International Telecommunication Union

# ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

# X.1147

(11/2018)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Secure applications and services (1) – Web security

# Security requirements and framework for big data analytics in mobile Internet services

Recommendation ITU-T X.1147

International Telecommunication Union

ITU-T X-SERIES RECOMMENDATIONS

**DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY**

| | |
|---|---|
| PUBLIC DATA NETWORKS | X.1–X.199 |
| OPEN SYSTEMS INTERCONNECTION | X.200–X.299 |
| INTERWORKING BETWEEN NETWORKS | X.300–X.399 |
| MESSAGE HANDLING SYSTEMS | X.400–X.499 |
| DIRECTORY | X.500–X.599 |
| OSI NETWORKING AND SYSTEM ASPECTS | X.600–X.699 |
| OSI MANAGEMENT | X.700–X.799 |
| SECURITY | X.800–X.849 |
| OSI APPLICATIONS | X.850–X.899 |
| OPEN DISTRIBUTED PROCESSING | X.900–X.999 |
| INFORMATION AND NETWORK SECURITY | |
| General security aspects | X.1000–X.1029 |
| Network security | X.1030–X.1049 |
| Security management | X.1050–X.1069 |
| Telebiometrics | X.1080–X.1099 |
| SECURE APPLICATIONS AND SERVICES (1) | |
| Multicast security | X.1100–X.1109 |
| Home network security | X.1110–X.1119 |
| Mobile security | X.1120–X.1139 |
| **Web security** | **X.1140–X.1149** |
| Security protocols (1) | X.1150–X.1159 |
| Peer-to-peer security | X.1160–X.1169 |
| Networked ID security | X.1170–X.1179 |
| IPTV security | X.1180–X.1199 |
| CYBERSPACE SECURITY | |
| Cybersecurity | X.1200–X.1229 |
| Countering spam | X.1230–X.1249 |
| Identity management | X.1250–X.1279 |
| SECURE APPLICATIONS AND SERVICES (2) | |
| Emergency communications | X.1300–X.1309 |
| Ubiquitous sensor network security | X.1310–X.1319 |
| Smart grid security | X.1330–X.1339 |
| Certified mail | X.1340–X.1349 |
| Internet of things (IoT) security | X.1360–X.1369 |
| Intelligent transportation system (ITS) security | X.1370–X.1389 |
| Distributed ledger technology security | X.1400–X.1429 |
| Distributed ledger technology security | X.1430–X.1449 |
| Security protocols (2) | X.1450–X.1459 |
| CYBERSECURITY INFORMATION EXCHANGE | |
| Overview of cybersecurity | X.1500–X.1519 |
| Vulnerability/state exchange | X.1520–X.1539 |
| Event/incident/heuristics exchange | X.1540–X.1549 |
| Exchange of policies | X.1550–X.1559 |
| Heuristics and information request | X.1560–X.1569 |
| Identification and discovery | X.1570–X.1579 |
| Assured exchange | X.1580–X.1589 |
| CLOUD COMPUTING SECURITY | |
| Overview of cloud computing security | X.1600–X.1601 |
| Cloud computing security design | X.1602–X.1639 |
| Cloud computing security best practices and guidelines | X.1640–X.1659 |
| Cloud computing security implementation | X.1660–X.1679 |
| Other cloud computing security | X.1680–X.1699 |

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

# Recommendation ITU-T X.1147

## Security requirements and framework for big data analytics in mobile Internet services


### Summary

Mobile Internet services harvest data in their big data infrastructure from multiple sources and multiple data dimensions with characteristics including scale, diversity, speed and possibly others like credibility or business value. Big data analysis drives nearly every aspect of mobile Internet services to improve service quality and user experience. According to big data aggregation and analysis, service providers can analyse users' interests more effectively and predict user's expectation more accurately, thus, they can significantly improve and add value to their services. Consequently, big data analysis becomes a valuable business trend in the telecommunication domain.

As the new technology develops, big data analytics will bring new security issues comparing to previous data analytics in mobile Internet services domain. Without comprehensive security mechanism, the unsecure and spiteful big data analysis will do harm to mobile Internet service provider's business security, and user's data security. Consequently, in order to ensure secure big data analysis in mobile Internet services, the security requirements need to be analysed exhaustively and the overall security framework need to be established.

Recommendation ITU-T X.1147 will analyse the security requirements of big data analytics in mobile Internet services and provide security framework.



### History

| Edition | Recommendation | Approval | Study Group | Unique ID* |
|---|---|---|---|---|
| 1.0 | ITU-T X.1147 | 2018-11-13 | 17 | 11.1002/1000/13726 |

### Keywords

Big data analytics, mobile Internet services, security framework.


---

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

## FOREWORD

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

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

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

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

## NOTE

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

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

## INTELLECTUAL PROPERTY RIGHTS

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

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

## Table of Contents

# Recommendation ITU-T X.1147

## Security requirements and framework for big data analytics in mobile Internet services

### 1 Scope

This Recommendation provides a security framework and requirements for big data analytics in mobile Internet services. The intent of this Recommendation is to study the challenges brought forward by big data analytics, and the specific security requirements for mobile Internet services as well as the security framework. The scope of this Recommendation will focus on security threats analysis, security requirements and a security framework.

### 2 References

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

[ITU-T Y.3600] Recommendation ITU-T Y.3600 (2015), *Big data – Cloud computing based requirements and capabilities*.

[ISO/IEC DIS 11179-1] ISO/IEC 11179-1:2015, *Information technology – Metadata registries (MDR) – Part 1: Framework*.

[ISO/IEC DIS 19763-1] ISO/IEC 19763-1:2015, *Information technology – Metamodel framework for interoperability (MFI) – Part 1: Framework*.

### 3 Definitions

#### 3.1 Terms defined elsewhere

This Recommendation uses the following term defined elsewhere:

**3.1.1 mobile terminal** [b-ITU-T X.1121]: An entity that has wireless network access function and connects to a mobile network for data communication with application servers or other mobile terminals.

#### 3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

**3.2.1 smart device**: A mobile terminal which has the capabilities to access additional wireless networks (Bluetooth, Wi-Fi, Zigbee and near field communication (NFC)), a camera, microphone and is able to launch applications.

**3.2.2 mobile Internet service**: A set of functions provided by a mobile Internet provider to a client software or system.

### 4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

NFC Near Field Communication

OSI Open Systems Interconnection

RDBMS Relational Database Management System

## 5 Conventions

None.

## 6 Overview of big data analysis in mobile Internet services

Due to improvements in the computation and storage ability of smart devices and the enhanced transmission rate in telecommunication networks, as well as the advent of service platforms, the mobile Internet services are more popular and more widely used. Due to frequent interaction between the users, networks, multiple types of devices, and service providers, data is growing at an unprecedented rate for a broad range of mobile Internet services areas.

Generally, big data technologies provide two benefits, cost efficiency and new insights from the large data volumes.

– Cost efficiency: Big data technologies were designed to offer a fast and scalable data process, for example, the ‘click stream' analysis of user's activities. Web portal and more generally digital service providers have a large volume of log data. Traditionally, they create a database and data warehouse system in their data centres and perform analysis in the batch system using the relational database management system (RDBMS). But the management cost has always been very high and there is no way to extract new features from the data set. Therefore, many service providers have replaced or are in the process of replacing existing systems to the distributed file system and pre-processing unit (sub-system of big data). They can reduce the data management cost to half or less of what it used to be.

– Extract new insight: Big data technologies enabled the development of analytics technologies which move the analysis to a new degree from raw data to business insight. That solution now includes prediction to the extent of allowing the implementation of decision assisting systems. This is indeed very different from the conventional systems because the way the data processing logic handles the raw data, and the kinds of information that can be extracted from the data set are already known. The way big data technology was designed allows the delivery of analytics that, from the perspective of a human being, would equate to guessing the result. For example, in many implementations, the system helps the creation of "candidate answers" and tries to collect some evidence in order to prove that one answer is better than others.

Whilst for mobile Internet services, cost efficiency is the most important benefit, getting new business insight is equally, if not more, important for the next generation of mobile Internet services. As the data source is not fixed and will be diverse, the analysis system could be used by malicious users or attackers to achieve illegal or unethical purposes.

Mobile Internet services harvest data in their big data infrastructure from multiple sources and multiple data dimensions with characteristics including, scale (volume), diversity (variety), high speed (velocity) and possibly others like credibility (veracity) or business value. Big data analysis now drives nearly every aspect of mobile Internet services to improve service quality and user experience. According to big data aggregation and analysis, service providers can analyse users' interests more effectively and predict user's expectation more accurately, thus, they can significantly improve and add value to their services, for example:

– mobile search application to precisely target users' search intentions in a timely way;

– mobile financial application to customize users' financial solutions in a timely way;

– mobile application recommendation to improve success rates of recommendations in a timely way.

Consequently, big data analysis, as a new technology, becomes a valuable business trend in the telecommunication domain. Figure 1 shows big data analysis in mobile Internet services.

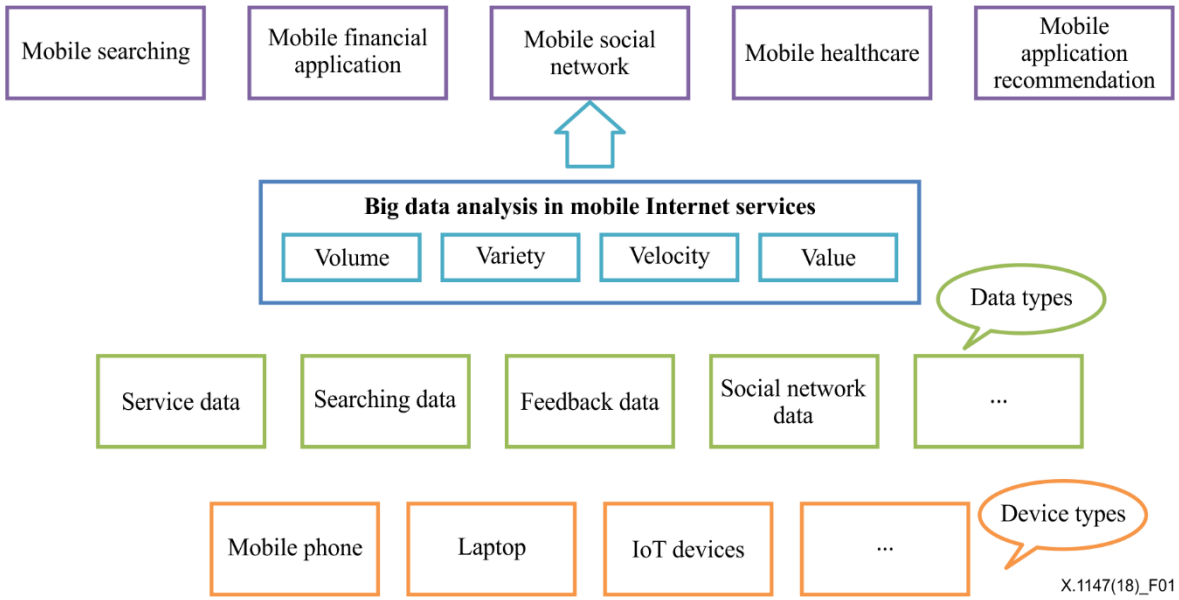


**Figure 1 – Big data analysis in mobile Internet services**

As a new technology, big data analysis in the mobile Internet services environment is different from general big data analysis. Details are given below:

a) Complicated data flow: The big data analysis processes may include data collection, data transaction, data analysis, data storage, and data application. A possible example of data flow is shown in Figure 2.

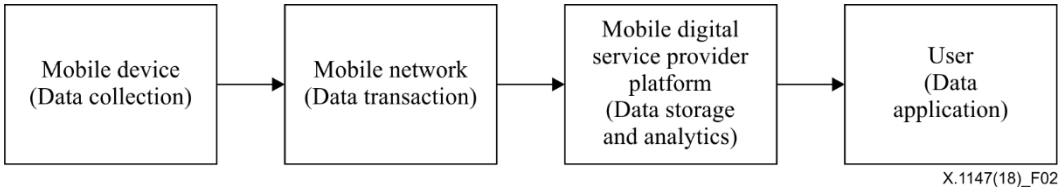


**Figure 2 – An example of data flow**

b) Asynchronous structure: The diagram in Figure 2 shows that not only is the data flow rich and complicated but the flow of data may also be asynchronous in nature and reaching near real time may be challenging.

Generally, big data analysis in mobile Internet services constitutes of the following entities:

a) The data collection entity, which collects data from smart devices.

b) The data pre-processing entity, which aggregates data, unifies the data collected in different formats, extracts data from unstructured data or semi-structured data into structured data.

c) The data analysis entity, which analyses the data of mobile Internet services in various data types and formats.

d) The data application entity, which applies the big data results for services.

## 7 Threats in mobile Internet big data analysis services

### 7.1 Analysis result overuse

This may occur when the data application entity uses the big data analysis beyond the intention of the original data analysis, or when the attackers illegally obtain the big data analysis result to develop business insights and mechanisms.

### 7.2 Data analysis without user's consent

This threat occurs when the data collection entity collect user's data and/or the data analysis entity analyze user related data without user's consent, including the scope, intention, method, result usage etc.

### 7.3 Data disclosure

Data disclosure occurs when the attackers impersonate a legal entity to disclose the original big data set and/or the result of big data analysis to the public. This may also occur when a legal entity (such as the data collection entity, data pre-processing entity, data analysis entity, data application entity) discloses the original big data set and/or the result of big data analysis by misuse.

### 7.4 Data forgery

The threat of data forgery occurs when a malicious mobile Internet user reports fake data to the data collection entity with certain propositions, e.g., identity-related information, location-related information, etc.

### 7.5 Disclosure information

During the big data analysis process, the attackers may impersonate a legal entity that has an opportunity to get any type of information, and in particular information relating to an identified or identifiable natural person.

### 7.6 Disclosure of inferred information

Prior to applying the result of big data analysis, if the data set of the analysis result is broader than its original analysis purpose, it may disclose the inferred information by subsequent analysis.

### 7.7 Disclosure of user behaviour information

The threat of disclosure of user behaviour information may occur when data analysis entity is tampered with or by the attackers impersonating a legal entity that has the opportunity to get user behaviour information (e.g., user's browsing preferences) for malicious purposes, such as reselling it for a profit.

### 7.8 Inaccurate or mistaken analysis

Inaccurate analysis may occur because of an inaccurate/unclear data source or analysis algorithm(s). Mistaken analysis occurs when the big data analysis services are attacked and tampered with. Also, it can happen in the case of logical design error of big data analysis services.

For unclear data sources, in particular data used in the mobile internet services whose source may not be recognized, it means that in the processing step of user data the proper privileges for those data are not identified.

### 7.9 Location information overuse

In the analysis process, the location information may be a key factor in predicting a user's expectations and requirements, but in some scenarios, the location information may not be the necessary element.

### 7.10 Over analysis

Over analysis may occur when the data analysis entity that analyses the big data sets gets more information than the intended original data analysis.

### 7.11 Trojan and viruses

These occur when a malicious mobile Internet user or attacker impersonates a legal user and injects Trojans or viruses into the data which will be collected by a mobile Internet service provider.

### 7.12 Unauthorized access

This threat occurs when an illegal entity (e.g., a data pre-processing entity, a data analysis entity) gains big data analyst results or even original data by masquerading as an authorized entity.

### 7.13 Unauthorized analysis

Unauthorized analysis occurs when an un-authorized entity analyses the big data from mobile Internet services by masquerading as an authorized entity.

### 7.14 Unauthorized analytical application

This may occur when tampered data analysis entity/data application entity or the attackers impersonate a legal entity to use the analytical result to develop business insights and mechanisms including prediction and decision assistance.

## 8 Relationship of security threats to entities

Security threats appear in particular places of the entities of big data analysis in mobile Internet services. The relationship of security threats and entities of big data analysis in mobile Internet services are shown in Table 1.

In Table 1, the letter "Y" (Yes) in each cell indicates that the entity is related to a particular security threat.

**Table 1 – Relationship of security threats to entities**

| Entities / Threats | The data collection entity | The data pre-processing entity | The data analysis entity | The data application entity |
|---|---|---|---|---|
| Analysis result overuse | | | | Y |
| Data analysis without user's consent | Y | | Y | |
| Data disclosure | Y | Y | Y | Y |
| Data forgery | Y | | | |
| Disclosure of information | Y | Y | Y | Y |
| Disclosure of inferred information | | | Y | |
| Disclosure of user's behaviour information | | | Y | |
| Inaccurate or mistaken analysis | | | Y | |
| Location information overuse | | | Y | Y |
| Over analysis | | | Y | |
| Trojan and viruses | Y | | | |
| Unauthorized access | Y | Y | Y | Y |
| Unauthorized analysis | | | Y | |
| Unauthorized analytical application | | | Y | Y |

# 9 Security requirements

## 9.1 Analysis algorithm(s) check

The accuracy and integrity of the analysis algorithm(s) is required to be checked.

## 9.2 Authentication

Authentication is required to confirm the identities of the entities. Authentication ensures the validity of the claimed identities of the entities participating in big data analysis and provides assurance that an entity is not attempting to masquerade as an authorized entity. Authentication techniques may be required as part of the authorization process, and can be augmented by single sign on capabilities.

## 9.3 Authorization

Authorization capabilities are required to ensure that only authorized users or entities are allowed to access the original data or the results of big data analysis.

## 9.4 Data minimization

The categories of data that are subject to collection are required to be strictly limited to those that are necessary to fulfil the stated purpose of use of the system. This purpose of use must be disclosed to the user in the course of obtaining consent.

### 9.5 Data retention limits

Stored data, including outputs of big data analysis, are required to be subject to clearly defined retention periods that include maximum limits. These periods must be set according to the purpose of use. The data retention period should be disclosed to users in the course of obtaining consent.

### 9.6 Data source check

The data source is required to be identified, to ensure that the data analysis entity has the proper privilege to analyse it.

### 9.7 Incident response for malware

Incident response process for malware detection is required to pre-deploy security mechanisms in response to and to deal with an attack in a timely manner.

### 9.8 Information protection

The security mechanisms should be deployed to protect and to prevent un-authorized access and disclosure of information and, in particular, any information relating to an identified or identifiable natural person.

### 9.9 Resistance to fake data

Resistance to fake data is required to ensure data authenticity and to ensure that data provenance is consistent with the smart device.

### 9.10 Secure data acquisition

Secure data acquisition is required to ensure secure data collection from a variety of smart devices and data transmission in mobile networks from eavesdropping, man-in-middle attacks, and data tampering, etc. These security measures should extend to data handled and stored at pre-processing stages, if applicable.

### 9.11 Secure audit

Secure audit is required to audit the entity's behaviour when analysing and using big data in mobile Internet services. Secure audit collects and makes available the necessary evidential information related to the analysis and use of any big data set/analysis results in mobile Internet services.

### 9.12 Secure data storage

Secure data storage is required to ensure the secure aggregation and storage of multiple-structure data from different smart devices and mobile applications.

### 9.13 User consent

User consent to the use of related data in big data analysis is required to be obtained from the user of mobile Internet services. The key point is that certain mobile Internet services that need to collect user data should inform, remind, display and briefly explain to the users that data may be collected and used for big data analysis, and obtain their consent in this regard.

## 10 Relationship between security requirements and security threats

Each security requirement is a countermeasure against certain security threats. The relationship between security requirements and security threats is shown in Table 2.

In Table 2, the letter "Y" (Yes) in each cell indicates that the security requirement is related to a particular security threat.

## Table 2 – Relationship between security requirements and security threats

| Requirements / Threats | Algorithm(s) check | Authentication | Authorization | Data minimization | Data retention limits | Data source check | Incident response for malware | Information protection | Resistance to fake data | Secure audit | Secure data acquisition | Secure data storage | User consent |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Analysis result overuse | | | | | | | | | | Y | | | |
| Data analysis without user's consent | | | | Y | | | | | | | | | Y |
| Data disclosure | | Y | Y | Y | Y | | | | | | | | |
| Data forgery | | Y | Y | | | | | | Y | | | | |
| Disclosure of information | | Y | Y | Y | Y | | | Y | | | | | |
| Disclosure of inferred information | | Y | Y | Y | Y | | | | | | | | |
| Disclosure of user's behaviour information | | Y | Y | | Y | | | | | | | | |
| Inaccurate or mistaken analysis | Y | | | | | Y | Y | | | | | | |
| Location information overuse | | | | Y | | | | | | | | | Y |
| Over analysis | | | | | | | | | | Y | | | |
| Trojan and viruses | | | | | | | Y | | | | | Y | |
| Unauthorized access | | Y | Y | | | | | | | | | | |
| Unauthorized analysis | | Y | Y | | | | | | | | | | |
| Unauthorized analytical application | | | | | | | | | | Y | | | |

## 11 Security functions for big data analytics in mobile Internet services

This clause describes some of the security functions that may be used to meet security requirements for big data analytics in mobile Internet services. They are:

– authentication;
– authorization;
– digital signature;
– encipherment;
– event detection;
– key exchange;
– security audit trail;
– security recovery; and
– user reminder.

### 11.1 Authorization

The authorization function may use the authenticated identity of a user or information about the user (such as membership within a known set of users) or the capabilities of the user, in order to determine and enforce the access rights of the user. If the user attempts to use an unauthorized resource or an authorized resource with an improper type of access, then the access control function will reject the attempt and may additionally report the incident for the purposes of generating an alarm or recording it as part of a security audit trail.

The access control function may be based on the use of the following items:

a) access control information bases, where the access rights of peer entities are maintained in a database;
b) authentication information, such as passwords, the possession and subsequent presentation of which is evidence of the accessing user's authorization;
c) capabilities, the possession and subsequent presentation of which is evidence of the access right to the user or resource defined by the capability;
d) security labels, which, when associated with a user, may be used to grant or deny access, usually according to a security policy;
e) time of attempted access;
f) route of attempted access;
g) duration of access; and
h) physical location of attempted access.

The access control function may be applied to the data analysis entity and the data application entity.

### 11.2 Authentication

Some of the security technologies that may be applied include the following:

– the use of authentication information, such as passwords supplied by a sending user and checked by the receiving user;
– cryptographic technologies; and
– the use of characteristics or possessions of the user and single sign on.

The authentication function may be incorporated in order to provide communicating user authentication. If the function fails in authenticating the user, this will result in the rejection or

termination of the connection and may cause a user to show up on the security audit trail and/or a report to a security management centre.

When cryptographic techniques are used, they may be combined with "handshaking" protocols to protect against replay (i.e., to ensure liveness).

The choices of security technologies, which are used to realize authentication, will depend upon the circumstances in which they need to be used for example:

– time stamping and synchronized clocks;
– two- and three-way handshakes (for unilateral and mutual authentication respectively); and
– non-repudiation functions achieved by digital signature or notarization mechanisms.

### 11.3 Digital signature

The digital signature function defines the following two processes:

– signing data; and
– verifying the signed data.

The first process uses information that is private (i.e., unique and confidential) to the signatory. The second process uses procedures and information which are publicly available but from which the signatory's private information cannot be deduced.

The signing process involves either an encipherment of the data or the production of a cryptographic check value of the data, using the signatory's private information as a private key.

The verification process involves the use of public procedures and information to determine whether the signature was produced correctly with the signatory's private information.

The essential characteristic of the signature function is the fact that the signature can only be produced using the signatory's private information. Thus, when the signature is verified, it can subsequently be proven to a third party (e.g., a judge or arbitrator) at any time that only the unique holder of the private information could have produced the signature.

Due to the diversity of the applications and the services explored in mobile Internet services, the digital signature algorithms may be different when this function is implemented.

### 11.4 Encipherment

The encipherment function can ensure the confidentiality of either communication data or stored data. Encipherment algorithms may be reversible or irreversible. There are two general classifications of reversible encipherment algorithms:

a) symmetric (i.e., secret key) encipherment, in which knowledge of the encipherment key implies knowledge of the decipherment key and vice versa; and
b) asymmetric (e.g., public key) encipherment, in which knowledge of the encipherment key does not imply knowledge of the decipherment key, or vice versa. The two keys of such a system are sometimes referred to as the "public key" and the "private key".

Irreversible encipherment algorithms may or may not use a key. When they use a key, this key may be public or secret. In the big data analysis in mobile Internet services scenarios, the choice of encipherment algorithms may be flexible.

### 11.5 Event detection

Security-relevant event detection includes the detection of apparent violations of security and may also include detection of "normal" events, such as a successful access (or log on). Security-relevant events may be detected by entities within open systems interconnection (OSI) including security

mechanisms. The specification of what constitutes an event is maintained by event handling management. Detection of various security-relevant events may, for example, cause one or more of the following actions:

a) local reporting of the event;

b) remote reporting of the event;

c) logging of the event; and

d) recovery action.

Examples of such security-relevant events are:

a) a specific security violation;

b) a specific selected event; and

c) an overflow on a count of the number of occurrences.

Standardization in this field will take into consideration the transmission of relevant information for event reporting and event logging and the syntactic and semantic definition to be used for the transmission of event reporting and event logging.

The event detection function could help to detect the security violations of the big data analysis and usage among the data pre-processing entity, data collection entity, the data analysis entity and the data application entity.

### 11.6 Key exchange

The key exchange function allows for key sharing in encipherment implementations, especially that of the symmetric encipherment algorithm.

### 11.7 Security audit trail

Security audit trails provide a valuable security mechanism as potentially they permit detection and investigation of breaches of security by permitting a subsequent security audit. A security audit is an independent review and examination of system records and activities in order to test for adequacy of system controls, to ensure compliance with established policy and operational procedures, to aid in damage assessment and to recommend any indicated changes in controls, policy and procedures. A security audit requires the recording of security-relevant information in a security audit trail and the analysis and reporting of information from the security audit trail. As logging or recording is considered to be a security mechanism it is described in this clause. The analysis and report generation is considered a security management function.

Collection of security audit trail information may be adapted to various requirements by specifying the kind of security-relevant events to be recorded (e.g., apparent security violations or completion of successful operations).

The known existence of a security audit trail may serve as a deterrent to some potential sources of security attacks.

OSI security audit trail considerations consider what information shall optionally be logged, under what conditions that information shall be logged and the syntactic and semantic definition to be used for the interchange of the security audit trail information.

This function could be used to audit the behaviour of the entities when analysing and using big data set/analysis results in mobile Internet services.

### 11.8 Security recovery

Security recovery deals with requests from mechanisms such as event handling and management functions and takes recovery actions as the result of applying a set of rules. These recovery actions may be of three kinds:

– immediate, where the system should be recovered as soon as possible, commonly within one day;

– temporary, where the system needs to be recovered within a few days, such as a week;

– long term, where it would take a relatively longer time to recover the system, for example, one month.

The security recovery function could be used for recovery of the mobile Internet service provider's assets such as system, software, hardware etc., when they are attacked by an attacker or malicious user.

### 11.9 User reminder

User reminder provides a mechanism to guarantee that the data collected from the mobile Internet service usage will be used in the big data analysis has been authorized by the mobile Internet services user.

The key point is that for a certain mobile Internet service that needs to collect user data, the service is to send a reminder to the user, to display it, and to briefly explain it to the user.

The user can be reminded whether data collection is planned and what data will be collected. They will also be informed how the data will be processed and handled.

### 11.10 Relationship between security functions and security requirements

The security functions listed and described in clause 9 are used to satisfy some of the security requirements. The mapping of security functions to security requirements is shown in Table 3.

In Table 3, the symbol "√" in each cell indicates that the security requirement is related to a particular security function. More precisely, the marked security requirement should be supported by the implementation of the marked function.

**Table 3 – Illustration of relationship between security requirements and security functions**

| Functions / Requirements | Autho-rization | Authen-tication | Digital signature | Encipher-ment | Event detection | Key exchange | Security audit trail | Security recovery | User reminder |
|---|---|---|---|---|---|---|---|---|---|
| Algorithm(s) check | | | | | √ | | | | |
| Authentication | | √ | √ | √ | | √ | | | |
| Authorization | √ | √ | | | | | | | |
| Data minimization | | | | | | | | | √ |
| Data retention limits | | | | | | | | | √ |
| Data source check | √ | | | | √ | | | | |

**Table 3 – Illustration of relationship between security requirements and security functions**

| Functions / Requirements | Autho-rization | Authen-tication | Digital signature | Encipher-ment | Event detection | Key exchange | Security audit trail | Security recovery | User reminder |
|---|---|---|---|---|---|---|---|---|---|
| Incident response for malware | | | | | √ | | | √ | |
| Information protection | √ | √ | √ | √ | | √ | | | |
| Resistance to fake data | | | √ | √ | | √ | | | |
| Secure audit | | | | | | | √ | | |
| Secure data acquisition | | | √ | √ | | √ | | | |
| Secure data storage | | | | √ | | √ | | | |
| User consent | | | | | | | | | √ |

# Bibliography


[b-ITU-T X.800] Recommendation ITU-T X.800 (1991), *Security Architecture for Open Systems Interconnection for CCITT applications*.

[b-ITU-T X.1121] Recommendation ITU-T X.1121 (2004), *Framework of security technologies for mobile end-to-end data communications*.

## SERIES OF ITU-T RECOMMENDATIONS

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

Printed in Switzerland
Geneva, 2019