|  |  |  |
| --- | --- | --- |
|  | World Telecommunication Standardization Assembly (WTSA-24)New Delhi, 15–24 October 2024 |  |
|  |
|  |  |
| PLENARY MEETING | Addendum 17 toDocument 37-E |
|  | 22 September 2024 |
|  | Original: English |
|  |
| Asia-Pacific Telecommunity Member Administrations |
| PROPOSED MODIFICATION to RESOLUTION 65 |
|  |
|  |

|  |  |
| --- | --- |
| **Abstract:** | This document contains the APT common proposal for modification of WTSA Resolution 65. "Calling Party Number Delivery, Calling Line Identification and Origin Identification Information".The proposed revisions aim to enhance the comprehensive standardization efforts of ITU-T, emphasizing the urgency of combating OI/CLI spoofing. The proposed changes provide clear instructions to encourage operators/service providers to ensure the reliability and verifiability of OI information, CPN, and CLI wherever applicable, by implementing signalling security mechanisms defined in the relevant ITU-T Recommendations. This initiative aims to address spoofing and other forms of numbering misuse effectively. |
| **Contact:** | Mr. Masanori Kondo Secretary GeneralAsia-Pacific Telecommunity | E-mail: aptwtsa@apt.int |

**Introduction**

Origin Identification (OI)/Calling Line Identification (CLI) spoofing has emerged as a significant concern. This technique enables scammers to mask their phone numbers, making it appear that they are calling from a trusted source. This issue is evolving with the advancement of Artificial Intelligence (AI) technology, which is capable of generating more sophisticated and realistic-sounding voices. OI/CLI spoofing is often employed in conjunction with robocalls and scams.

Study Group 11 (SG11) of the International Telecommunication Union's Telecommunication Standardization Sector (ITU-T) has meticulously developed an extensive set of Recommendations, including ITU-T Q.3057, ITU-T Q.3062, and ITU-T Q.3063. These Recommendations delineate a uniform methodology for the integration and validation of digital certificates within the framework of signalling message exchanges. In correspondence with these developments, SG11 has also spearheaded the revision of several protocols within the Signalling System No. 7 (SS7) and BICC with Amendments 2 to ITU-T Q.931, 6 to ITU-T Q.763, and 6 to ITU-T Q.1902.3, all aimed at seamlessly embedding support for digital certificates. This multifaceted strategy is designed to be a forward-thinking solution that is equally applicable to both traditional and Internet Protocol (IP)-based network infrastructures. Throughout this developmental phase, SG11 has fostered collaborative relationships with Study Groups 2 and 17 (SG2 and SG17), from which valuable insights and constructive feedback have been garnered. Moving forward, such synergistic cooperation remains an indispensable component of future endeavours.

Furthermore, educating users on the critical importance of dependable calling party numbers equips them with the knowledge to identify legitimate callers and abstain from engaging with spoofed calls. This empowerment enables them to take proactive control of their telephone communications. When users are made aware of the intricacies of spoofing and its potential ramifications, such as financial scams, identity theft, and harassment, their awareness of the associated risks is heightened. This heightened awareness fosters a sense of vigilance regarding their personal safety and security, thereby promoting a more cautious and informed approach to telephone communication.

**Proposal**

APT Member Administrations propose to modify WTSA Resolution 65, “Calling party number delivery, calling line identification and origin identification information”.

MOD APT/37A17/1

RESOLUTION 65 (Rev. New Delhi, 2024)

Calling party number delivery, calling line identification and origin identification information

(Johannesburg, 2008; Dubai, 2012; Hammamet, 2016; Geneva, 2022; New Delhi, 2024)

The World Telecommunication Standardization Assembly (New Delhi, 2024),

concerned

*a)* that there appears to be a trend to either suppress or amend the transmission across international boundaries of calling party number (CPN), calling line identification (CLI) and origin identification (OI) information, in particular the country code and the national destination code;

*b)* that such practices have an unfavourable effect on security and economic issues, in particular for developing countries[[1]](#footnote-1)1;

*c)* that previous generation signalling protocols and telecommunication networks were designed with limited consideration for security and privacy and hence are vulnerable to attacks on ICT infrastructure including exploiting signalling protocols used for different ICT services*;*

*d)* that there is an ever growing increase of usage of spoofed CLI, SMS interception, voice cloning technologies, etc., resulting in take-over of users’ assets or personal information;

*e)* about the number of cases so far reported to the Director of the Telecommunication Standardization Bureau (TSB) on ITU‑T E.164 numbering misappropriation and misuse related to CPN non-delivery;

*f)* that work on this topic in Study Group 2 of the ITU Telecommunication Standardization Sector (ITU‑T) needs to be expedited and expanded to cater for the changing environment of service delivery and network infrastructures, including emerging telecommunications/information and communication technologies and services, such as next-generation networks and future networks,

noting

*a)* relevant ITU‑T Recommendations, in particular:

i) ITU‑T E.156: Guidelines for ITU‑T action on reported misuse of ITU‑T E.164 number resources;

ii) ITU‑T E.157: International calling party number delivery;

iii) ITU-T E.370: Service principles when public circuit switches international telecommunication networks interwork with IP-based networks;

iv) ITU‑T E.164: The international public telecommunication numbering plan;

v) ITU‑T I.251.3: Number identification supplementary services: Calling line identification presentation;

vi) ITU‑T I.251.4: Number identification supplementary services: Calling line identification restriction;

vii) ITU‑T I.251.7: Number identification supplementary services: Malicious call identification;

viii) ITU‑T Q.731.x-series, concerning stage 3 descriptions for number identification supplementary services using Signalling System No. 7;

ix) ITU‑T Q.764: Signalling System No. 7 – ISDN User Part signalling procedures;

x) ITU‑T Q.1912.5: Interworking between Session Initiation Protocol (SIP) and Bearer Independent Call Control protocol or ISDN User Part;

xi) ITU-T Q.3057: Signalling requirements and architecture for interconnection between trustable network entities;

xii) Amendment 7 to ITU-T Q.763: Extensions for the support for the calling line identification authentication;

xiii) Amendment 2 to ITU-T Q.931: Extensions for the support for the calling line identification authentication;

xiv) Amendment 6 to ITU-T Q.1902.3: Extensions for the support for the calling line identification authentication;

xv) ITU-T Q.3062: Signalling procedures and protocols for enabling interconnection between trustable network entities in support of existing and emerging networks;

xvi) ITU-T Q.3063: Signalling procedures of calling line identification authentication;

xvii) ITU-T X.509: Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks,

*b)* relevant resolutions:

i) Resolution 61 (Rev. Geneva, 2022) of this assembly, on misappropriation and misuse of international telecommunication numbering resources;

ii) Resolution 21 (Rev.  Bucharest, 2022) of the Plenipotentiary Conference, on measures concerning alternative calling procedures on international telecommunication networks;

iii) Resolution 29 (Rev. Geneva, 2022) of this assembly, on alternative calling procedures on international telecommunication networks;

*c)* No. 32 (Article 3.6) of the International Telecommunication Regulations (Dubai, 2012) (ITRs) regarding the provision of international CLI by the signatory Member States to the ITRs,

noting further

*a)* that some countries and regions have adopted national laws, directives and recommendations regarding CPN non-delivery and spoofing, and/or on ensuring confidence in OI, and that some countries have national data-protection and data-privacy laws, directives and recommendations;

*b)* that the CPN makes it possible to identify the party responsible for making the call;

*c)* that the presence of verification mechanisms for the various calling party identifiers may increase the reliability of the information transmitted;

*d)* that implementation of reference architecture specified in ITU-T Q.3057 and other relevant ITU-T Recommendations for the interconnection between trustable network entities (NEs) may ensure the trustworthiness of information transmitted over telecom network;

*e)* that digital signatures (digital certificates) used in signalling exchanges should be globally interoperable and shared trust chains;

*f)* that user should aware that CPN/OI may be spoofed,

reaffirming

that it is the sovereign right of each country to regulate its telecommunications and, as such, regulate the provision of CLI, CPN delivery and OI information, taking into account the Preamble to the ITU Constitution and the relevant provisions of the ITRs related to the provision of CLI information,

resolves

1 that international CPN delivery shall be provided on the basis of the relevant ITU‑T Recommendations;

2 that international CLI and OI delivery shall be provided on the basis of the relevant ITU-T Recommendations where technically possible;

3 that the delivered CPN should contain at least either the calling party number or the specially allocated number of the operator/service provider responsible for making the call, so that a terminating country can identify the operator/service provider of the outgoing call, or identify the terminal that originates the call, before it is delivered from the originating country to that terminating country;

4 that the delivered CPN and the CLI, if delivered, shall include sufficient information to allow proper billing and accounting, for each international call;

5 that the OI information in a heterogeneous networking environment shall, where technically possible, be an identifier assigned to a subscriber by the originating service provider, or be replaced by a default identifier by the originating provider to identify the origin of the call, if specified by the administration;

6 that the CPN, CLI and OI information shall be transmitted transparently by transit networks (including hubs);

7 to encourage operators/service providers to make OI information, wherever applicable, CPN and CLI reliable and verifiable in order to combat spoofing and other forms of numbering misuse;

8 that ITU-T should further study registration procedures for the issuing of digital certificates to the authorized service providers by the Trusted Signalling Certification Authority (TSCA) including appointment of TSCA;

9 to encourage all stakeholders to make efforts for early implementation of trust framework and signalling security mechanisms specified in Recommendation ITU-T Q.3057 and other relevant ITU-T Recommendations,

instructs

1 ITU‑T Study Group 2, ITU‑T Study Group 3 and, where required, ITU‑T Study Groups 11 and 17 to strengthen cooperation and further study the emerging issues of CPN delivery, CLI and OI information, in particular for a heterogeneous networking environment, including security methods and possible validation techniques;

2 the study groups concerned to expedite work on Recommendations that would provide additional detail and guidance for the implementation of this resolution,

instructs the Director of the Telecommunication Standardization Bureau

1 to report on the progress achieved by the study groups in implementing this resolution, which is intended to improve security and minimize fraud, and minimize technical harm as called for by Article 42 of the Constitution;

2 to share information on country experiences regarding the implementation of this resolution, in a centralized location,

invites Member States, Sector Members, Associate Members and Academia

1 to contribute to this work, to share information regarding their experiences in implementing this resolution and to cooperate in the implementation of this resolution;

2 to consider developing, within their national regulatory and legal frameworks, guidelines or other means for implementing this resolution;

3 to collaborate on public awareness campaigns aimed at educating users about spoofing tactics and the importance of verifying CPN.

1. 1 These include the least developed countries, small island developing states, landlocked developing countries and countries with economies in transition. [↑](#footnote-ref-1)