ITUPublications

International Telecommunication Union
Standardization Sector

ITU-T Technical Report

(12/2025)

XSTR.sd-cnc

Data security guidelines for the coordination of networking and computing

Technical Report ITU-T XSTR.sd-cnc

Data security guidelines for the coordination of networking and computing

Summary

This Technical Report provides data security guidelines for the coordination of networking and computing (CNC).

It covers introduction for data categorization (including resource operation and maintenance data, outsourced data and transaction data) in CNC, identifies threats to different categories of data and offers security guidelines to mitigate identified threats.

Keywords

Coordination of networking and computing (CNC), data security.

Note

This is an informative ITU-T publication. Mandatory provisions, such as those found in ITU-T Recommendations, are outside the scope of this publication. This publication should only be referenced bibliographically in ITU-T Recommendations.

Editor: Ke WANG
China Mobile
China

Tel: +8613488788496
E-mail: wangkeyj@chinamobile.com

Table of Contents

Technical Report ITU-T XSTR.sd-cnc

Data security guidelines for the coordination of networking and computing

1 Scope

This Technical Report provides data security guidelines for the coordination of networking and computing (CNC). It covers introduction for data categorization (including resource operation and maintenance data, outsourced data and transaction data) in CNC, identifies threats to different categories of data and offers security guidelines to mitigate identified threats.

2 References

[ITU-T X.1641] Recommendation ITU-T X.1641 (2016), *Guidelines for cloud service customer data security.*

[ITU-T Y.3400] Recommendation ITU-T Y.3400 (2023), *Coordination of networking and computing in IMT-2020 networks and beyond – Requirements.*

3 Definitions

3.1 Terms defined elsewhere

None.

3.2 Terms defined in this Technical Report

This Technical Report defines the following term:

3.2.1 coordination of networking and computing (CNC): The organization of utilization, control and management of computing, storage and networking resources for provisioning and optimization, satisfying the requirements of resource users and improving resource utilization.

NOTE – Based on [ITU-T Y.3400].

4 Abbreviations and acronyms

This Technical Report uses the following abbreviations and acronyms:

CNC Coordination of Networking and Computing

CPU Central Processing Unit

FMSC Fixed, Mobile and Satellite Convergence

QoS Quality of Service

5 Data identification based on CNC requirements and scenarios

In [ITU-T Y.3400], various requirements for CNC are described. Based on these requirements, relevant data is identified.

5.1 Measurement of resources

The data related to the "measurement of resources" requirements is shown in Table 5-1.

Table 5-1 – Data related to "measurement of resources" requirements

Requirements from [ITU-T Y.3400]	Data
Multiple dimensions of computing resources	– Computing resource type – Computing resource characteristics, such as capacity, performance, central processing unit (CPU) frequency and number of CPU cores
Multiple dimensions of storage resources	– Storage resource type, storage resource – Characteristics, such as storage capacity, storage access speed, storage operation time cycle and storage reliability
Multiple dimensions of networking resources	– Networking resource type – Networking resource characteristics, such as bandwidth and delay

5.2 Identification and addressing of resources

The data related to "identification and addressing of resources" requirements is shown in Table 5-2.

Table 5-2 – Data related to "Identification and addressing of resources" requirements

Requirements from [ITU-T Y.3400]	Data
Multiple dimensions of computing resources	– Computing resource type – Computing resource characteristics, such as capacity, performance, central processing unit (CPU) frequency and number of CPU cores
Multiple dimensions of storage resources	– Storage resource type – Storage resource characteristics, such as storage capacity, storage access speed, storage operation time cycle and storage reliability
Multiple dimensions of networking resources	– Networking resource type – Networking resource characteristics, such as bandwidth and delay

5.3 Awareness of resources

The data related to "awareness of resources" requirements is shown in Table 5-3.

Table 5-3 – Data related to "awareness of resources" requirements

Requirements from [ITU-T Y.3400]	Data
Awareness of resource attributes	– Resource type – Resource characteristics – Resource location – Resource cluster (if applicable)
Awareness of subscription information on resources	Subscription information
Awareness of resource operational status information	Response time

Table 5-3 – Data related to "awareness of resources" requirements

Requirements from [ITU-T Y.3400]	Data
Anomaly usages of resources and their locations	Location
Adjust the awareness period	Expected frequency of resource status changes and/or resource usage
Aware of the priority of resource requirements	Different requirements of resource users, include multiple parameters, such as latency and security related parameters, and resource users may specify their priority

5.4 Joint scheduling of resources

The data related to "joint scheduling of resources" requirements is shown in Table 5-4.

Table 5-4 – Data related to "joint scheduling of resources" requirements

Requirements from [ITU-T Y.3400]	Data
The coordination of networking, computing and storage resources	Resource operation status information and resource requirements
Support of the generation of joint scheduling policies of resources	Joint scheduling policies

5.5 Unified management and orchestration of resources

The data related to "unified management and orchestration of resources" requirements is shown in Table 5-5.

Table 5-5 – Data related to "unified management and orchestration of resources" requirements

Requirements from [ITU-T Y.3400]	Data
Support unified registration, configuration, provision and authentication of resources	– Information of registration, configuration, provision – authentication information
Support the monitoring of resources	Capacity monitoring, fault monitoring and performance monitoring

5.6 Resource transaction

The data related to "resource transaction" requirements is shown in Table 5-6.

Table 5-6 – Data related to "resource transaction" requirements

Requirements from [ITU-T Y.3400]	Data
Support unified management of resource transaction information	Accounting information and multiparty settlement information
Match the resource user's requirements and resource providers' supply	– User's requirements – Resource providers' supply
Support the capability of storage management of transaction data	– Data related to resource transaction contract information

Table 5-6 – Data related to "resource transaction" requirements

Requirements from [ITU-T Y.3400]	Data
	– Resource transaction ledger information and resource exchange information
Support multiple resource transaction policies	Monetary and/or non-monetary incentives

5.7 Energy saving

The data related to the requirements for "energy saving" is shown in Table 5-7.

Table 5-7 – Data related to "energy saving" requirements

Requirements from [ITU-T Y.3400]	Data
Awareness of energy related information	Consumption, energy type and energy efficiency
Aware of resource energy requirements	Energy consumption demand
Support resource scheduling policies	Resource energy requirements and energy related information

5.8 Quality of service (QoS) assurance

The data related to "QoS assurance" requirements is shown in Table 5-8.

Table 5-8 – Data related to "QoS assurance" requirements

Requirements from [ITU-T Y.3400]	Data
New requirements on QoS assurance	QoS planning, QoS provisioning, QoS monitoring and QoS optimization

5.9 Fixed, mobile and satellite convergence (FMSC)

[ITU-T Y.3400] describes the functional requirements of CNC supporting fixed, mobile and satellite convergence (FMSC) and does not cover specific data.

5.10 Intelligence and automation level

The data related to "intelligence and automation level" requirements is shown in Table 5-9.

Table 5-9 – Data related to "intelligence and automation level" requirements

Requirements from [ITU-T Y.3400]	Data
Have the capability of intelligent scheduling	Scheduling strategy
Have the capability of intelligent management operation and maintenance	– Intelligent fault, intelligent configuration – Intelligent accounting

5.11 Security

The data related to "security" requirements is shown in Table 5-10.

Table 5-10 – Data related to "security" requirements

Requirements from [ITU-T Y.3400]	Data
Verify the credibility of resource information	– The source of the resource information and the resource attributes – Authentication and encryption mechanisms
Authenticate and authorize the source of resource scheduling policy	– Information of authentication and authorization – Scheduling policy
Authenticate the identity of resource users	Identity of resource users
Keep the resource usage records of resource users confidential	– Information on resource usage time, resource usage amount and resource usage location
Keep the resource status information confidential	– Resource status information – Security policies

5.12 Scenarios of CNC

[ITU-T Y.3400] describes different service scenarios of CNC; related data is shown in Table 5-11.

Table 5-11 – Data related to scenarios of CNC

Requirements from [ITU-T Y.3400]	Data
Different service scenarios have different requirements for resources	Data of service

6 Data categorization

Based on the data identified in clause 5, a data categorization method is proposed.

6.1 Data of resource attributes

Data of resource attributes, which includes information about relevant CNC resources, such as computing, storage and networking.

The data details are as follows:

a) Resource type.

b) Resource characteristics, such as computing capacity, performance, central processing unit (CPU) frequency and number of CPU cores, storage capacity, storage access speed, storage operation time cycle and storage reliability, network bandwidth and network delay.

c) Source of the resource.

d) Resource location.

e) Resource cluster (if applicable).

6.2 Data of resources management and orchestration

Data of resources management and orchestration, which includes data of joint scheduling of resources, data of unified management and orchestration.

The specific data details are as follows:

a) Resource status: resource operation status, response time, expected frequency of resource status changes and resource usage.

b) Information of resources unified management and orchestration: Information of resources registration, configuration, provision; information of capacity monitoring, fault monitoring and performance monitoring.

c) Data of resources joint scheduling: joint scheduling policies, scheduling strategies of intelligent scheduling and intelligent configuration.

d) Other CNC operation-related data: energy consumption demand, energy consumption, energy type and energy efficiency, resource energy requirements.

6.3 Data of resources transaction

Data of resources transaction, includes accounting information, multiparty settlement information, resource matching information and other related data of resource transaction.

The specific data details are as follows:

a) Resource matching: information of user's requirements (including multiple parameters, such as latency and security related parameters, and resource users may specify their priority) and resource providers' supply.

b) Data of transaction content: accounting information and multiparty settlement information, resource transaction contract information, resource transaction ledger information, multiple resource transaction policies and transaction incentives.

6.4 Data of security

Data of security includes data generated by CNC related security mechanisms. Security mechanisms are used to ensure the secure operation of CNC.

The specific data details are as follows:

a) Information of authentication.

b) Authorization and encryption.

c) Identity of resource users and providers.

d) Security policies.

6.5 Data of application

Data of applications refers to the data generated by services in CNC. Different services have different applications. Thus, no typical data is listed here.

7 Threats to data in coordination of networking and computing

Different data categories follow distinct flows during their lifecycle and face different threats. The following sections detail these threats for each category (similar cases are consolidated in the descriptions).

7.1 Threats to data of resource attributes

7.1.1 Creation/collection

Resource attribute information is collected during the resource's establishment. This data serves as the foundation for resource allocation in services, and faces the following risks:

a) The data collection interface may be attacked or accessed without authorization, causing data leakage.

b) If data collection exceeds the expected range, it will cause the leakage of computing resource information.

7.1.2 Transmission

The data of resource attributes is transmitted between resources and the resource management entity. Typically, they are located in different domains. During data collection, this transmission usually occurs through external networks. In the aforementioned scenarios, the following risks exist:

a) Data transmitted through insecure channels may be easily intercepted by attackers.

b) Data transmitted in plaintext can be easily intercepted by attackers.

7.1.3 Storage

The data of resource attributes is stored in the resource management entity (this can be a dedicated server or a virtual machine on a shared server). This data is controlled by the operator and faces the following risks:

a) Inadequate management of administrator accounts may result in unauthorized access or data theft by malicious administrators.

b) The resource management entity lacks sufficient network security protection capabilities, and once attacked, it can cause stored data to be destroyed or stolen, leading to data leakage.

7.1.4 Use

When utilized within the entity of resource management, data is also exposed to risks such as unauthorized data usage and theft by administrators.

7.1.5 Migration

When data storage resources need to be modified, the data must be migrated to new storage. During the migration, data may be lost or damaged, affecting regular service activities.

7.1.6 Destruction

When the data storage resources reach the retention time or the platform needs to migrate stored data, data in storage resources need to be destroyed. Incomplete destruction could allow data recovery, resulting in information disclosure.

7.2 Threats to data of resources management and orchestration

The lifecycle of this category of data is similar to data of resource attributes, and the security risks are also similar.

7.3 Threats to transaction data

The lifecycle of this category is similar to that of resource attributes. The difference is that this type of data needs less frequent transmission across security domains. Due to the economic interests involved in transaction data, transaction data and security data are more likely to be attacked.

7.4 Threats to data of security

The lifecycle of this category is similar to that of resource attributes. The difference is that this type of data needs less frequent transmission across security domains. Because transaction data involves economic interests, both transaction data and security data are more vulnerable to attacks.

7.5 Threats to data of application

7.5.1 Transmission

Data of application is transmitted to computing resources or storage resources. Attackers may intercept the data during transmission.

7.5.2 Storage

Due to the need to coordinate different resources to provide storage capabilities, data of application may be stored in multiple heterogeneous resources. This distributed storage architecture introduces several security risks:

a) Storage resources are provided by third parties, and administrator of the resource provider may steal data, resulting in data leakage.

b) Storage providers implement varying security policies. When data flows between different storage resources or backup data is stored in environments different from the original data, this increases the risk of data leakage.

c) When data from multiple applications is stored on the same storage resource without isolation, imperfect data access control mechanisms may lead to unauthorized data exchange between applications, resulting in data leakage.

7.5.3 Use

Application data can be processed across computing resources, and the computation may be distributed among multiple resources. However, data computation faces risks, such as computing resources forging results to save computational power.

7.5.4 Migration

When storage or computing resources need to be updated, data need to be migrated. The risks involved include the following:

a) If data is lost or damaged during migration, the subsequent calculations cannot be executed.

b) If data from some computing or storage resources needs to be migrated while other data is still in use, it may disrupt normal business operations.

7.5.5 Destruction

When data storage reaches its retention period or is requested for deletion by the user, the data must be destroyed. If the data is not completely erased and can be recovered, it poses a risk of data leakage.

8 Data security guidelines for CNC

8.1 Security guidelines to data of resource attributes

8.1.1 Creation/collection

In the stage of data creation/collection, the following security measures can be used:

a) When collecting such data through resource measurement and sensing processes, implement access control restrictions on both awareness interfaces and measurement interfaces.

b) Maintain data collection logs to facilitate auditing of collection activities.

c) Restrict access to data collection interfaces with frequent abnormal access behaviour.

8.1.2 Transmission

In the stage of data transmission, please refer to clause 7.2 of [ITU-T X.1641].

8.1.3 Storage

In the stage of data storage, the following security measures can be used:

a) Implement access control measures to restrict unauthorized access to data.

b) Perform integrity verification on stored data.

c) Encryption can be used for storing key data.

d) Implement a data backup mechanism to ensure data availability. Backup data security measures should maintain consistency with the original data, including access control policies, network security protections and encryption standards.

e) Store different categories of data separately.

8.1.4 Use

In the stage of data use, the following security measures can be used:

a) Implement access control measures to restrict unauthorized data usage.

b) Authorize users to access resource data for which they have been granted service permissions.

8.1.5 Migration

In the stage of data migration, the following security measures can be used:

a) Ensure that data integrity and confidentiality are not compromised during migration.

b) Ensure that data migration does not disrupt service and application continuity.

c) Ensure security consistency (including network protection policies and access control strategies) is maintained both before and after data migration.

d) Develop a data backup and recovery plan prior to data migration to prevent potential data breaches or loss.

e) Verify that all previously stored data in the new storage resources has been completely erased prior to migration.

8.1.6 Destruction

For security protection recommendations in the stage of destruction, please refer to clause 7.6 in [ITU-T X.1641].

8.2 Security guidelines to data of resources management and orchestration

For security guidelines on data of resources management and orchestration, please refer to clause 8.1.

8.3 Security guidelines to data of resources transaction

For this category of data, in addition to the security measures specified in clause 8.1, the following additional measures can be used.

8.3.1 Creation/collection

Data generated during transaction processes requires strict management and control to prevent attacker tampering.

8.3.2 Storage

In the stage of data storage, the following security measures can be used:

a) Store key transaction data (such as payment information and billing details) in encrypted form.

b) Define a dedicated security administrator role with exclusive access privileges to security data.

c) Implement fine-grained access control mechanisms for data protection, preventing leakage due to excessive permissions or unauthorized access.

d) Store resource transaction data in isolated environments.

8.3.3 Migration

Data can be encrypted during migration and transmission.

8.4 Security guidelines to data of security and privacy

For this category of data, in addition to the relevant security measures described in clause 8.1, the following additional security measures can be used.

8.4.1 Storage

In the stage of data storage, the following security measures can be used:

a) Store passwords, security certificates and other data involved in the authentication process in encrypted form.

b) Retain log data for a specified period to support security auditing.

8.4.2 Use

Set up a dedicated log administrator account to access and manage log data. Regular security administrators should not be allowed to access log files.

8.5 Security guidelines to data of application

Protection for data in this category complies with resource users' security requirements. When users do not specify particular security requirements, implement the security measures from clause 7 of [ITU-T X.1641] as a baseline, supplemented by the following additional measures.

8.5.1 Storage

In the stage of data storage, the following security measures can be used:

a) When a user's data of the same category is distributed across multiple storage resources (as illustrated in Scenario 2 of [ITU-T Y.3400]), these resources will maintain consistent security policies including: network protections, access controls, authorization mechanisms and encryption standards.

b) Regular auditing of data access activities can be used.

c) For accounts with frequent abnormal access, restrict their access permissions.

d) For applications requiring high real-time performance, data backup methods can be used to adapted based on their business continuity requirements.

8.5.2 Use

In the stage of data usage, the following security measures can be used:

a) Data access is restricted to resource owners exclusively. For other users requiring access, it is advisable to obtain explicit authorization.

b) For applications with a large number of access users, perform secondary authorization and set up administrator accounts for the applications, allowing administrators to set up and manage regular access accounts.

c) Regular audits of account access behaviour can be used. Restrict access permissions for accounts exhibiting frequent anomalous activities.