ITUPublications
Recommendations

International Telecommunication Union
Standardization Sector

Recommendation

ITU-T X.1454 (09/2023)

SERIES X: Data networks, open system communications and security

Secure applications and services (2) – Application Security (2)

Security measures for location-enabled smart office services

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	X.1000-X.1099
SECURE APPLICATIONS AND SERVICES (1)	X.1100-X.1199
CYBERSPACE SECURITY	X.1200-X.1299
SECURE APPLICATIONS AND SERVICES (2)	X.1300-X.1499
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.1350-X.1369
Intelligent transportation system (ITS) security	X.1370-X.1399
Distributed ledger technology (DLT) security	X.1400-X.1429
Application Security (2)	**X.1450-X.1459**
Web security (2)	X.1470-X.1489
CYBERSECURITY INFORMATION EXCHANGE	X.1500-X.1599
CLOUD COMPUTING SECURITY	X.1600-X.1699
QUANTUM COMMUNICATION	X.1700-X.1729
DATA SECURITY	X.1750-X.1799
IMT-2020 SECURITY	X.1800-X.1819

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

Recommendation ITU-T X.1454

Security measures for location-enabled smart office services

Summary

Smart office services combining multiple smart applications aim to improve the quality of office-based businesses and enhance efficiency management. Since information and communication technologies (ICTs) serve as the basis for technologies in smart office services, the telecommunication operator plays an important role among the stakeholders in smart office services.

Typical smart office services include smart parking, smart driving, smart retail shop, smart office, smart meeting room management, smart water and smart energy consumption management. Among these typical smart office services, the location data provided by the operator is one of the key elements in most smart office service implementations.

In order to ensure the security of location-enabled smart office services, security threats and relevant security requirements specific to location-enabled services need to be analysed and the overall security measures established.

Recommendation ITU-T X.1454 analyses the typical application scenarios of location-enabled smart office services, specifies their security threats and requirements and establishes security measures for the operator and key stakeholders in a smart office to safeguard location-enabled services.

History *

Edition	Recommendation	Approval	Study Group	Unique ID
1.0	ITU-T X.1454	2023-09-08	17	11.1002/1000/15111

Keywords

Location, security measures, smart office services.

* To access the Recommendation, type the URL https://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID.

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/software copyrights, 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 appropriate ITU-T databases available via the ITU-T website at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Recommendation ITU-T X.1454

Security measures for location-enabled smart office services

1 Scope

This Recommendation analyses the typical application scenarios of location-enabled smart office services, specifies the security threats and requirements specific to the location-enabled services and thereby establishes the security measures for the operator and key stakeholders in a smart office to safeguard the location-enabled services.

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.

None.

3 Definitions

3.1 Terms defined elsewhere

None.

3.2 Terms defined in this Recommendation

This Recommendation defines the following term:

3.2.1 smart office service: A service combining multiple smart applications (e.g., smart parking, smart water, smart retail store) that aims to serve and support the work of an office-based business, improve its quality and the efficiency of its management and create a office environment suitable for people.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

DDoS Distributed Denial of Service

GNSS Global Navigation Satellite System

ICT Information and Communication Technology

RNSS Radio Navigation Satellite System

SEM Smart Environmental Monitoring

UWB Ultrawideband

Wi-Fi Wireless Fidelity

5 Conventions

The keywords "is required to" indicate a requirement which must be strictly followed and from which no deviation is permitted if conformance to this document is to be claimed.

6 Overview of location-enabled smart office services

According to the vision of smart sustainable cities, which uses information and communication technologies (ICTs) and other means to improve quality of life, the efficiency of urban operation and services, and competitiveness, the smart office service becomes a typical application in a smart sustainable city.

The smart office service combining multiple smart applications (e.g., smart parking, smart water, smart retail store) aims to improve the quality of an office-based business' offerings and the efficiency of its management.

As smart office services combine multiple smart applications, the key stakeholders are diverse. Since ICTs serve as the basis for technologies in smart office services, among typical smart office services, the location data provided by the operator is one of the key elements in most of the implementation of these services.

The main key stakeholders in location-enabled smart office systems are:

– The smart office service provider;

– The data and computation provider;

– The sensing and infrastructure provider;

– The user.

NOTE – These key stakeholders, the smart office service provider, data and computation provider, and sensing and infrastructure provider in location-enabled smart office systems could be separated providers or a provider of integrated services.

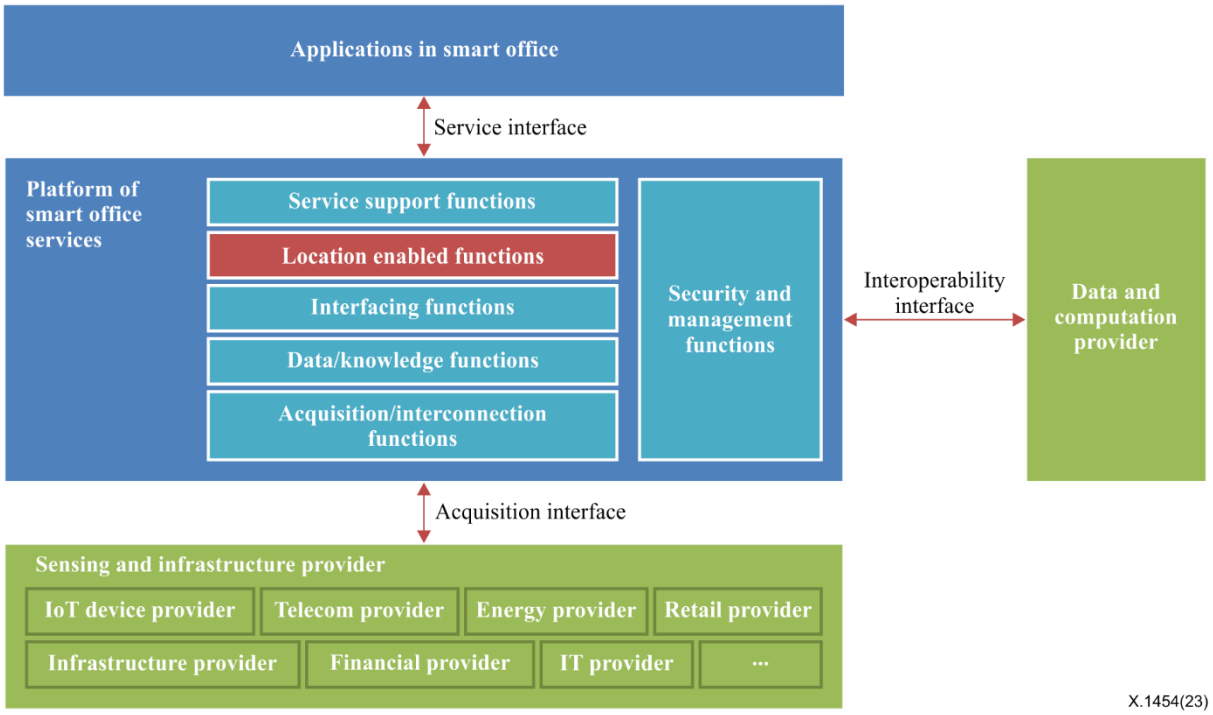

Figure 1 – Overview of a location-enabled smart office system

The location-enabled smart office system provides the following functions:

– **Acquisition/interconnection functions:** These provide data capture mechanisms from different sources of data collection systems.

– **Data / knowledge functions:** These support data processing, adding value and transforming information into knowledge.

– **Interfacing functions:** These enable access to information at different levels.

– **Location-enabled functions:** These provide location data from the operator's system.

– **Service support functions:** These coordinate all the possible services involved in each action provide support to interoperability functions.

– **Security and management functions:** These provide horizontal functionalities such as audits, monitoring and security.

The interfaces enable the communication between the functions:

– **Acquisition interface:** This interface enables information collection from the external elements.

– **Interoperability interface:** This interface enables communication with external data providers and the third-party computation systems.

– **Service interface:** This interface enables application-to-application access to support functions provided by the platform of smart office services.

7 Typical application scenarios of location-enabled smart office services

7.1 Smart parking

Smart parking brings an efficient integration of parking resources in an office parking and coordinates parking facilities together with other systems (e.g., external payment system, WEB / app-parking system).

Smart parking may include typical functions such as parking guidance, parking space reservation, vehicle reverse search, vehicle automatic access control and self-service payment. The location-enabled smart parking functions are as follows:

– **Parking guidance:** The location information of unoccupied parking spaces supports the publication of parking guidance information.

– **Parking space reservation:** The location information can help in searching for information about available parking spaces and in reserving parking spaces in advance.

– **Vehicle reverse search:** The location information could help vehicle users identify where their vehicles are parked in case they forget where they have left them.

7.2 Smart environmental monitoring

As a self-monitoring and self-protecting environmental monitoring application, smart environmental monitoring (SEM) can be aware of the current environmental status.

SEM may include functional entities of SEM platforms, SEM devices and the network. The location-enabled smart environment monitoring functions are as follows:

– **Measurement setting management:** the location of a device is the necessary information for the measurement settings along with environmental factors.

– **Data presentation:** raw data at each given location (of one or more SEM devices) is the optional information for the environmental quality presentation.

7.3 Smart delivery

Smart delivery takes advantage of the driverless vehicle and robot application in a smart office scenario, and can deliver packages, files, office supplies, etc. automatically.

The location-enabled smart delivery functions are as follows:

– Assist the auto-drive by offering the positioning capability to centimetre-level accuracy.

– Enhance the efficiency of vehicle/robot dispatch by mapping the delivery order with the device's location.

– Optimize the delivery routeing and monitor the delivery process by tracking the vehicle/robot's real time location and trail.

8 Security threats to location-enabled smart office service

8.1 Security threats to data

8.1.1 Location data eavesdropping

The location data in smart office services may be based on the open wireless network; an attacker may eavesdrop on the location data by monitoring the wireless channel.

8.1.2 Location data tampering

An attacker may capture the data pack within the location data transmitted from the network, and maliciously modify/forge the location data to launch further attacks. In some scenarios, the modified/forged location data may cause safety issues, e.g., smart parking, smart driving and emergency rescue.

8.1.3 Intercept location data report

An attacker may capture or tamper with IoT devices by refusing to report the IoT devices' location data to the network or the smart office service platform.

8.1.4 Unauthorized location data invocation

Without the authentication mechanism between the applications and the smart office service platform, the location data may unauthorizedly be invoked by the attacker.

8.1.5 Unavailable data

The non-unified data format may lead to the application being unavailable in a smart office; for example, the non-unified indoor location data format (including the data related to the floor, room, desk), may confuse the robot when it is delivering the package to the recipient.

8.1.6 Disclosure of behaviour information

This threat may occur when a smart office platform is tampered with or when an attacker impersonates a legal entity with an opportunity to obtain users' behaviour information (e.g., route planning preferences) for malicious purposes, such as reselling it at a profit.

8.1.7 Positioning without user consent

This threat occurs when the location function entity collects the user's location data and analyses the related data without the user's consent, including in terms of the scope, intention, method, result and usage.

8.2 Security threats to the device

8.2.1 Vulnerability of hardware and software

It is possible to introduce security vulnerabilities and threats to the process of positioning device development. For instance, ports for debugging may not be protected properly, weak encryption algorithms may be used, and there may be a failure to apply hardware and software updates and a lack of a timely integrity check.

8.2.2 Positioning device manipulation

An attacker may manipulate a positioning device by tampering with the systems of the sensing and infrastructure, leading to an inaccurate positioning result.

8.3 Security threats to the interfaces

8.3.1 Acquisition interface

The interface between the sensing and infrastructure provider and the platform of smart office services is vulnerable to the following threats:

– **Sniff data:** Without authentication and authorization mechanisms between the smart office service platform and the sensing and infrastructure provider, an attacker may impersonate the smart office service platform to collect sensing and infrastructure data.

– **Denial of service:** An attacker may launch distributed denial of service (DDoS) attacks by modifying the data collect policy (e.g., frequently collecting the sensing and infrastructure data in a very short time).

– **Information leakage:** The mobile devices periodically send service data, especially location data, via acquisition interface to a platform of smart office services; an attacker may notice a user's daily routine if they can sniff the service and location data.

8.3.2 Interoperability interface

The interface between the smart office service platform and the data/computation provider is vulnerable to the following threats:

– **Unauthorized data access:** Without authentication and authorization mechanisms between the smart office service platform and data/computation provider, the interoperability interface may be tampered with by the attacker to access the service data, location data and profile data.

– **Falsifying data:** Without authentication and authorization mechanisms between the smart office service platform and data/computation provider, the interoperability interface may be tampered with by the attacker to falsify the service data, location data and profile data; this threat could result in information leakage, incorrect platform running and incorrect billing of the data/computation provider.

8.3.3 Service interface

The interface between the smart office service platform and the applications in the smart office are vulnerable to the following threats:

– **Unauthorized data access:** Without authentication and authorization mechanisms between the smart office service platform and applications in the smart office, the service interface may be tampered with by an attacker to access the service data, location data and profile data.

– **Falsifying data:** Without authentication and authorization mechanisms between the smart office service platform and applications in the smart office, the service interface may be tampered with by the attacker to falsify the service data, location data and profile data; this threat could result in incorrect billing of customers.

8.4 Security threats to the platform

8.4.1 Vulnerability of hybrid localization technologies

Location function as one of the basic function entities in the platform layer may need to aggregate hybrid localization technologies which are based on the multiple wireless systems, such as GNSS, RNSS, Bluetooth, Wi-Fi, cellular network and ultrawideband (UWB). The implementation of these hybrid localization technologies involves information extraction, positioning calculation and filtering the vulnerability of the aggregation process, and the algorithm may produce an inaccurate positioning result.

8.4.2 Capability exposure

A smart office platform exposes the location and other service capabilities to the smart applications; an unauthorized entity may insert, change or delete the capability usage privilege. The unauthorized entity could be a person, a program or a device. These attacks occur when an attacker adds data to an existing connection with service capability usage by hijacking the connection or maliciously sending configuration data. This can result in a denial-of-service attack and allow access to the service data.

8.5 Security threats to the smart application

8.5.1 Unauthorized usage

This threat occurs when an unauthorized smart application gains service capabilities offered by a smart office platform by masquerading as an authorized entity.

8.5.2 Trojan horse and virus injection

These occur when an attacker impersonates a legal smart application and injects a Trojan horse or a virus into the smart application; this will harm and even launch further attacks on the smart office platform.

8.6 Relationship of security threats to key stakeholders

The relationship between security threats and key stakeholders of location-enabled smart office services are shown in Table 1.

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

Table 1 – Relationship of security threats to entities

The key stakeholder / **Threats**	**The smart office service provider**	**The data and computation provider**	**The sensing and infrastructure provider**	**The user**
Location data eavesdropping	Y		Y	Y
Location data tampering	Y		Y	Y
Intercept location data report	Y		Y	Y
Unauthorized location data invocation	Y		Y	Y
Data unavailable	Y	Y		

Table 1 – Relationship of security threats to entities

Threats \ The key stakeholder	The smart office service provider	The data and computation provider	The sensing and infrastructure provider	The user
Disclosure of behaviour information	Y	Y	Y	Y
Positioning without the user's consent	Y		Y	Y
Sniff data	Y		Y	Y
Denial of service	Y		Y	
Information leakage	Y		Y	Y
Unauthorized data access	Y	Y	Y	Y
Falsifying data	Y	Y	Y	Y
Vulnerability of hybrid localization technologies			Y	
Capability exposure	Y			
Vulnerability of hardware and software			Y	
Positioning device manipulation			Y	
Unauthorized usage	Y			
Trojan horse and virus injection	Y			

9 Security requirements of location-enabled smart office service

9.1 Security requirements for the data

– R-01: It is required that the smart office service provider, the data and computation provider, and the sensing and infrastructure provider provide a functionality to ensure the confidentiality of data, especially location data.

– R-02: It is required that the smart office service provider, the data and computation provider, and the sensing and infrastructure provider provide a functionality to ensure the integrity of data, especially location data.

– R-03: It is required that the smart office service provider, the data and computation provider, and the sensing and infrastructure provider ensure that only authorized users or devices are allowed access to data, especially to location data.

– R-04: It is required that the smart office service provider, the data and computation provider, and the sensing and infrastructure provider confirm the identities of entities and prevent attackers attempting to masquerade as an authorized entity.

– R-05: It is required that the smart office service provider provide a functionality to ensure that only authorized devices or applications are allowed to access the office environment.

– R-06: It is required that the smart office service provider, the data and computation provider, and the sensing and infrastructure provider establish a collaboration mechanism to unify the format of the data.

– R-07: It is required that the smart office service provider, the data and computation provider, and the sensing and infrastructure provider be authorized by the user's consent to collect users' personal data, especially location data. The user's consent includes consent to reminders, display and briefly explaining the users' personal data collection to the user.

As for the data of a location-enabled smart office service, security requirements deriving from the corresponding security threats are shown in Table 2.

Table 2 – Security requirements of the data mapping to the security threats

Security threats	Security requirements
Location data eavesdropping	R-01, R-02, R-03, R-04
Location data tampering	R-03, R-04
Intercept location data report	R-03, R-04
Unauthorized location data invocation	R-03, R-04, R-05
Unavailable data	R-06
Disclosure of behaviour information	R-01, R-03, R-04
Positioning without user's consent	R-07

9.2 Security requirements for the device

– R-08: It is required that the smart office service provider, the data and computation provider, and the sensing and infrastructure provider provide an incident response process for malware detection, pre-deploy security mechanisms in response to an attack and deal with an attack in time.

– R-09: It is required that the sensing and infrastructure provider ensure an attacker cannot access data even if the hardware is captured, which includes by means of the following:

  • Verifying the authenticity and integrity of software on a device using cryptographically generated digital signatures [b-ISO/IEC 9796-3];

  • Controlling traffic that is destined to terminate at a device by a firewall, intrusion detection and intrusion protection.

– R-10: It is required that the smart office service provider, the data and computation provider, and the sensing and infrastructure provider use appropriate encryption algorithms to ensure the confidentiality of data, especially of location data.

– R-11: It is required that the sensing and infrastructure provider provide a functionality to confirm the identities of entities and prevent any attacker attempting to masquerade as an authorized entity.

As for a device of a location-enabled smart office service, security requirements deriving from the corresponding security threats are shown in Table 3.

Table 3 – Security requirements of the device mapping to the security threats

Security threats	Security requirements
Vulnerability of hardware and software	R-08, R-09, R-10
Positioning device manipulation	R-09, R-11,

9.3 Security requirements for interfaces

– R-12: It is required that the smart office service provider and the sensing and infrastructure provider provide a functionality to ensure that only authorized users or devices are allowed access to sensing and infrastructure data through the interfaces.

– R-13: It is required to provide a functionality by the smart office service provider and the sensing and infrastructure provider to confirm the identities of entities and prevent any attacker attempting to masquerade as an authorized entity.

– R-14: It is required that the smart office service provider and the sensing and infrastructure provider provide a functionality to ensure data especially the location data confidentiality.

– R-15: It is required that the smart office service provider and the data and computation provider provide a functionality to ensure that only authorized users are allowed access to service data, location data and profile data.

– R-16: It is required that the smart office service provider and the data and computation provider provide a functionality provider to confirm the identities of entities and prevent any attacker attempting to masquerade as an authorized entity.

– R-17: It is required that the smart office service provider and the data and computation provider provide a functionality to ensure service data, location data and profile data integrity.

As for the interface of location-enabled smart office service, security requirements deriving from the corresponding security threats are shown in Table 4.

Table 4 – Security requirements of the interfaces mapping to the security threats

Security threats	Security requirements
Sniff data	R-12, R-13
Denial of service	R-13
Information leakage	R-13, R-14
Unauthorized data access	R-15, R-16
Falsifying data	R-17

9.4 Security requirements for the platform

– R-18: It is required that the sensing and infrastructure provider provide a functionality to check the accuracy and integrity of the hybrid localization algorithm(s).

– R-19: It is required that the smart office service provider provide a functionality to ensure that only authorized devices or applications are allowed to access the location-enabled smart office service.

– R-20: It is required that the smart office service provider provide a functionality to confirm the identities of entities and prevent any attacker attempting to masquerade as an authorized entity.

As for the platform of location-enabled smart office service, security requirements deriving from the corresponding security threats are shown in Table 5.

Table 5 – Security requirements of the platform mapping to the security threats

Security threats	Security requirements
Vulnerability of hybrid localization technologies	R-18
Capability exposure	R-19, R-20

9.5 Security requirements for the smart application

– R-21: It is required that the smart office service provider provide a functionality to ensure that only authorized users or devices are allowed access to data, especially location data.

– R-22: It is required that the smart office service provider provide a functionality to ensure that only authorized devices or applications are allowed to access the smart office service.

– R-23: It is required to provide a functionality by the smart office service provider to ensure that only authorized users or devices are allowed access to the location-enabled smart office service.

– R-24: It is required that the smart office service provider provide a functionality to provide an incident response process for malware detection, to pre-deploy security mechanisms in response to and to deal with an attack in time.

As for the smart application of a location-enabled smart office service, security requirements deriving from the corresponding security threats are shown in Table 6.

Table 6 – Security requirements of the smart application mapping to the security threats

Security threats	Security requirements
Unauthorized usage	R-21, R-22
Trojan horse and virus injection	R-23, R-24

10 Security functions

To fulfil the security requirements for the location-enabled smart office service, there are several security functions that include but are not limited to the following:

– Data encryption and key management;

– Identity management and access control;

– Integrity verification;

– Security monitoring and security event response;

– User reminder.

10.1 Data encryption and key management

Encryption and key management are the key mechanisms to protect data confidentiality in smart office services. Encryption supplies a resource protection approach, while key management supplies cryptographic key control.

The encryption shall follow the relevant industrial and government standards. It includes but is not limited to the following elements:

– Encryption of dynamic data in service processes;

– Encryption of static data in the database;

– Encryption of data in the backup file.

Key management comprises the generation, distribution, sharing, rekeying and revocation of cryptographic keys for data confidentiality and authentication. The management forms the foundation of service security, which includes but is not limited to the following:

– **Key information protection:** Key information shall be protected as sensitive data and its security level shall be set higher than others.

– **Backup and recovery:** As a potential incident may cause the loss of a specific key and stop a service, it is essential to set the backup and recovery solution of a key.

10.2 Identity management and access control

Identity management should be provided for the entities of the smart office service, which can supply the raw data for access control, authorization and audit.

– It supports the whole life cycle management of identity, such as register, role and permission assignment, permission modification and deleting. Furthermore, the identity registration and modification should have an approval procedure for an administrator.

– It supports entity password management, which includes the set of entity password policies based on the client security policy, such as cryptographic algorithms, the length of a password, the complexity of a password and the cycle of password updating. It could support various types of passwords, such as graphical passwords, sound-based passwords and so on. Furthermore, it also supports the functions of password synchronization and password reset.

– Identity management should include an identity account naming policy and identity account application policy.

Access control should be provided to manage entity access to the smart office service, which uses the authenticated identity of an entity or capability of an entity to determine and enforce the entity access privilege. Access control can reject unauthorized or improper access attempts and report them to generate an alarm or perform a security audit trail.

– Authentication data, such as password, possession and subsequent presentation, as the evidence of entity access authorization;

– Security label, produced according to office security policy;

– Time of attempted access;

– Route of attempted access;

– Duration of access;

– Physical location of attempted access.

10.3 Integrity verification

Data integrity verification has two levels:

– **Single data unit or field level:** The verification of a single data unit level comprises two processes: one at the sending entity and one at the receiving entity. The sending entity appends to data a quantity that is a function of the data itself. The receiving entity generates a corresponding quantity and compares its result with the received quantity to determine whether the data have been modified in transmission.

– **Stream of data units or fields level:** The verification of the stream of the data unit level requests the addition of some form of explicit ordering, e.g., sequence number, time stamp or cryptographic chain.

Data integrity verification using a pre-deploy mechanism to verify the data format and a cryptographically generated digital signature mechanism to verify the untampered data.

10.4 Software and algorithm(s) integrity verification using cryptographically generated digital signatures mechanism – Security monitoring and security event response

Security monitoring could be provided to service administrators for inspecting service faults and performance. The monitoring includes but is not limited to the following:

– **Health status monitoring:** Includes gathering and displaying the security event log, vulnerability information, alteration of security device configuration, performance and operational status on service. It helps administrators to have awareness of the overall service health status.

– **Abnormal behaviour detection:** Includes illegal log-in, illegal access and violation access to specific services, and the abnormal modifications of a physical device.

– **Physical security monitoring:** Includes the temperature and humidity observation, closed-circuit television (CCTV), entrance guard, a fire protection system, air conditioner, power supply system and surveillance.

Security event response deals with requests and recovery from mechanisms such as event handling and management functions and takes recovery actions as the result of applying a set of rules.

10.5 User reminder

The user reminder provides a mechanism to guarantee that the data collected from the sensing device will be used and has been authorized by the location-enabled smart office services user.

The key point is that for a certain location-enabled smart office 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.

10.6 Relationship of security function to security requirements

Table 7 provides security functions to meet corresponding security requirements for a location-enabled smart service.

Table 7 – Security requirements of the smart application mapping to the security threats

Security functions	Security requirements	
Data encryption and key management	For the data: R-01	
	Security requirements for the device	R-09, R-10, R-11
	Security requirements for the interfaces	R-14
Identity management and access control	Security requirements for the data	R-03, R-04, R-05
	Security requirements for the interfaces	R-12, R-13, R-15, R-16
	Security requirements for the platform	R-19, R-20
	Security requirements for the smart application	R-21, R-22, R-23
Integrity verification	Security requirements for the data	R-02, R-06
	Security requirements for the interfaces	R-17
	Security requirements for the platform	R-18

Table 7 – Security requirements of the smart application mapping to the security threats

Security functions	Security requirements	
Security monitoring and security event response	Security requirements for the device	R-08, R-09
	Security requirements for the smart application	R-24
User reminder	Security requirements for the data	R-07

Bibliography

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

[b-ISO/IEC 9796-3] ISO/IEC 9796-3:2006, *Information technology – Security techniques – Digital signature schemes giving message recovery – Part 3: Discrete logarithm based mechanisms.*

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

Published in Switzerland
Geneva, 2023