information, authentication on the user may be omitted. For example, transaction documents exchanged synchronously after the user authentication do not have to go through the authentication every time.

User authentication by WEP is a one-way authentication and user information may be exposed in case of hacking by AP modulation. Therefore, it is desirable to combine it with other user authentication methods.

Although the user authentication method by ID/password is very simple and inexpensive, risks followed by the exposure of ID/password lies dormant. This method may be used if the effect of user authentication error on the business is trivial.

If the effect of user authentication failure on the business is significant, it is safe to use a method that has combined several authentication methods or an authentication method with low authentication failure rate. However, since the user authentication with low authentication failure rate brings an incidental effect called the increase of cost, the cost aspect also shall be considered along with safety when selecting the user authentication method.

6.2.4.3 Electronic documents and applications

Electronic document authentication is not absolutely required if the electronic document in use may be disclosed as a subject of simple reference. However, a mechanism for verifying integrity or confirming originality shall apply in case of the mobile electronic documents that have legal effect.

Since applications continue to be used for writing and storing electronic documents, they shall be authenticated through the verification of application authentication number.

6.2.4.4 Mobile OS Platform and MD

Forgery of mobile OS platform is very easy. Since the damage on the business may be very significant, if a fraudulent act is performed by the forgery of platform, authentication shall be performed using platform number, etc. prior to the use of platform.

Since MDs also may be forged easily by theft, authentication of MDs through a USIM shall precede in every case.

6.3 Mobile confidentiality

6.3.1 Requirements

Confidentiality shall be maintained on MDs, electronic documents used in MDs and the wireless network to send them under any circumstances. Under a wireless environment, anyone can easily intercept or alter data through wiretapping or monitoring. Even worse, one may impersonate a falsified user by stealing the MD itself. Through a satisfactory maintenance of confidentiality which may become most problematic in terms of security in a mobile communication, even the integrity of mobile electronic documents may be guaranteed, and it even enables safe transmission and reception of the data used in the mobile authentication process.

In order to ensure the confidentiality of mobile data in an environment where the flow of data is easily exposed in the wireless network and the problems are caused by it, the mobile system shall have the following characteristics:

— Performance: Although the performance of MDs has improved a lot, there is still a lot of burden to fully use the algorithm for security. Therefore, high confidentiality shall be maintained even with the limited computing resources of the MD. For example, an algorithm showing high security level even with low key value or operational time shall be used.

— Robustness: MDs may get lost or stolen easily and the wireless network may be suddenly interrupted. In other words, since the types of situations that may suddenly occur are too diverse compared to the wired environment and the intensity of shock followed by such a situation is also great, the robustness to prepare for such situations is required. For example, methods to prevent the leakage of important business documents stored inside even under the situations of drastic accidents such as loss of MD shall be presented.

— Agility: Types of security attacks on wireless networks are getting very diverse and intelligent. Therefore, pre-emptive and active security measures are required. For example, one shall be able to fundamentally block the illegal network access by changing the encryption key value or changing the network configuration on a regular cycle.

6.3.2 Sub-functionality for mobile confidentiality management

6.3.2.1 General

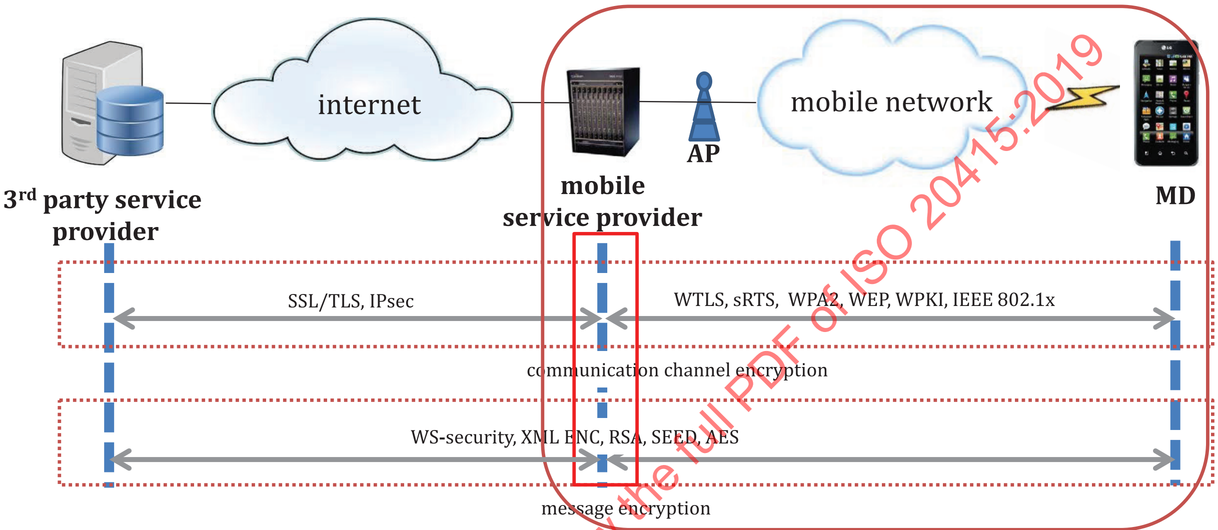
Subjects of confidentiality under the mobile environment are MDs, wireless channels and electronic documents. Since it is impossible to apply confidentiality on OS and all apps in an MD, it is performed as a form of storing platform key values or various types of important information requiring confidentiality management into an MTM (mobile trusted module), For the confidentiality management, encryption function on a wireless channel is the method of encrypting all data exchanged on the channel using a fixed key or a variable key. Encryption of electronic documents is performed by the method of pointing out and encrypting specific parts of the electronic document contents. Confidentiality shall be managed on MDs and electronic documents by the user, and the encryption of wireless channel shall be guaranteed by the MD and MS.

6.3.2.2 Confidentiality for wireless channel

Mobile channels can be more vulnerable to sniffing and spoofing caused by inappropriate users compared with wired channels. Accordingly, when transmitting or receiving electronic documents through wireless channels, encryption shall be considered and assumed. However, it is necessary to adopt a proper encrypting method suitable to the mobile type, by considering the computing power of MD and the bandwidth of mobile channels.

The method to encrypt wireless channels can be divided into the static way and the dynamic way based on the type of encryption key. And it is also divided into the single authentication method and the mutual authentication method. The static method generates the encryption key and uses it through mobile network without any changes, which is vulnerable to mobile network attacks and it is not easy to distribute the encryption keys safely. The dynamic method generates the encryption key frequently during mobile transmission and reception, which is far safer than the static one. A single authentication only performs the authentication process on the MD for two-way communications between the MD and the mobile server, while a mutual authentication performs two-way authentication between the MD and the mobile server. Also, as shown in Figure 7, the protocol for mobile channel confidentiality can be divided into a protocol applicable to the transport layer and a protocol applicable to message encryption.

In order for the MD to use the wireless network, it shall know the name of the AP, which is the so-called SSID (service set ID). One SSID shall be assigned to each access point, and the SSID is used in the wireless network list when composing a wireless network. The AP broadcasts its own SSID and does not support security. The AP utilizes the MAC (media access control) address for identifying the MD in the mobile network. However, as the MAC address can be easily copied or changed for use, it has a problem for being used as an access control to mobile network.


internet
mobile network
AP
3rd party service provider
mobile service provider
MD
SSL/TLS, IPsec
WTLS, sRTS, WPA2, WEP, WPKI, IEEE 802.1x
communication channel encryption
WS-security, XML ENC, RSA, SEED, AES
message encryption

Key

WTLS	wireless transport layer security
SRTP	secure real-time transport protocol

Figure 7 — Mobile confidentiality protocols

Device authentication protocols for wireless channel encryption and encrypted transmission/reception between devices shall be as follows.

- WEP encrypts the mobile network channel using the encryption keys. But, as it uses a static encryption key, it is vulnerable to passive and active network attacks. In addition, it is not easy to distribute the encryption keys safely.
- WPA uses a dynamic encryption key by enhancing the vulnerability for encryption. It uses TKIP (temporal key integrity protocol) as an encryption technique, which is a method to generate new keys for encryption at regular intervals when transmitting packets. It can minimize the risk of hacking by changing the encryption keys dynamically.
- 802.1x authentication and EAP (extensible authentication protocol) is a port address protocol which protects the network through authentication. When a wireless network user gets authentication through 802.1x for network access, the access point opens a virtual port, permitting the communications, and when failing to get authentication, the user cannot use the virtual port, blocked from the communications. Major components include the MD, the access point and the authentication server.

— As MD5[1] has no mutual authentication stage toward the MD and network, it only provides one-way authentication. Above all, it does not support automatic distribution and circulation of WEP, which cannot reduce the management burden of manual WEP key maintenance, so it is rarely used.

6.3.2.3 Confidentiality for electronic document

For security, a transmitter can select the encryption method and transmit electronic documents which are attached for mobile transmission/reception. This is for confidentiality of documents, which is different from network encryption.

Encrypted section ranges from the MD to the mobile server or from the MD to a receiver's MD. When encrypting attached documents, if encryption "from the MD to a mobile server' shall be maintained, a transmitter shall encrypt the mobile server for the server to be decoded by encrypting it with a public key of the mobile server. In this case, the mobile server shall manage the transmitting/receiving history in an encrypted state and manage the individual key and password for accessing to the individual key in order to decode encrypted documents.

When encryption "from the MD to the MD" shall be maintained, it shall be possible for a receiver's MD to be decoded by encrypting the MD with a public key. But, when it is requested to decode the documents encrypted based on the agreement between a mobile server and the receiving MD, the transmitting MD shall encrypt the document to be decoded in both the mobile server and the receiving MD. The mobile server shall manage the transmitting/receiving history at an encrypted state and manage individual key and password for accessing the individual key for the encrypted documents to be decoded. Here, the mobile server shall notify the receiving MD that the encrypted documents can be decoded by the mobile server. When the transmitting MD transmits documents to the receiving MD, the receiving MD shall register the range of encryption to the mobile server in order to identify the range for encryption.

6.3.2.4 Confidentiality for mobile device

Mobile device security means a device to protect various kinds of data and electronic documents in an encrypted type and to block a random usage when the MD is lost or robbed.

The MTM is a mobile information security technology which is equipped to the MD, blocking hacking perfectly. It is TCG (trusted computing group)-standard mobile security hardware which can solve all problems relevant to security including user authentication, platform authentication, device authentication and data protection.

An MTM-based MD security system can prevent information leakage due to lost/robbery, detect and respond to the attempt to change the MD environment and prevent illegal fabrication of the MD by unauthenticated users under an open platform environment.

The mobile MD security system shall be able to provide middleware management and security function abstract API (application program interface) in order to safely operate application services which require high level of security such as authentication/payment/smart banking in the MD.

The system shall perform the measurement and verification of integrity of terminal's boot loader, kernel, OS, major native system servers by stages when the MD is turned on, and it shall provide a function to detect illegal modification by MD hacking or malicious codes through the integrity verification.

6.3.3 Usage criteria for mobile confidentiality

6.3.3.1 General

For the mobile confidentiality, the best confidentiality can be maintained when all confidentiality functions mentioned in 6.3.2 are applied. In other words, the best confidentiality can be maintained by maintaining confidentiality of electronic documents, maintaining confidentiality of wireless

[1] A widely used cryptographic hash function producing a 128-bit (16-byte) hash value, typically expressed in text format as a 32-digit hexadecimal number.

transmission channels using a variable key, attachment of electronic signature by an individual key of the user and MD/MS authentication of both parties. However, the confidentiality which is adequate to guarantee safety and reliability may be maintained even if the next best combination is selected considering the performance or cost. The usage criteria for mobile confidentiality may be defined as the criteria which enable mobile system to maintain confidentiality to the extent of not introducing problems followed by the damage of confidentiality in the business aspect through the combination of certain confidentiality functions. Determination criteria to demonstrate the flexibility of applying mobile confidentiality are the openness status of electronic documents, the status of authenticating the MS already by a communication service provider and the number of people connecting to the mobile network.

6.3.3.2 Confidentiality of electronic documents

If there are no problems even if the electronic document is disclosed, it isn't necessary to apply the functions for maintaining confidentiality of documents. However, the confidentiality functions of electronic document shall apply in case of documents that have legal effect or contain nondisclosed information. If the confidentiality of the wireless channel is guaranteed, the application status on the confidentiality of the electronic document may be determined according to the business situation or company policy. For example, in case of electronic documents that shall not be exposed under any circumstances such as important contract information, etc., confidentiality functions of the electronic document and confidentiality functions of the wireless channel may apply at the same time.

6.3.3.3 Confidentiality of wireless channels

In order to guarantee reliability and safety of a mobile network, confidentiality of wireless channels shall be basically guaranteed. One-way authentication of the MD and two-way authentication of the MD/MS may be required for the execution of confidentiality on a wireless channel. At this time, authentication may be performed just with the one-way authentication of the MD by omitting the MS authentication by a reliable network service provider. Also, in case of wireless channels with great business impact followed by hacking, high risk of hacking requires a channel encryption using the variable key method rather than the fixed key method.

6.3.3.4 Electronic signature

In case of electronic documents with important significance in legal aspect such as contracts or transactions, the electronic signature is absolutely required. That is because the verification of integrity on the document is possible through the electronic signature. If a proof of the original is required, the electronic signature shall be written by including the information on the time of completing the preparation of the electronic document. In the PKI system, an individual shall use a private key to make an electronic signature for an electronic document, and in order for a business partner to verify the electronic signature, a public key certificate of the person who created the digital signature is required. However, the electronic signature is not required in case of electronic documents for simple reference or electronic documents that may be disclosed.

6.3.3.5 Confidentiality of the MD

It is safe to utilize the MTM in case of storing highest level of trade secret or information, etc into an MD. Or it is also possible to store in the MD by writing important company information as data of an encrypted form. In an MD which only stores information that can be disclosed, it isn't necessary to store the information as data of an encrypted form.

6.4 Mobile reliable messaging

6.4.1 Requirements

Mobile reliable messaging shall have a wireless session where a reliable messaging function shall detect whether the virtual line for communication is alive, shall revive immediately if a dead session is discovered, shall be able to handle as integrity even if handover occurs in the middle of transmitting/receiving messages and definitely prove that the message has been sent/received. In other words, mobile reliable messaging means a function which enables users to trust the fact that a message was transmitted within the time that can be understood by the sender/receiver even if a user does not have any status information on the mobile network or wireless network when transmitting messages via mobile. It may also include the function which enables the receiver to receive documents in the order sent by the sender depending on circumstances. Such reliable messaging has a few requirements.

- Recoverability: it shall have the ability to recover by itself. In other words, the ability to detect abnormalities and recover by itself is required even if the message transmission channel is broken.
- Continuity: it shall have the ability to transmit/receive data without disconnections even if the wireless channel is broken or handover occurs.
- Robustness: diverse forms of problems may occur in the wireless network and it shall have the robustness to transmit/receive electronic documents without problems even under such situations.

6.4.2 Functionality for mobile reliable messaging

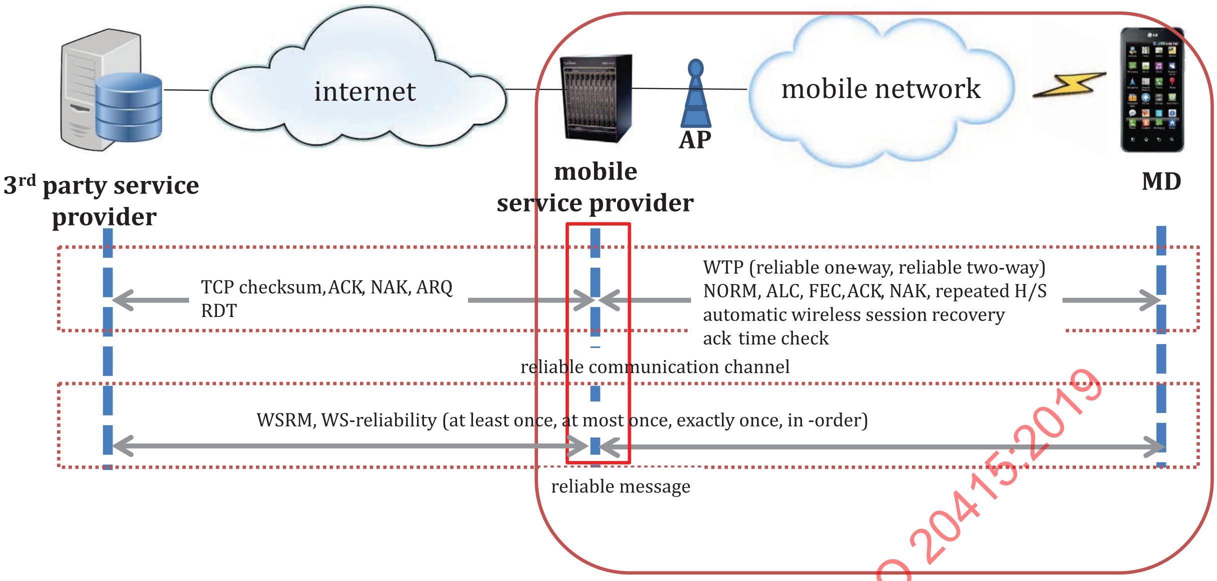
6.4.2.1 General

For reliable transmission of mobile electronic documents, it requires the ability for mobile session detection, mobile session recovery, transmission guarantee, sequential transmission, mobile transaction and handover. Since reliable messaging function is performed by transmitting and receiving messages between the MD and the MS, a mobile service provider shall monitor all status information at all times to prepare for the occurrence of problems.

6.4.2.2 Wireless session detection

When transmitting electronic documents through the mobile network, sometimes mobile channel does not work at an unexpected point of time. It is difficult to figure out whether the current mobile session is on or off when it enters a radio shadow area where it is hard to detect radio wave. In some cases, a DoS attack may disable a mobile session. In preparation for such a case, it is necessary to check the validity of mobile session constantly.

The mobile session detection means an ability to detect whether a session for transmitting/receiving electronic documents operates without any problems. In the mobile network, transmission may be slowed down randomly in the radio wave range, and abnormal situations may frequently occur such as hand-off, power-off or when the area covered by the AP is changed. Accordingly, there shall be criteria for determining whether there is an abnormality, and for checking the transmission/reception of message and the messaging point of time, which can check whether the mobile session operates normally or not. In order to detect the mobile session, the transmitting party shall be equipped with a device to receive the ACK message for confirming reception of the mobile data, and the receiving party shall have a function to make and transmit the ACK message including the message ID when receiving the data. Of course, the mobile receiving party shall have a function to determine whether the transmitted data loses data such as checksum, and the mobile transmitting party shall have a function to determine the validity of the transmitted ACK message.


internet
mobile network
3rd party service provider
mobile service provider
AP
MD
TCP checksum, ACK, NAK, ARQ
RDT
WTP (reliable one-way, reliable two-way)
NORM, ALC, FEC, ACK, NAK, repeated H/S
automatic wireless session recovery
ack time check
reliable communication channel
WSRM, WS-reliability (at least once, at most once, exactly once, in -order)
reliable message

Key

WTP	wireless transaction protocol
WSRM	web service reliable messaging
ARQ	automatic repeat request
RDT	reliable data transport
NORM	NACK oriented reliable multicast
ALC	asynchronous layered coding
FEC	forward error correction
H/S	handshake

Figure 8 — Mobile reliable transmission protocols

In the shadow area where electromagnetic waves are difficult to reach, it is unreliable to transmit or receive data. Even if the network transmits data at high speed, if the MD moves to the shadow area, the communication speed may suddenly drop or the communication session may be lost. If the MD leaves the shadow area, data communication can be restored. However, it is difficult to directly detect in the TCP layer whether the MD has entered the shadow area or got out of the shadow area, and it can only be estimated by receiving ACK messages.

When sending an SYN message, a data packet requesting session connection and losing it while transmitting through mobile network, the MS re-transmits the SYN message for session connection at a certain time interval. If the MS does not get ACK for the SYN message from the MD even after several attempts, the MS decides the connection failure.

While transmitting messages, it is possible to detect the validity of mobile session through NACK (negative acknowledgement). If the MS or MD does not receive the ACK of the specific ID packet after sequentially transmitting message packets, it determines that there is a problem with the mobile session.

The MS is responsible for the connection between the mobile network and the wired network, and the most important role is to map the mobile private IP port into the Internet authorized IP port. When a new MD requests network access, it makes network connection with a server in the public network by changing the network request into the public IP address of the mobile server. In this process, it maintains the session information which maps <private IP: port of the access device> into <public IP: port> in the mobile server. As long as this information is maintained, the device can exchange packets with the server normally. However, as it is not possible to maintain such information permanently, if there is no packet which is exchanged through this session, the information is removed and the network connection is forcibly terminated. In case of forced termination, the MD and the mobile server cannot communicate with each other through the same socket connection any longer. If it is necessary to maintain the network connection, a Keep-Alive message shall be transmitted before deleting the mobile session.

It shall be possible to detect that a message containing electronic documents is lost while sending the electronic document. In case that the message is lost due to the MD's entering the shadow area or a radio wave problem, the message shall be re-transmitted. As the MD requires time to recognize the gap between the time to start message loss and the time to recover the loss, it causes a time gap. It is most important in detecting the mobile session to minimize the time gap.

6.4.2.3 Mobile session recovery

While transmission/receiving electronic documents, mobile session recovery shall be arranged immediately after detecting a break in the mobile session. A process for doing this starts when it finds that data packet is being lost, or when it finds that the mobile server's session information has been deleted.

For recovering mobile session, the MD or MS shall have a function to promptly figure out whether the mobile session is broken or not. That is, it shall figure out whether the ACK message is delayed or lost, and immediately after figuring this out, it shall be able to re-transmit the lost message. However, in some cases, transmission delay may occur, without loss of message, so it shall have a function to effectively differentiate message loss from transmission delay. It shall have a function to transmit message stably through recovered session after recovering the mobile session.

6.4.2.4 Transmission guarantee

Transmission guarantee is to ensure the transmission of electronic documents between the MD and the MS. That is, an electronic document transmitted through mobile network shall be transmitted necessarily once. Of course, it would be better to transmit the document exactly once, in case that it is not possible, it shall be transmitted at least once. Transmission guarantee means a function to be able to send the electronic document data at least once in any cases. In case that the MD is in a radio shadow area or mobile radio wave is somewhat delayed, it may cause a situation where the transmitting party sends the electronic documents, but the receiving party has difficulty to confirm whether it receives them or not. In such a case, the transmitting party continues to resend the electronic documents until it receives a clear response from the receiving party. It requires a functional requirement to be able to set the time interval or the number of resending as an optimized value. The transmission guarantee can be arranged at the level of mobile transmission channel and at the level of electronic document application as shown in Figure 8.

— Mobile transmission channel

It is to give the sole identifier to the mobile transmission data packet and to figure out the integrity of data transmission when the MD or mobile server receives the data packet by checking whether the identifier has been lost or not. It adds the ID value of the received data packet to the ACK and allows the receiver to figure out whether data has been lost or not. Or, in case that the data packet is lost, the receiver sends the NACK to the transmitter, notifying that data has been lost.

— Electronic document application

The electronic document application transmits an electronic document and waits for the ACK message from a receiver. When it receives the ACK message, it considers that the receiver normally receives the electronic document and finalizes the electronic document transmission process. If it cannot get the ACK message, it re-transmits the same document. When it gets the ACK on the re-transmitted document, it finalizes the transmission process. But in some cases, if the receiver delays in sending the ACK or the transmitter gets the ACK message late due to a problem of the mobile channel, it may get the ACK message after re-transmitting the same electronic document. That is, the receiving application may receive the same electronic document more than once. In preparation for such a case, the receiving application shall have a function to delete duplicated electronic documents.

6.4.2.5 Sequential transmission

Sequential transmission means to match the transmitting order with the receiving order of the electronic document data packet. For doing this, it requires a field within the data packet having information on the transmitting order of the data packet. The receiving party shall have a function to reassemble data packets based on the transmitting order.

Sequential transmission is a means to allow the receiver to receive electronic documents in the order being transmitted by the transmitter when transmitting electronic documents. The sequential transmission can be arranged at both levels of mobile transmission channel and electronic document application.

— Mobile transmission channel

The transmitter can give a sequential number when transmitting mobile data packets composing the electronic documents, and the receiver can reassemble the electronic document data packet based on the sequential numbers.

— Electronic document application

The transmitter's electronic document application separately transmits data composing the electronic document, and at this time, it gives a sequential number to each data. The receiver's application combines data and reconfigures the electronic document based on the sequential numbers.

6.4.2.6 Mobile transaction

Mobile transaction means an ability to complete one unit for transmitting/receiving one electronic document (transaction) through the mobile network. Generally, the transaction for transmitting electronic document is completed when a transmitter sends one electronic document and a receiver sends an ACK message. When the transmitter cannot receive the ACK message under the abnormal situation, the ability to complete the transaction is required. Mobile transaction considers that one transaction is completed when it receives the ACK message on the electronic documents transmitted from the transmitting party. In order to prevent resending of message by the transmitting party before the ACK message arrives at the receiving party, the receiving party can send the hold-on message to the transmitting party in advance. That is, the receiving party requires a function to detect the delay of ACK sending and to send the hold-on message. The transmitting party shall not resend the data packet even when it does not receive the ACK, and when it receives a hold-on message from the receiving party, it shall be able to stop the transmitting process temporarily. In two-way mobile transaction, one mobile transaction is considered to be completed when the transmitting party sends a message, the receiving party sends the response message, and the transmitting party again sends an ACK message on the response data. The transmitting party shall store the history of the ACK message on the response data for a certain period of time after sending the ACK message for preparing the case that the response message is resent.

In order to transmit/receive electronic documents reliably using the mobile network, one of the following mobile transactions can be used:

— One-way electronic document transaction

It is a transaction which transmits one-way electronic documents from a transmitter to a receiver using mobile network. The transmitter waits for the ACK message from the receiver after transmitting the electronic document. When it gets the ACK message, the transaction is considered to be ended normally. If it cannot get the ACK message, it re-transmits the same electronic document. The receiver immediately sends the ACK message after receiving the electronic document and maintains the state information of the sent ACK message for a certain period of time through which it can respond to the problem of data loss or re-transmission of the same document.

— Two-way electronic document transaction

It is a transaction where a transmitter sends electronic document through mobile network, and the receiver sends a response document to the transmitter. The transaction is ended when the transmitter sends the electronic document, the receiver sends the response document, and the transmitter sends the ACK message to the receiver. As the receiver sends response document, which means that the receiver normally receives the transmitter's electronic document, the receiver does not need to send an additional ACK message. However, as the transmitter may re-transmit the same electronic document when the receiver's sending of the response document is delayed, in such a case, the receiver has to send the ACK to the transmitter that it shall hold on before the receiver sends a response document. The transmitter can prepare for the case where the responding message is re-transmitted by sending the ACK message after getting a responding message from the receiver and by saving the information.

6.4.2.7 Mobile document handover

The handover ability allows a mobile device to continue the service offered by the previous cell even if it moves out of the cell to another cell; when moving between sectors within the service cell or moving from one cell to another, the current wireless channel is automatically switched. For a natural handover, a handover at both the wireless and wired levels between the two neighbouring cells shall be established. The mobile document handover ability is an ability to enable seamless data communications even when a mobile device moves out of the cell range while transmitting/receiving an electronic document.

According to the range of handover, the mobile document handover is divided into intra-cell handover, inter-cell handover and inter-network handover summarized in Table 1. Intra-cell handover is also called "softer" handover as it occurs within a cell. It changes the channel in use within the cell coverage of the current terminal. A range of signals are supposed to overlap at the boundary between sectors, and in a softer handover, terminals that pass through such a boundary can communicate through the two sectors; this is possible because the transmission/reception signals generated in a base station are processed through a single final modulator/demodulator for the most stable handover. It is true that in most cases, electronic documents within a cell can be handed over without a data interruption, but coping with data discontinuity that may occur when a channel is changed is also necessary.

Inter-cell handover, also known as "soft" handover, is the most common handover adopting a "connect-before-break" method. It establishes a connection with a new base station before completely disconnecting from the previous base station. In this type of handover, an efficient technique is needed to minimize a handover delay and a cell loss that may occur in the course of a connection re-establishment or release of the existing connection. Inter-cell handover supports continuous communications of a mobile terminal that moves out of the existing cell boundary by linking it with a new base station. In this method, however, there is a high risk of data omission or data loss due to a handover delay in transmitting/receiving electronic documents.

Inter-network handover hands over the control to the base station of another layer to better process the signals; it does not indicate a handover caused by a signal movement (e.g. inter-layer handover in a hierarchical cell structure). If a method of distinguishing different frequencies or codes used between layer cells is adopted in a hierarchical cell structure, inter-layer handover can be made via soft handover. Such a soft handover, however, is not possible if different frequencies are used. Thus, a hard handover process, also known as a break-before-connect method, is needed to cut off the signals sent by the previous base station and to connect to the signals from the next new base station. When handover takes place between different networks, the method and environment for processing signals are different from network to network even if both networks use the same frequency; this may cause a momentary cutoff of conversation and reconnection attempt. Therefore, this hard handover shall overcome issues such as a complete cutoff of communications and reconnection attempt at the time of electronic document transmission/reception. Data transmission shall be resumed from the disconnected point after reconnection.