

# Recommendation **ITU-T X.2011 (04/2024)**

SERIES X: Data networks, open system communications  
and security

Metaverse and digital twin security – Digital twins

---

## **Security guidelines for digital twin network**



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 (I)	X.1100-X.1199
CYBERSPACE SECURITY	X.1200-X.1299
SECURE APPLICATIONS AND SERVICES (II)	X.1300-X.1499
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
INTERNATIONAL MOBILE TELECOMMUNICATIONS (IMT) SECURITY	X.1800-X.1839
METAVEVERSE AND DIGITAL TWIN SECURITY	X.2000-X.2199
<b>Digital twins</b>	<b>X.2000-X.2049</b>
Smart community	X.2050-X.2099
Other metaverse security	X.2100-X.2149
SOFTWARE SUPPLY CHAIN SECURITY	X.2150-X.2199
ARTIFICIAL INTELLIGENCE (AI) / MACHINE LEARNING (ML) SECURITY	X.2200-X.2249

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

# Recommendation ITU-T X.2011

## Security guidelines for digital twin network

### Summary

A digital twin network (DTN) is a virtual representation of a physical network, analysing, diagnosing, simulating and controlling a physical network based on data, model and interface, so as to achieve real-time interactive mapping between the physical network and the DTN. Just like the real network, the DTN will also face security risks and various attacks and it is required to be secure enough to resist all likely attacks.

Recommendation ITU-T X.20122 describes security guidelines and requirements for DTNs. It also provides countermeasures to strengthen security, which will be helpful for all telecommunication operators to improve the security operation of DTNs.

### History \*

Edition	Recommendation	Approval	Study Group	Unique ID
1.0	ITU-T X.2011	2024-04-29	17	11.1002/1000/15887

### Keywords

Countering measures, digital twin network, digital twin, security requirements, threats.

---

\* 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/>.

© ITU 2024

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

## Table of Contents

	<b>Page</b>
1 Scope.....	1
2 References.....	1
3 Definitions .....	1
3.1 Terms defined elsewhere .....	1
3.2 Terms defined in this Recommendation .....	1
4 Abbreviations and acronyms .....	1
5 Conventions .....	2
6 Overview of digital twin network.....	2
7 Security threats to digital twin networks .....	4
7.1 Threats to physical network layer.....	4
7.2 Threats to interfaces .....	4
7.3 Threats to network digital twin layer.....	5
7.4 Threats to network application layer .....	6
8 Security requirements for digital twin networks .....	6
8.1 Security requirements for the physical network layer.....	6
8.2 Security requirements for interfaces.....	6
8.3 Security requirements for network digital twin layer.....	7
8.4 Security requirements for network application layer .....	9
9 Security countermeasure for digital twin network.....	9
9.1 Access control .....	9
9.2 Trustworthiness of data .....	9
9.3 Confidentiality of data.....	10
9.4 Adaptive selection and adjustment of security mechanisms .....	10
Annex A – End-to-end attribute-based encryption mechanisms on DTN data.....	11
Bibliography.....	13



# Recommendation ITU-T X.2011

## Security guidelines for digital twin network

### 1 Scope

This Recommendation contains security guidelines and requirements for digital twin networks (DTNs). This Recommendation:

- Describes security threats to DTNs, including to the process of physical network digitalization;
- Analyses security requirements for DTNs, including for the process of physical network digitalization; and
- Provides technical and management measures to counter identified security threats.

### 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 X.1751] Recommendation ITU-T X.1751 (2020), *Security guidelines on big data lifecycle management by telecommunication operators*.

[ITU-T Y.3090] Recommendation ITU-T Y.3090 (2022), *Digital twin network – Requirements and architecture*.

### 3 Definitions

#### 3.1 Terms defined elsewhere

This Recommendation uses the following term defined elsewhere:

**3.1.1 digital twin network** [ITU-T Y.3090]: A virtual representation of a physical network. It is useful for analysing, diagnosing, emulating and controlling the physical network based on data, model and interface, to achieve the real-time interactive mapping between the physical network and virtual twin network.

#### 3.2 Terms defined in this Recommendation

None.

### 4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

DDoS	Distributed Denial-of-Service
DLT	Distributed Ledger Technology
DTMF	Digital Twin Management Function
DTN	Digital Twin Network

HTTPS	Hypertext Transfer Protocol Secure
IPSec	Internet Protocol Security
NEF	Network Exposure Function
NF	Network Function
NRF	Network function Repository Function
PKI	Public Key Infrastructure
SBA	Service Based Architecture
SLA	Service Level Agreement
TEE	Trusted Execution Environment
TLS	Transport Layer Security
TPM	Trusted Platform Module
UE	User Equipment
VLAN	Virtual Local Area Network

## 5 Conventions

In this Recommendation:

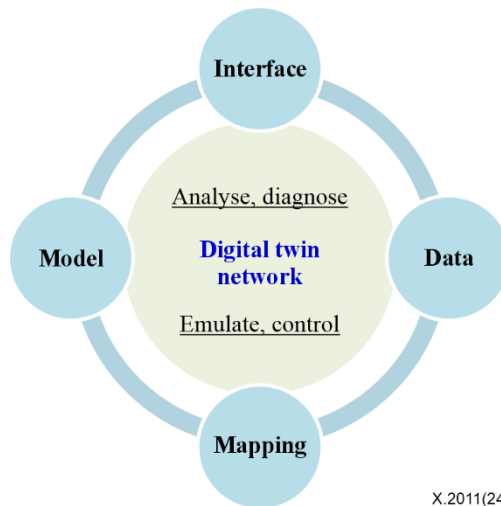
The keywords "is required to" indicate a requirement which must be strictly followed and from which no deviation is permitted, if conformance to this document is to be claimed.

The keywords "is recommended" indicate a requirement which is recommended but which is not absolutely required. Thus, this requirement need not be present to claim conformance.

## 6 Overview of digital twin network

DTN is a virtual representation of the physical network, analysing, diagnosing, emulating and controlling it based on data, model and interface so as to achieve a real-time interactive mapping between the physical network and the DTN. The DTN has four key characteristics: data, mapping, model and interface, as shown in Figure 1. These can be described as follows:

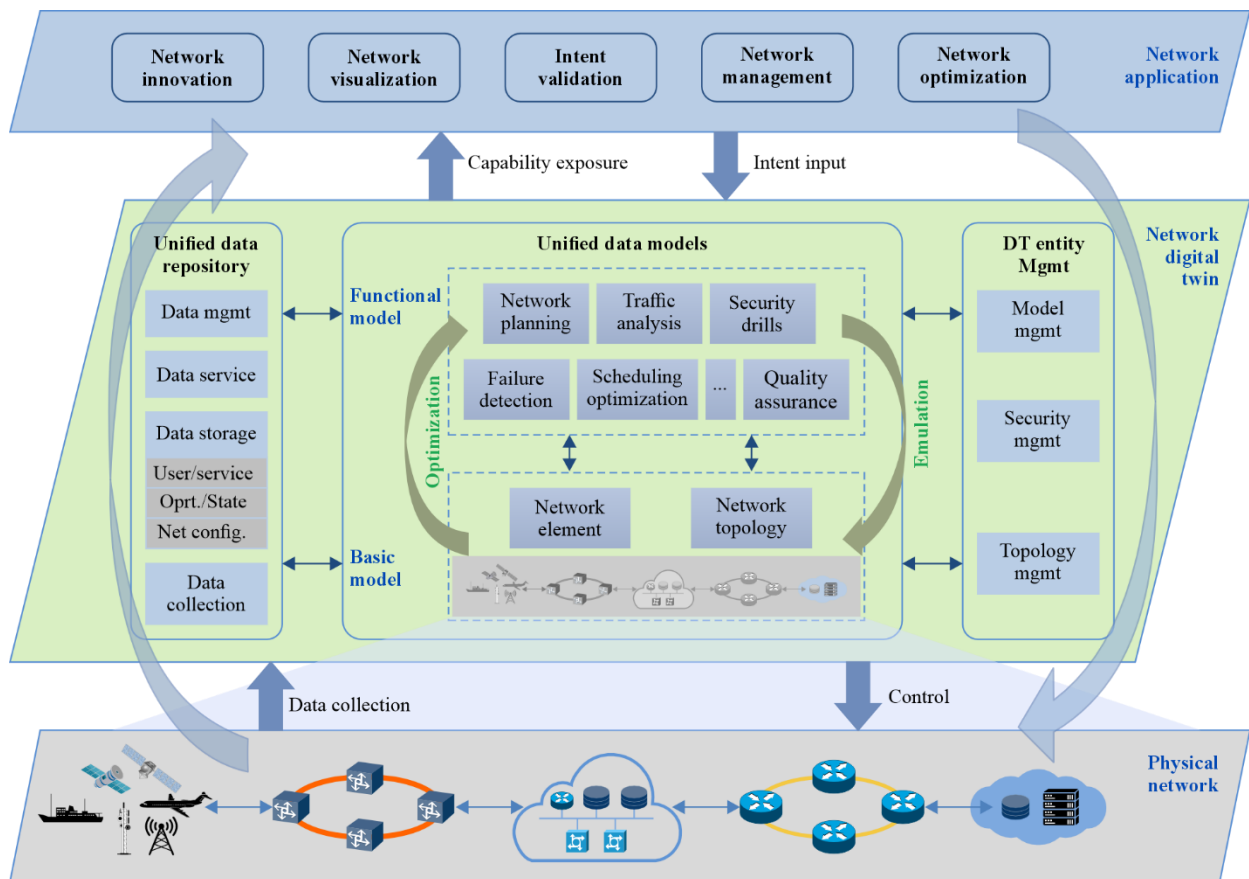
- 1) Data is the cornerstone for constructing a DTN system. Massive network data collected from the physical network can be stored in a virtual twin network as a unified data repository, which can be a single source of truth and provide timely and accurate data support for models.
- 2) Real-time interactive mapping between a physical network and a virtual twin network is the most typical feature that makes a DTN different from a network simulation system.
- 3) The model is the source of the ability of a DTN. Various data models built in virtual twin networks can be designed and flexibly combined to serve network applications.
- 4) The standardized interface is the key enabler that effectively ensures the compatibility and scalability of the DTN system. Southbound interfaces connect the physical network and virtual twin networks while northbound interfaces exchange information between virtual twin networks and network applications.



X.2011(24)

**Figure 1 – Key characteristics of a digital twin network**

Based on these four key characteristics, a DTN creates an accurate digital network simulation platform, which can digitally show the running status and health state of the network infrastructures including physical network devices, logical network devices, ports and links. A DTN can help users clearly perceive the network state, efficiently mine valuable network information and explore innovative network applications with friendly immersive interactive interfaces. Through artificial intelligence (AI) / machine learning (ML), big data and cloud technology, a DTN can also help the physical network realize low-cost trials, intelligent decision-making, efficient innovation and predictive maintenance. A reference architecture of a DTN with three layers is shown in Figure 2.



X.2011(24)

**Figure 2 – A reference architecture of a digital twin network**

- 1) The bottom layer of the DTN is the physical network layer. All network elements in the physical networks exchange massive network data and control with a network digital twin entity, via southbound interfaces.
- 2) The middle layer is the network digital twin layer, which is the core of the DTN system. This layer includes three key subsystems: a unified data repository, unified data models and digital twin entity management.
- 3) The top layer is the network application layer. Network applications input the requirements to the network digital twin layer through the northbound interfaces and deploy services through modelling instances. Network applications can be deployed rapidly with lower cost and higher efficiency and less impact on the running of a network business [ITU-T Y.3090].

## **7 Security threats to digital twin networks**

DTNs have the characteristics of digitization, networking and intelligence and their application scenarios are more open, interconnected and shared. With the continuous expansion of their application fields, network security issues will gradually become prominent. DTNs and their applications may face the security risks and challenges described in this clause, which lists the threats for the four layers according to the DTN architecture described above:

- 1) Threats to the physical network layer;
- 2) Threats to interfaces;
- 3) Threats to the network digital twin layer;
- 4) Threats to the network application layer.

### **7.1 Threats to physical network layer**

#### **7.1.1 Threats to sensing devices**

Sensing devices are the cells of a DTN, the basic link to realize network configuration information, network operation status and user service data collection. These sensing devices are large in number and widely distributed. If the security vulnerabilities of hardware, software and data interfaces are maliciously exploited, the physical network will be greatly impacted.

#### **7.1.2 Threats to network elements**

If network elements (e.g., core network, access network) are attacked through the new interfaces introduced by the DTN, this may not only endanger user data but also damage the availability of network and computing resources, such as the availability of base station services.

### **7.2 Threats to interfaces**

#### **7.2.1 Data collection from network infrastructure**

A relatively closed physical network, such as a radio access network, may increase multiple exposed interfaces due to the introduction of a DTN. Attackers can use these interfaces to launch more attacks, such as data eavesdropping and tampering. In addition, the frequency of data collection is too high, which may lead to a distributed denial-of-service (DDoS) attack. If the data cannot be collected and uploaded in time, the real-time performance of a DTN may be affected, especially when the DTN is used for security applications, and this may lead to untimely risk analysis and response. In addition, the security measures of the interface may affect the data transmission efficiency and then affect the real-time requirements.

## **7.2.2 Control instructions from network digital twin to network infrastructure**

The virtualized twin parts of a DTN may be more vulnerable to attack and can even send false control instructions to the physical network and cause chaos in the real world. The newly issued instructions of a model may conflict with the instructions executed by the NF or issued by other models, resulting in the failure of the security policy.

## **7.2.3 Intent translation from network application**

Attackers may affect the physical network by inputting the false requirements or launch network attacks against a DTN via an exposed interface.

## **7.2.4 Information exchange of a network application and network digital twin**

This interface transmits interaction information between a DTN and the network application layer, and this information may be at risk of being stolen or tampered with.

## **7.3 Threats to the network digital twin layer**

### **7.3.1 Threats to unified data repository**

In the process of application, a DTN needs to generate and store massive device data, user data, interaction data and management data, etc. These data could be accidentally leaked and accessed by attackers without authorization; how to guarantee the security of these data transmission and storage is a challenge for the network. The multilevel collaboration of heterogeneous networks leads to greater security risks and difficulties in data sharing, which may lead to a failure of data sharing, and it is difficult to meet the relevant requirements for data sharing in DTN. When the network digital twin layer itself is tampered with or has logic errors, the data will also be destroyed, making it difficult to meet the requirements for application and analysis of data in a DTN.

### **7.3.2 Threats to unified data models**

The digitization process of the physical world mainly refers to the representation of physical objects into digital models that can be recognized by computers and networks. Modelling technology is one of the core technologies of digitization, and includes mapping and scanning, geometric modelling, network modelling, system modelling, process modelling and so on. The risks faced by the modelling include the unsecure operation of the models and unsecure models themselves.

Unsecure operation of the models includes unauthorized operations on the model, such as illegal upload, tampering, deletion, disclosure and access.

Unsecure models are associated with the following issues:

- Incapability to deal with abnormal data input (e.g., interference data or lossy data) or attacks (e.g., adversarial inputs, model stealing).
- Vulnerabilities of the model introduced by improper model design or implementation, e.g., extensive influence, improper access control to sensitive data, and wrong or untimely instructions. These can be exploited to obtain the corresponding network resources (e.g., SLA, user data, business logic).
- Untrusted models that cannot execute their claimed functions.
- Policy conflicts among models resulting in bypassing security-related instructions.

### **7.3.3 Threats to management**

The integration of digital twin with cloud computing, Internet of things, big data, mobile Internet, industrial Internet and other technologies, as well as the in-depth intervention of third-party collaboration services and multilevel collaboration of a large number of heterogeneous platforms are inevitable trends. When the security problems of various emerging technologies have not been fully exposed, the integration of multitechnologies and multiservices makes network security

problems more complex and changeable, and the risks of network security increase sharply, bringing more intrusion methods and attack routes. At the same time, the network security management mechanisms and specifications for new services and applications are also lagging behind to varying degrees, which will bring new challenges to security operation and maintenance.

Lack of management (e.g., addition, deletion, modification, query) of security policy (e.g., policies on authentication, authorization, encryption and integrity protection) may result in the improper security configuration of the DTN and lead to an inability to resist attacks to the data, model, applications and so on. Security policy needs to be managed, which includes its creation, reading, updating and deleting.

## **7.4 Threats to network application layer**

The network applications input requirements to the DTN, and deploy the services in it through the model instance. Threats to network applications are as follows:

- Spoofing: Attackers may masquerade as the network digital twin layer to obtain information on requirements such as network data and user data for further attacks. Attackers can also pretend to report incorrect data, such as statistics, to applications. In addition, malicious applications can be disguised as legitimate applications to obtain corresponding network resources or input incorrect requirements which may impact the physical network through the network digital twin.
- Repudiation: The application users or the administrators deny an operation as improper input to the application.
- Exploitation to vulnerability: Vulnerabilities in the application can result in unauthorized access or improper requirements, leading to the wrong configuration of the twin network, which may affect the physical network. The attackers can also obtain the corresponding network resources (such as SLA, user data, business logic) by exploiting the vulnerabilities of the application, so as to prepare for further attacks.

## **8 Security requirements for digital twin networks**

A DTN is required to be secure enough to avoid all possible attacks. After the network has been attacked maliciously, all kinds of defence plans also need to be fully considered. Clauses 8.1 to 8.4 describe security considerations and requirements according to the threats to a DTN.

### **8.1 Security requirements for the physical network layer**

#### **8.1.1 Security requirements for sensing devices**

- It is required to verify the integrity of hardware and software of sensing equipment.
- It is required to verify the identity of sensing devices to avoid introducing false devices.

#### **8.1.2 Security requirements for network elements**

- It is required to authorize the access to the network elements before the DTN collects network data and sends network controls.
- It is required to provide detection and warning of abnormal collection behaviour.
- It is recommended to ensure the network elements are trustworthy.

### **8.2 Security requirements for interfaces**

#### **8.2.1 General requirements**

- It is required to perform authentication and authorization between peers using the interfaces.

- It is required to protect the integrity of the communication at the interfaces.
- It is recommended to protect the confidentiality of the communication at the interfaces.
- It is required to protect against replay attacks.

### **8.2.2 Security requirements for data-collection interfaces**

- It is required to support anti-DDoS attacks from the network infrastructure.

### **8.2.3 Security requirements for control interfaces**

- It is recommended to support separation between the network management plane and any other transmission plane.
- It is recommended to support the detection of policy conflicts and give a resolution to avoid the bypass of mandatory network policies.
- It is recommended to support phased, minimized and hierarchical confidentiality protection for the control instructions for the different security domains of the network.
- It is required to record all the control instructions.

### **8.2.4 Security requirements for intent translation interfaces**

- It is recommended to support the classification of intention, and dynamically allocate the authority of intention input according to the user's business type.
- It is recommended to support the manual adjustment of the results of intention translation to ensure that the network strategy can meet the needs of users.

## **8.3 Security requirements for network digital twin layer**

### **8.3.1 Security requirements for the unified data repository**

- The confidentiality, integrity and reliability of the sensitive data in the DTN are required to be maintained throughout its lifecycle, including during creation, storage, usage, sharing, archiving and destruction [ITU-T Y.3090].
- It is required to allocate necessary privileges to the unified data repository to deal with the data (e.g., collection, preprocessing).
- It is required to support fine-grained authorization for data access to ensure that data in the unified data repository can only be accessed by the privileged entities (e.g., model, users and network applications).
- It is recommended not to collect personally identifiable information. The network users' consent is required to authorize that the personal data can be collected. Utilization of sensitive data is recommended to be audited, with audit logs generated [ITU-T X.1751].
- It is required to ensure the trustworthiness and traceability of the collected data.
- It is required to classify the sensitive data with different levels. It is recommended to support secure protection methods for data and computing processes. It is recommended to support a selection function of secure protection methods to deal with the data according to different levels of requirements for the real-time, confidentiality, integrity and trustworthiness of the data.

### **8.3.2 Security requirements for unified data models**

- It is required to support the integrity and confidentiality protection of the models and the data used.
- It is required to allocate necessary privileges to the models with different purposes and security levels to access the data, other models and network functions (NFs).

- It is required for the model, or any other NFs that may store the model, to be able to check that the entity (e.g., network applications or other models) is authorized to retrieve that model.
- It is required to detect security vulnerabilities before a model is deployed to eliminate potential risks and damages in advance.
- It is required for a model to be auditable in order to evaluate its security including whether the data is sufficient for twinning and simulation, the affected objects (e.g., NFs, services, users) of the control instructions and the privilege of data used for models.
- It is recommended to provide mechanisms to ensure that the model is able to operate normally when facing abnormal data input and attacks.
- It is required to support policy conflict detection. It is recommended to set different priorities for different models to ensure that the security control cannot be bypassed.
- It is recommended to support monitoring and alert of the consistency between the basic model and the physical network.
- It is recommended to support building multiple twins for multiple network security domains and to collect data as the corresponding security requirements for each domain.

### **8.3.3 Security requirements for management and operation**

- It is required to support the management function including authentication and authorization of a DTN platform's users.
- It is required to support the security interaction of models and data of different domains. It is recommended to make sure the models, data and the providers in other domains are trustworthy.
- It is required to support management of the policy and methods on lifecycle data security, model security, application security, network security and interactive security of the DTN including but not limited to encryption and integrity.
- It is required to support authorization of the operations including create-read-update-delete for lifecycle data, models, applications and users.
- It is required to support the management of security-related material used in a DTN such as certificates used for SBA security and user equipment (UE) credentials used for primary authentication/slice authentication/secondary authentication [b-3GPP TS 33.501]. It is recommended for the management to include the generation, storage, deletion, backup and recovery of security-related material.
- Before connecting to the production network, a security test of DTN components including devices and networks is required to be carried out. A security test of devices includes but is not limited to checking whether they are configured according to the security requirements for the account, service port, system log, password strength, vulnerability, anti-virus software and network element specific security functions. A security test of networks includes but is not limited to checking whether they are configured according to the security requirements for the network assets, topology, security domain, firewall, router, etc. (e.g., security domain topology, security domain assets, VLAN access control strategy, boundary interconnection).
- It is required to regularly monitor the security of asset management, account password, compliance configuration, vulnerability and patch management.
- It is required to support an incident response function in response to and to deal with attacks in time, at least including security emergency plan management, security event monitoring, security event early warning and security event disposal.

- It is required to support log and audit functions of the DTN. Audit logs that document any alteration to stored data are required to be maintained. Logs are required to be securely stored and attempts to alter them are recommended to be captured and reported.
- It is required not to use weak passwords and easy-to-guess passwords. It is required to modify the password regularly and protect the account and password properly. The account lifecycle, account allocation principles and password configuration rules are required to be clarified and strictly controlled.

#### **8.4 Security requirements for network application layer**

- It is required for applications to authenticate the users and the entities of the network digital twin layer.
- It is required to allocate privileges to the applications using models and support permission verification when the application accesses the DTN system.
- The minimum access to the network digital twin is required in the network application layer [ITU-T Y.3090].
- It is required to detect security vulnerabilities before applications are deployed.

### **9 Security countermeasure for digital twin network**

This clause provides some available and feasible countermeasures to meet the security requirements defined in clause 8.

#### **9.1 Access control**

According to clause 8, data, models, network elements and applications are required to be protected from unauthorized access. Some available and feasible security methods, such as a whitelist/blacklist [b-IETF RFC 5782] [b-IETF RFC 5851], ACL [b-IETF RFC 4314] or an access token [b-IETF RFC 6749] [b-IETF RFC 7519] can be used to provide access control. To provide non-repudiation of data access in a multi-partner context, distributed ledger technology (DLT) based storage and access control can be used. When the physical network is an IMT-2020 network, the existing access control mechanism and related network elements such as NRF or NEF [b-3GPP TS 33.501] might be considered for reuse.

#### **9.2 Trustworthiness of data**

- Trustworthiness of the data source: According to clause 8, data sources (e.g., network elements, data providers in other domains) for DTN are recommended to be trustworthy, which means the identity and the behaviours of each data source need to be trustworthy. Some available and feasible security methods, such as PKI certificate [b-ITU-T X.509], DLT based certificate management [b-ITU-T X.1409] or decentralized identity management [b-ITU-T X.1403], can be used to make sure the identity of the data source is trustworthy. Some available and feasible security methods, such as TEE, TPM [b-ISO/IEC 11889] or zero trust [b-ITU-T X.1011], can be used to make sure the behaviours of the data source are trustworthy.
- Tamper-proof data in transit: According to clause 8, data for DTN are required to be protected from being tampered or modified in transit in different scenarios including transit from the physical network layer to a unified data repository, transit between unified data repository and models, and transit among different domains. Some available and feasible security methods, such as HTTPS [b-IETF RFC 2818], transport layer security (TLS) [b-IETF RFC 5246] or the IPsec protocols ([b-IETF RFC 4301], [b-IETF RFC 4303], [b-IETF RFC 4835]), can be used to provide data integrity in transit for suitable scenarios and protocols.

- Tamper-proof data in storage: According to clause 8, an integrity detection mechanism is recommended to be provided to determine the damage and loss of data. Some available and feasible security methods, such as digital signature and hash algorithm, can be used to provide data integrity in transit for suitable scenarios and protocols.
- Traceability of data: According to clause 8, data for DTN are required to be traceable, which means the record of where the data come from and go to needs to be auditable. Some available and feasible security methods, such as digital signature, log, DLT based security audit [b-ITU-T X.1409] or digital watermark can be used to assure the traceability of data.

### 9.3 Confidentiality of data

- Confidentiality in transit: Some available and feasible security methods, such as HTTPS [b-IETF RFC 2818], TLS [b-IETF RFC 5246] or the IPSec protocols ([b-IETF RFC 4301], [b-IETF RFC 4303], [b-IETF RFC 4835]), can be used to establish secure transmission channels to provide data confidentiality in transit.
- Confidentiality in storage: Cryptographic encryption can be used to provide confidentiality of the DTN data which are stored in the files or tables of a database. Since one kind of data might be used by multiple data models, attribute-based encryption can be used to distribute keys online with only one ciphertext and one-time encryption to provide confidentiality and fine-grained access control to certain data. Only the keys associated with the admission attribute can decrypt the DTN data. The keys can be distributed by the data providers (e.g., the devices in the physical network) who also authorize the access from the data models to their data, in which case the plain text of the twin data can be invisible to the unified data repository and attackers can only obtain encrypted data from the data warehouse even if the unified data repository is not trusted. The detail of this approach is described in Annex A, which is suitable for the data and data providers who need end-to-end confidentiality protection and to authorize by itself.
- Confidentiality in usage: Some available and feasible security methods, such as data masking, anonymization and confidential computing, can be used to make the data invisible during use by the data models.

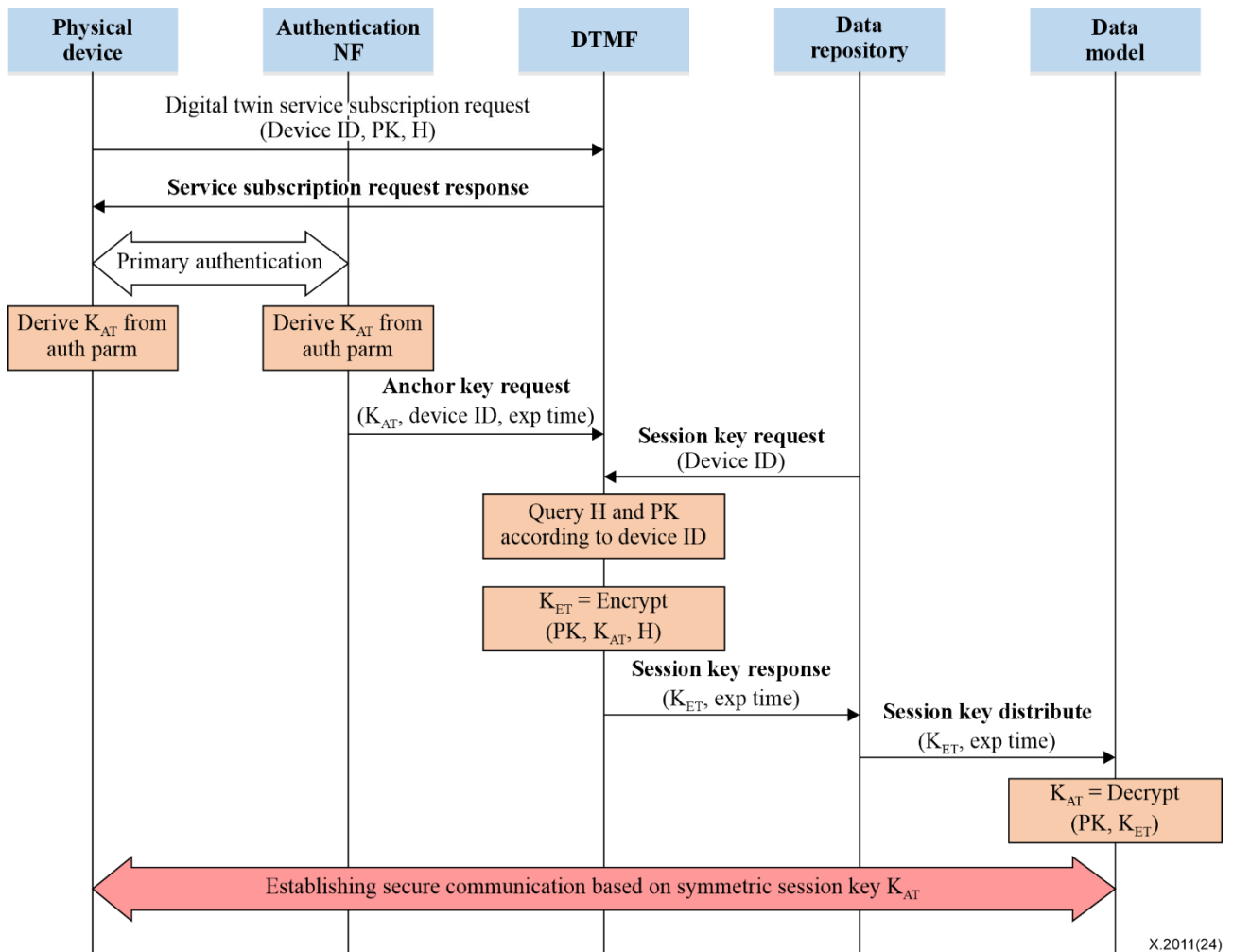
### 9.4 Adaptive selection and adjustment of security mechanisms

The diverse and dynamic DTN data sources and models require differentiated security requirements (e.g., real-time, integrity and trustworthiness) to be dynamically met. Security mechanisms have different security and non-security effects, such as security level, efficiency, cost, information loss, software and hardware support, availability and visibility. A selection and adjustment approach of the security protection mechanisms based on the requirements of models and data can be considered for adoption. In detail, at first, data providers report the data they can provide and the security mechanisms they can support. The mapping between the security mechanisms and the attributes need to be established in advance. Information of the applications or models and that of the data they use need to be reported. Security information can be obtained or analysed from the information. Based on the security information, the security requirements (e.g., confidentiality, credibility, real-time) of DTN data can be decided. Candidate data providers are determined based on the data they can provide. The DTN data security mechanisms list is generated based on the data providers' support for the security mechanisms and the security mechanism's satisfaction with the security requirements. If the data providers' security mechanisms do not meet the security requirements, other data providers are to be selected or the application or models are to be notified to replace the data used. Finally, the data providers and related security entities are configured with the security mechanisms. Meanwhile, the status of the network is obtained and data providers and related security entities are redetermined and reconfigured to support security policies with redetermined security mechanisms if needed.

## Annex A

### End-to-end attribute-based encryption mechanisms on DTN data

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



**Figure A.1 – Workflow of end-to-end attribute-based encryption mechanism on DTN data**

Figure A.1 shows the end-to-end attribute-based encryption mechanisms on DTN data.

- 1) The digital twin management function (DTMF) is introduced in the network infrastructure layer, which manages the digital twin service and provides a security capability for digital twin application. The physical device and data model obtain the public key and private key associated with the admission attribute from the trusted key distribution centre.
- 2) The physical device (including UE and NFs) needs to send the digital twin service subscription request to the DTMF before connecting to the DTN, including twin public key PK, data access policy H and device ID.
- 3) After receiving the request, the DTMF verifies whether physical devices support the digital twin protocol, then the DTMF saves PK, H and device ID and sends the digital twin service subscription response.
- 4) After the physical device authentication with the authentication NF, the symmetric session key  $K_{AT}$  is derived from the parameters generated during the primary authentication process in the physical device and authentication NF.

- 5) The authentication NF sends a twin key anchoring the key request to the DTMF, carrying the parameter  $\langle K_{AT}, \text{device ID}, \text{and expiration time} \rangle$ . The expiration time of the  $K_{AT}$  can be set according to the level of security requirements. The  $K_{AT}$  needs to be refreshed when the expiration has passed or the physical device has been re-authenticated. Then the DTMF saves the  $K_{AT}$ .
- 6) When the data repository sends a session key request to the DTMF, the DTMF calculates  $K_{ET} = \text{Encrypt}(PK, K_{AT}, H)$  with CP\_ABE encryption algorithm, and sends the  $\langle K_{ET}, \text{expiration time} \rangle$  to the data repository.
- 7) The data repository has the map  $M$  between physical devices and the data model. Then the data repository distributes the  $\langle K_{ET}, \text{expiration time} \rangle$  to the multiple twin data model of the physical device.
- 8) The data model decrypts the  $K_{ET}$  using the twin private key  $SK$ ,  $K_{AT} = \text{Decrypt}(K_{ET}, SK)$ .
- 9) The physical device establishes secure communication with the data model based on the symmetric session key  $K_{AT}$ .

## Bibliography

- [b-ITU-T X.509] Recommendation ITU-T X.509 (2019) | ISO/IEC 9594-8:2019, *Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks*.
- [b-ITU-T X.1011] Recommendation ITU-T X.1011 (2021), *Guidelines for continuous protection of service access process*.
- [b-ITU-T X.1403] Recommendation ITU-T X.1403 (2020), *Security guidelines for using distributed ledger technology for decentralized identity management*.
- [b-ITU-T X.1409] Recommendation ITU-T X.1409 (2022), *Security services based on distributed ledger technology*.
- [b-IETF RFC 2818] IETF RFC 2818 (2000), *HTTP over TLS*.  
<https://datatracker.ietf.org/doc/html/rfc2818>
- [b-IETF RFC 4301] IETF RFC 4301 (2005), *Security architecture for the Internet protocol*.  
<https://datatracker.ietf.org/doc/html/rfc4301>
- [b-IETF RFC 4303] IETF RFC 4303 (2005), *IP encapsulating security payload (ESP)*.  
<https://datatracker.ietf.org/doc/html/rfc4303>
- [b-IETF RFC 4314] IETF RFC 4314 (2005), *IMAP4 access control list (ACL) extension*.  
<https://datatracker.ietf.org/doc/html/rfc4314>
- [b-IETF RFC 4835] IETF RFC 4835 (2007), *Cryptographic algorithm implementation requirements for encapsulating security payload (ESP) and authentication header (AH)*. <https://datatracker.ietf.org/doc/html/rfc4835>
- [b-IETF RFC 5246] IETF RFC 5246 (2008), *The transport layer security (TLS) protocol: Version 1.2*. <https://datatracker.ietf.org/doc/html/rfc5851>
- [b-IETF RFC 5782] IETF RFC 5782 (2010), *DNS blacklists and whitelists*.  
<https://datatracker.ietf.org/doc/html/rfc5782>
- [b-IETF RFC 5851] IETF RFC 5851 (2010), *Framework and requirements for an access node control mechanism in broadband multi-service networks*.  
<https://datatracker.ietf.org/doc/html/rfc5851>
- [b-IETF RFC 6749] IETF RFC 6749 (2012), *The OAuth 2.0 authorization framework*.  
<https://datatracker.ietf.org/doc/html/rfc6749>
- [b-IETF RFC 7519] IETF RFC 7519 (2015), *JSON Web Token (JWT)*.
- [b-3GPP TS 33.210] 3GPP TS 33.210 (2022), *Network domain security (NDS); IP network layer security*.  
<https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=2279>
- [b-3GPP TS 33.501] 3GPP TS 33.501 V17.1.0 (2022), *Security architecture and procedures for 5G system (Release 17)*.
- [b-ISO 11889] ISO/IEC 11889:2015 (TCG 2.0), *Information technology – Trusted platform Library — Part 1: Architecture*.  
[https://standards.iso.org/ittf/PubliclyAvailableStandards/c066510\\_ISO\\_IEC\\_11889-1\\_2015.zip](https://standards.iso.org/ittf/PubliclyAvailableStandards/c066510_ISO_IEC_11889-1_2015.zip)





## 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
<b>Series X</b>	<b>Data networks, open system communications and security</b>
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