Network Working Group
Internet-Draft
Intended status: Informational
Expires: 23 April 2026

X. Si
China Telecom

20 October 2025

# Problem Statement of Zero Trust Deployment in Telecom Network Environments
draft-si-sag-zerotrust-promblem-00

## Abstract

Zero Trust, as a security paradigm, has achieved global practical consensus. However, its large-scale deployment in telecommunications network environments presents unique challenges. Operationally standards tailored to the specific requirements of telecom networks are needed.

## Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in "RFC2119" when, and only when, they appear in all capitals, as shown here.

## Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 23 April 2026.

## Copyright Notice

Table of Contents



## 1. Introduction

As a critical security paradigm addressing the limitations of traditional "perimeter-based security models," the concepts of Zero Trust and continuous dynamic trust have achieved widespread practical consensus. However, diverse industry sectors exhibit distinct business characteristics and network environments, leading to significant variations in Zero Trust implementation pathways and technical emphases: some scenarios prioritize fine-grained access control, others focus on network cloaking and attack surface reduction, while certain approaches emphasize continuous risk assessment.

To effectively realize dynamic trust solutions, the following considerations must be addressed:

1) How to mitigate bandwidth demands and latency constraints imposed by continuous validation mechanisms within Zero Trust architectures on communication processes.

2) How to accurately assess trust levels between different entities.

3) How to upgrade trust mechanisms for existing network architectures while minimizing migration costs.

## 2. Existing Mechanisms

Current Zero Trust standards such as ITU-T X.1011 and NIST SP 800-207 provide directional guidance primarily from governance frameworks and architectural principles perspectives. The former emphasizes maturity models and organizational processes for Zero Trust, while the latter focuses on the logical division of component roles. Neither standard specifically addresses the practical deployment scenarios of telecommunications cloud networks, resulting in a lack of standardized references for operators to balance security requirements with business continuity. These gaps directly hinder the large-scale advancement of Zero Trust in telecommunications cloud network environments.

## 3. Gap Analysis

Significant disparities exist between existing frameworks and engineering practices in the actual deployment of operator telecommunications networks.

1) Regarding the balance between continuous validation and communication efficiency, operator networks must support ultra-large-scale concurrent connections and low-latency sensitive services. While existing standards emphasize the necessity of "continuous validation," they fail to establish quantitative constraints on critical technical parameters such as validation frequency, session persistence mechanisms, and incremental state synchronization. This leads to potential issues in practice, including significant bandwidth redundancy, cumulative handshake latency, and state management overhead, which adversely impact the real-time performance of core services and user experience. The absence of clear baselines for "performance-security" trade-offs makes it challenging for operators to meet telecommunications-grade SLA requirements while ensuring security.

2) In terms of precise trust level assessment and cross-domain interoperability, operator services involve multiple entity types and contextual scenarios, requiring trust decisions to integrate dynamic attributes such as device fingerprints, behavioral baselines, and environmental risks. Although existing standards enumerate dimensions like "user identity, device status, and network environment," they do not define the minimal necessary attribute sets, weight distribution rules, or cross-domain standardized expression methods. This results in non-comparable trust scores across different entities and non-reusable cross-domain policies, thereby obstructing trust result mutual recognition and federated collaboration, and creating a lack of anchoring points for constructing globally consistent dynamic trust systems.

3) while existing standards encourage "phased implementation," they neither define collaborative models with traditional security technologies nor provide specific guidance for upgrade deployments, making it difficult to identify feasible paths that simultaneously address security requirements and business continuity.

## 4. Problem Statement

The primary challenges in current telecommunications network dynamic trust scenarios include:

1) Communication Efficiency and Continuous Validation Balance: Reliance on continuous validation mechanisms for multidimensional attributes such as user identity, device status, and environmental context. However, in operator-grade networks or high-real-time service scenarios, frequent identity re-authentication, policy negotiation, or encryption handshakes may introduce significant bandwidth overhead and end-to-end latency.

2) Standardization of Dynamic Trust Assessment: Evaluation dimensions and calculation models for trust levels of different entities lack unified definitions. This disparity hinders cross-domain trust transfer implementation and obstructs integration between Zero Trust and existing identity/attribute standardization components.

3) Gradual Trust Upgrade: Telecommunications infrastructure exhibits multi-layer heterogeneity with long life cycles, where comprehensive security migration incurs extremely high costs and may even pose business continuity risks. Solutions must consider achieving transition to "dynamic trust models" through standardized interfaces, compatibility protocols, and layered deployment strategies, while minimizing modifications to existing network topologies.

Addressing these challenges is essential to further extend trust mechanisms across network architectures and ensure network security.

## 5. Requirements

To ensure the interoperability, scalability, and economic feasibility of Zero Trust technologies, coordinated standardization efforts for key Zero Trust components must be advanced.

Communication Efficiency Optimization: Define low-overhead protocols supporting continuous validation;

Trust Assessment Standardization: Discuss universal measurement rules for cross-domain trust levels;

Guidelines: Propose compatibility specifications between existing network architectures and Zero Trust models.

## 6. Security Considerations

This information document introduces no any extra security problem to the Internet.

## 7. IANA Considerations

None

## Author’s Address

Xuan Si
China Telecom
Kangqiao Town, Pudong New District
Shanghai
201315
China
Email: six1@chinatelecom.cn