Overview of ITU activities on combating telephone fraud using public-key certificates

Denis ANDREEV
Advisor of ITU-T SG11, TSB/ITU
https://linkedin.com/in/denis-andreev-ict

KEY ATTACKS SCENARIOS ON FIXED AND MOBILE NETWORKS (MOST POPULAR SCENARIOS)

Spoofed CLI used for different attacks (e.g. robocalls, telephone spam, AI-based calls, etc.)

Fake Calling Line Identification presentation

Bad actor

+41 22 xxx-xx-xx
Pretending legitimate entity (e.g. Banks, Police, etc.).

Telephone subscriber

SCENARIO 1

It is also used for password recovery on different Internet resources (e.g. PayPal, etc.)

Bank

SMS
Intercepting SMS with one-time-password (OTP)

Bad actor

X

Bank's application

See YouTube

SCENARIO 2

Customer has no information about this attack

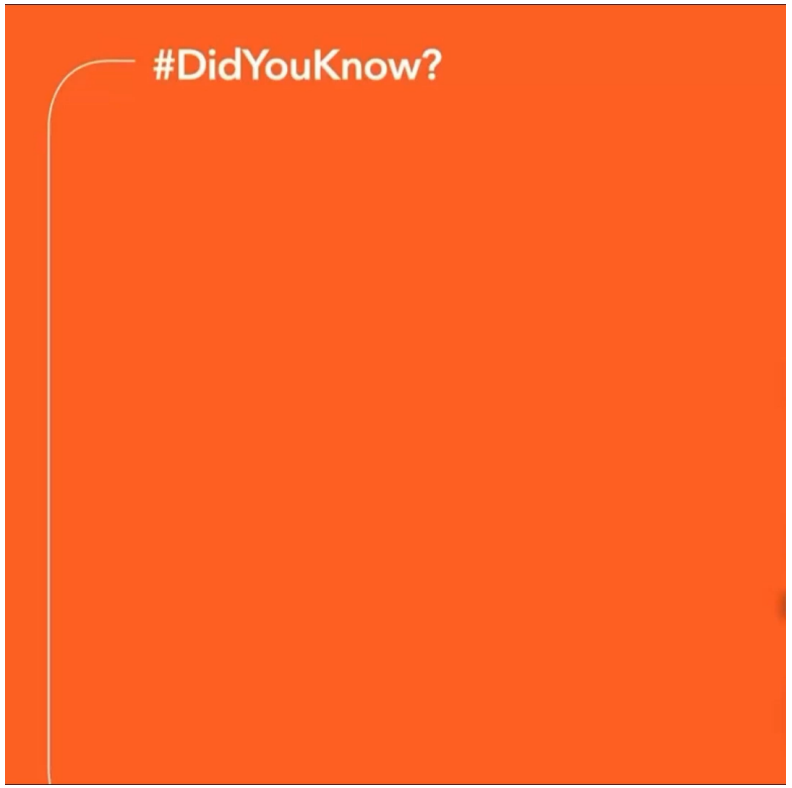
Demo: SMS OTP Intercept*

* Ref: 2019: ITU Workshop - Brainstorming session on SS7 vulnerabilities

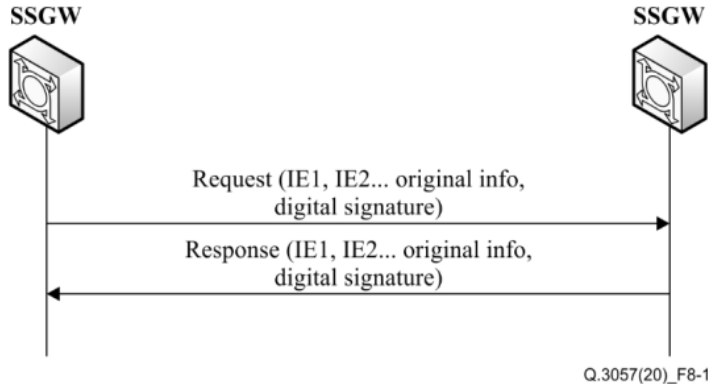
Combating scam calls, robocalls, number spoofing

ITU develops set of standards for signing the Calling Line Identification (CLI) by digital public-key certificates (ITU-T X.509) at the signalling level which enhance the reliability and trustworthiness of voice communications

YouTube



https://itu.int/go/SIG-SECURITY



Trusted Signalling Certification Authority (TSCA) as a new network element which issues trusted digital certificates (ITU-T X.509) to each operator's Signalling Security Gateway (SSGW). **The SSGW** is in charge of validating the signatures of other operator's certificates and allowing or blocking the signalling packets.

ITU-T

TELECOMMUNICATION STANDARDIZATION SECTOR OF ITU

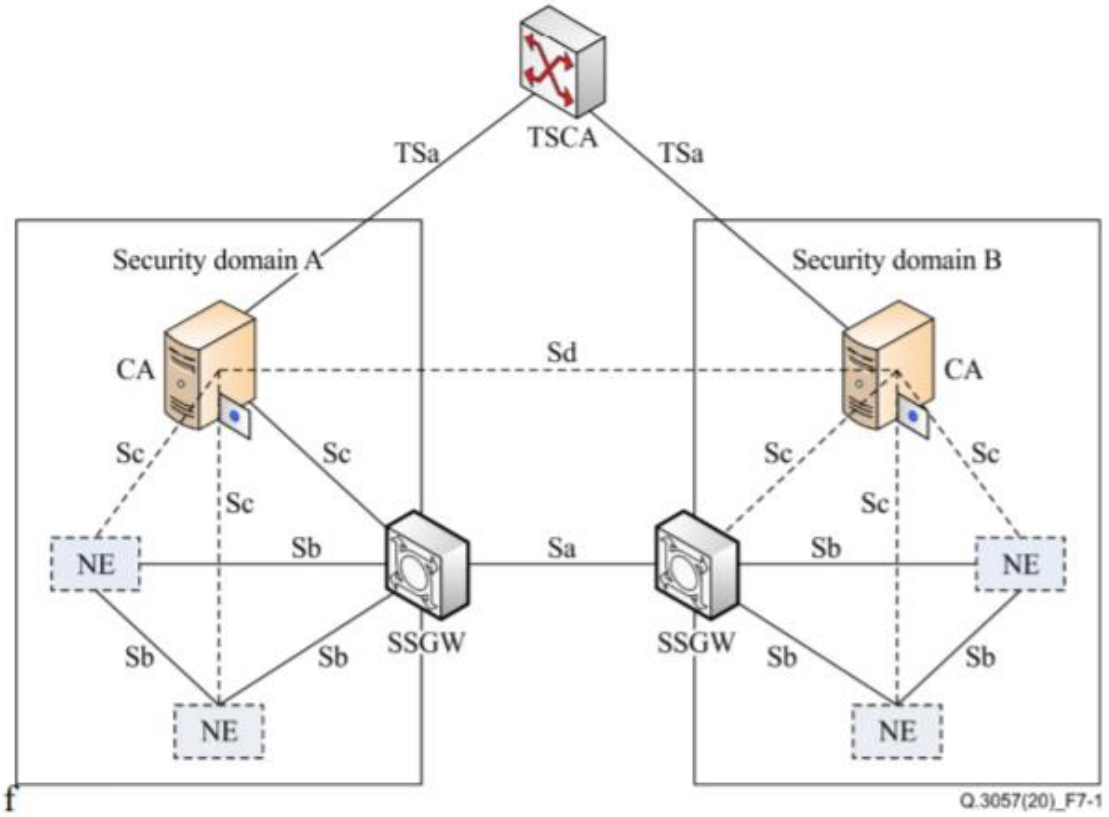
Q.3057

(04/2020)

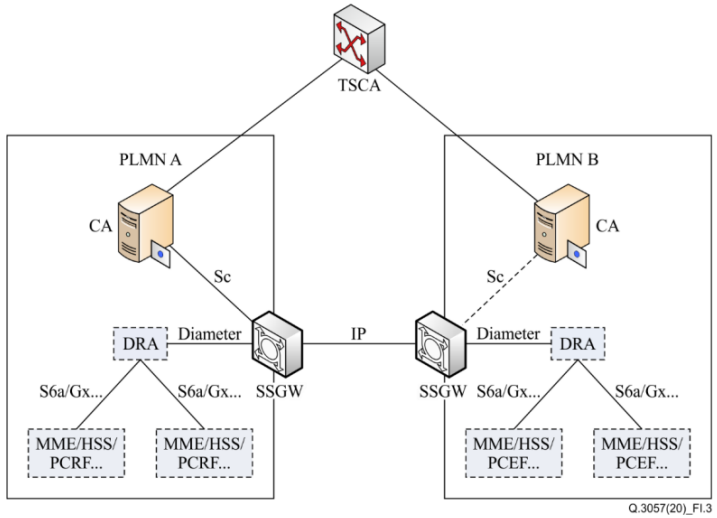
SERIES Q: SWITCHING AND SIGNALLING, AND ASSOCIATED MEASUREMENTS AND TESTS

Signalling requirements and protocols for the NGN – Network signalling and control functional architecture

Signalling requirements and architecture for interconnection between trustable network entities

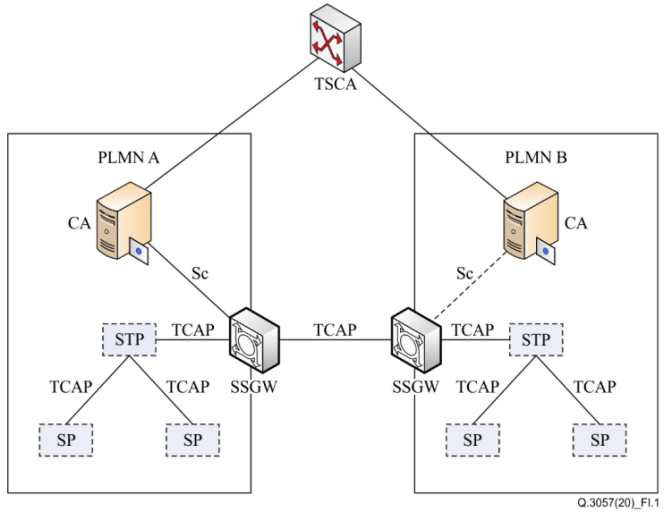


Applications



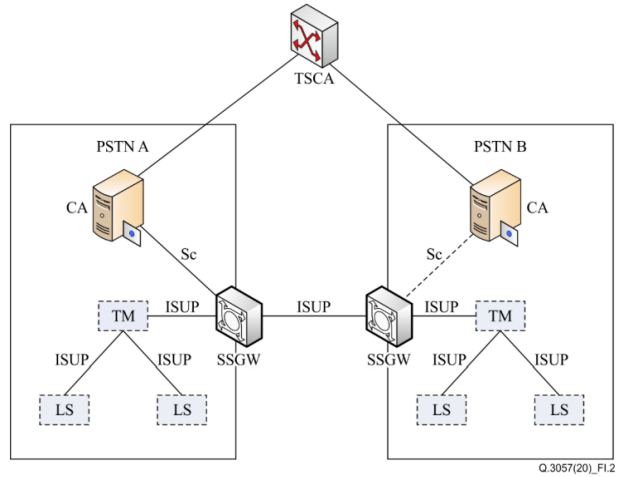
Security Diameter transaction architecture

(Ref. ITU-T Q.3057)



Security TCAP transaction architecture

(Ref. ITU-T Q.3057)



CLI transit architecture

(Ref. ITU-T Q.3057)

Key Q/A of ITU webinar

Note: excerpt from Q/A transcript, ITU webinar, November 2022

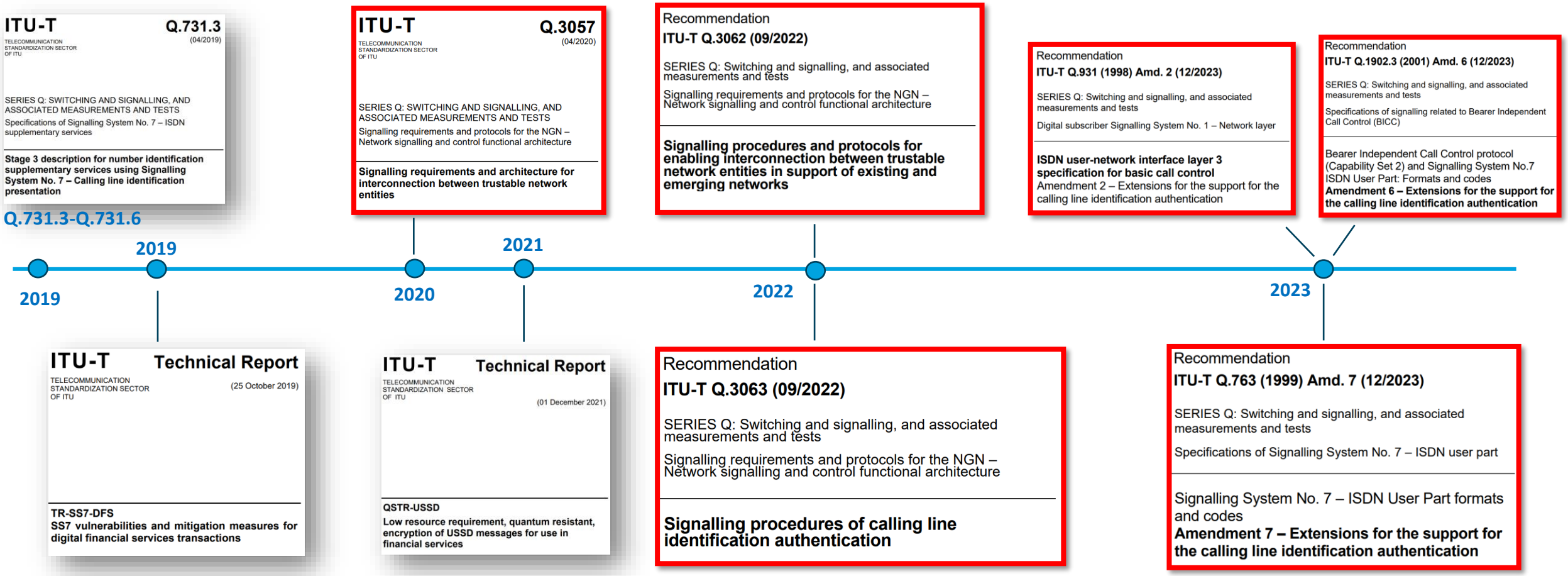
Questions transcript provided by moderator

ITU Webinar Series on Signalling Security:
Episode 2: "Securing legacy telecom network services"

7 November 2022

#	Question	Answer
1.	Are there CLI authentication protocols other than STIR/SHAKEN?	The STIR/SHAKEN are basically frameworks for operator authentication but it is not Calling Line Identification (CLI). In general, STIR/SHAKEN does not authenticate the subscriber's phone number while it authenticates the operator on the network. STIR/SHAKEN was designed for VoIP protocols which are widely used over 4G, 5G, etc. However, STIR/SHAKEN is not applicable for legacy networks such as (2G and 3G) which are switched based networks. Those networks utilize different protocols on signalling and payload (audio channel) levels. In this regard, ITU-T SG11 developed number of standards (ITU-T Q.3057, Q.3062 and Q.3063) which define approach on incorporating digital signature (digital certificate) into signalling exchange. This approach might be considered as equivalent to STIR/SHAKEN but can be used on existing and legacy networks as it is applicable to wide number of protocols including SS7, DIAMETER, SIP, etc. STIR/SHAKEN and ITU-T approaches use the same authentication or cryptography scheme, but ITU-T standards define the details on how digitally sign the phone number in signalling exchange.
2.	Do you think that STIR/SHAKEN will be widely deployed outside the US and Canada as a counter-measure to caller ID spoofing? If so, who would provide the global director of certification authorities? Could ITU do that? Regarding your slide 25, Trust Model, could the ITU be the trust anchor?	The deployment of such solutions (STIR/SHAKEN or ITU-based solution) depends on the willingness of the countries. Any country may deploy it locally following implementation of relevant legislation and regulation mechanisms. Some countries may have bilateral agreement on such implementations. As example US and Canada agreed to deploy STIR/SHAKEN together. However, for solving problem on the global level, international deployment is needed and ITU may play a lead role as authority which may provide such globally recognized digital certificates all over the world. Those certificates might be used in all similar solutions such as STIR/SHAKEN or ITU-T Q.3057, ITU-T Q.3062 and ITU-T Q.3063. The global deployment of such solutions may can be interoperable and may mitigate the number of different attacks on existing and legacy networks. In other words, the trust anchor for the trust model for those tokens definitely can be ITU as UN specialized agency which is responsible for International Numbering Resources and it is globally trusted organization.
3.	What is the way forward for implementation of ITU-T Recommendations ITU-T Q.3057, ITU-T Q.3062 and ITU-T Q.3063 which define the usage of digital signatures in the signalling exchange?	In terms of ITU-T SG11, in terms of the technical standards, ITU-T SG11 developed the basic principles and protocols that are required to deploy such solution. Now, ITU-T SG2 may start working on operational procedures and define on how operators may apply for security tokens, where the trusted root is set out and other relevant issues.

ITU-T Recommendations and Technical Reports (in force)



ITU-T Workshops and Webinars

2016 [ITU Workshop on “SS7 Security"]

2019

[ITU Brainstorming session on SS7 vulnerabilities and the impact on different industries including digital financial services]

2024

[Preventing fraud using Secure Telephony Signalling Framework]

2021

https://itu.int/go/WS-SSP

2022

https://itu.int/go/WB-SSP-01

https://itu.int/go/WB-SSP-02

Key takeaways:

“

…

- The **trust anchor needs to be a globally trusted SDO**, **preferably one already in charge of numbering** and this anchor must interoperate with existing repositories (such as the ones in the US and Canada).

…”

Ref.: https://www.itu.int/en/ITU-T/Workshops-and-Seminars/2021/1129/Pages/default.aspx

Resolution 65 – Calling party number delivery, calling line identification and origin identification information (WTSA-24)

Noting further

…

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

d) that the implementation of the reference architecture specified in Recommendation **ITU-T Q.3057** and other relevant ITU-T Recommendations for the interconnection between trustable network entities **may ensure the security of signalling information transmitted over telecommunication networks**;

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

Instructs

…

2 **ITU-T Study Group 2**, in close collaboration with **ITU-T Study Group 11**, **to develop, deploy and maintain a procedure, in accordance with ITU-T Recommendations, for selecting registration authorities**, including the selection of trusted signalling certification authorities**, to support the allocation of digital public certificates to be used in the signalling exchange** of telecommunication networks;

invites Member States, Sector Members and Associate Members

…

3 **to encourage service providers to utilize public-key certificates (e.g. ITU-T X.509) in order to sign CLI** and other information in the signalling exchange;

4 to encourage all stakeholders to make efforts towards the **early implementation** of the trust framework and **signalling security mechanisms specified in Recommendation ITU-T Q.3057** and other relevant ITU-T Recommendations;

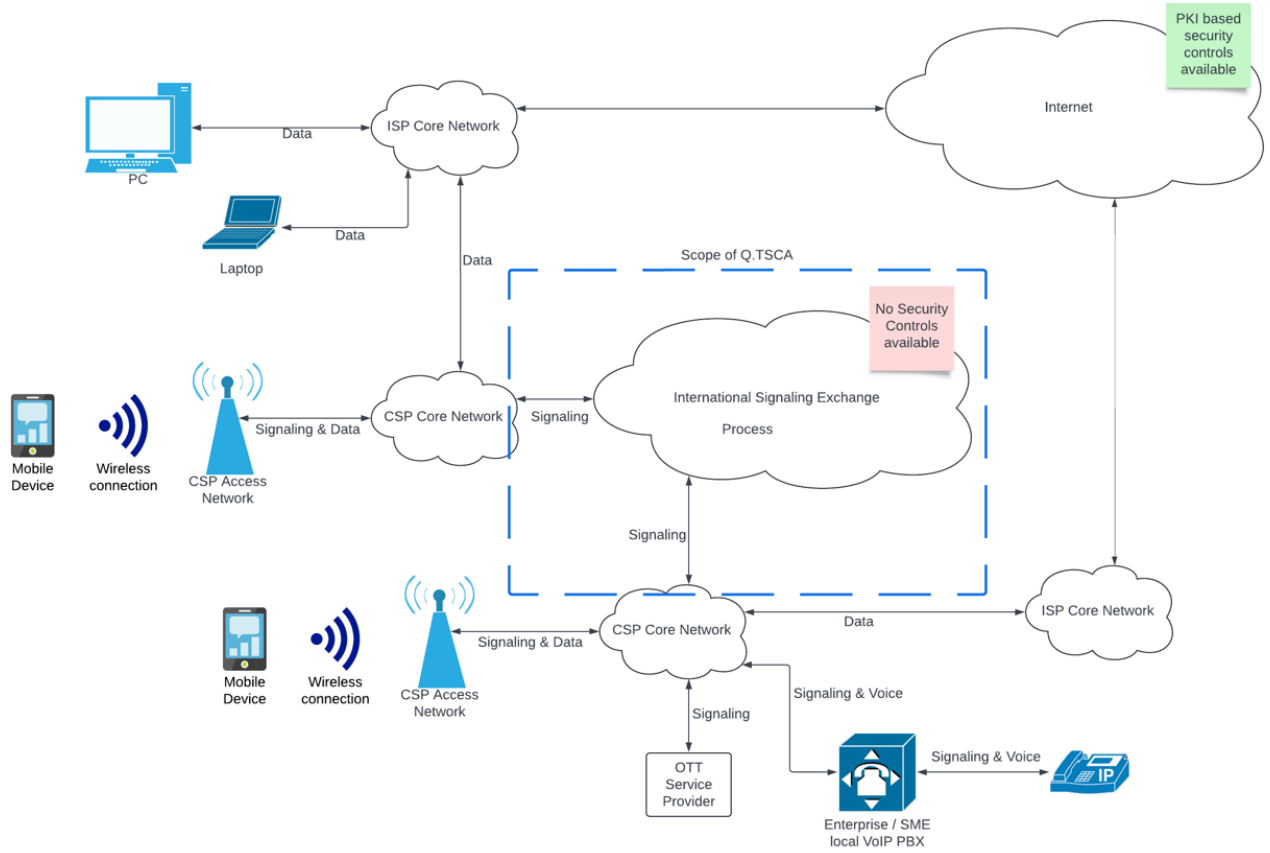
Ongoing work

Draft Q.TSCA

Requirements for issuing End-Entity and Certification Authority certificates for enabling trustable signalling interconnection between network entities

It specifies the **requirements for the verification of information elements in certificate signing requests** and the allocation of End-Entity and CA public-key certificates for telecom security within the international signalling exchange networks in support of existing and emerging networks, **in continuation of the previous work done in ITU-T Q.3057, ITU-T Q.3062 and ITU-T Q.3063**.

Assignment of roles to entities, determination of the trust chain structure and the definition of operational procedure are not in the scope of this Recommendation.



(Ref. draft Output Q.TSCA, February 2025)

ITU-T SG2 activities

ITU-T E.RAA4Q.TSCA
Registration Authority Assignment criteria to issue digital public certificates for use by Q.TSCA

Summary

This recommendation is intended to provide a consistent and transparent means by which registration authorities will be selected for the purpose of the issuance of certificates to facilitate trust in secure signalling of telephone numbers.

Scope

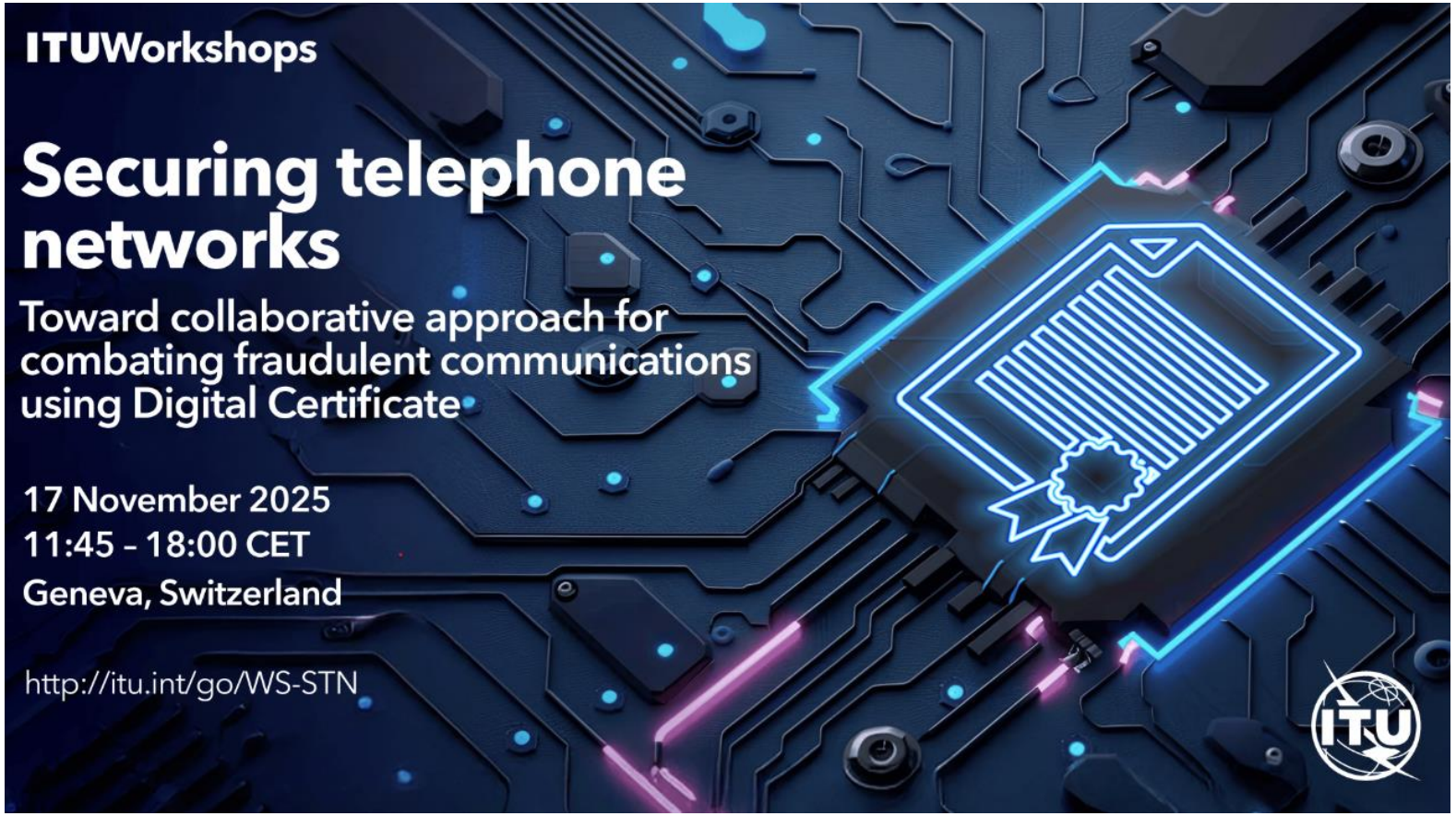
ITU-T E. Registration Authority Assignments (E.RAA) defines the criteria for the selection of registration authorities, and the process by which the Director of TSB will utilise the criteria to select registration authorities to support the allocation of ITU-T X.509 digital public-key certificates that will facilitate secure signalling of telephone numbers

Ref. SG2-TD280-R1/PLEN, August 2025

Upcoming ITU Workshop

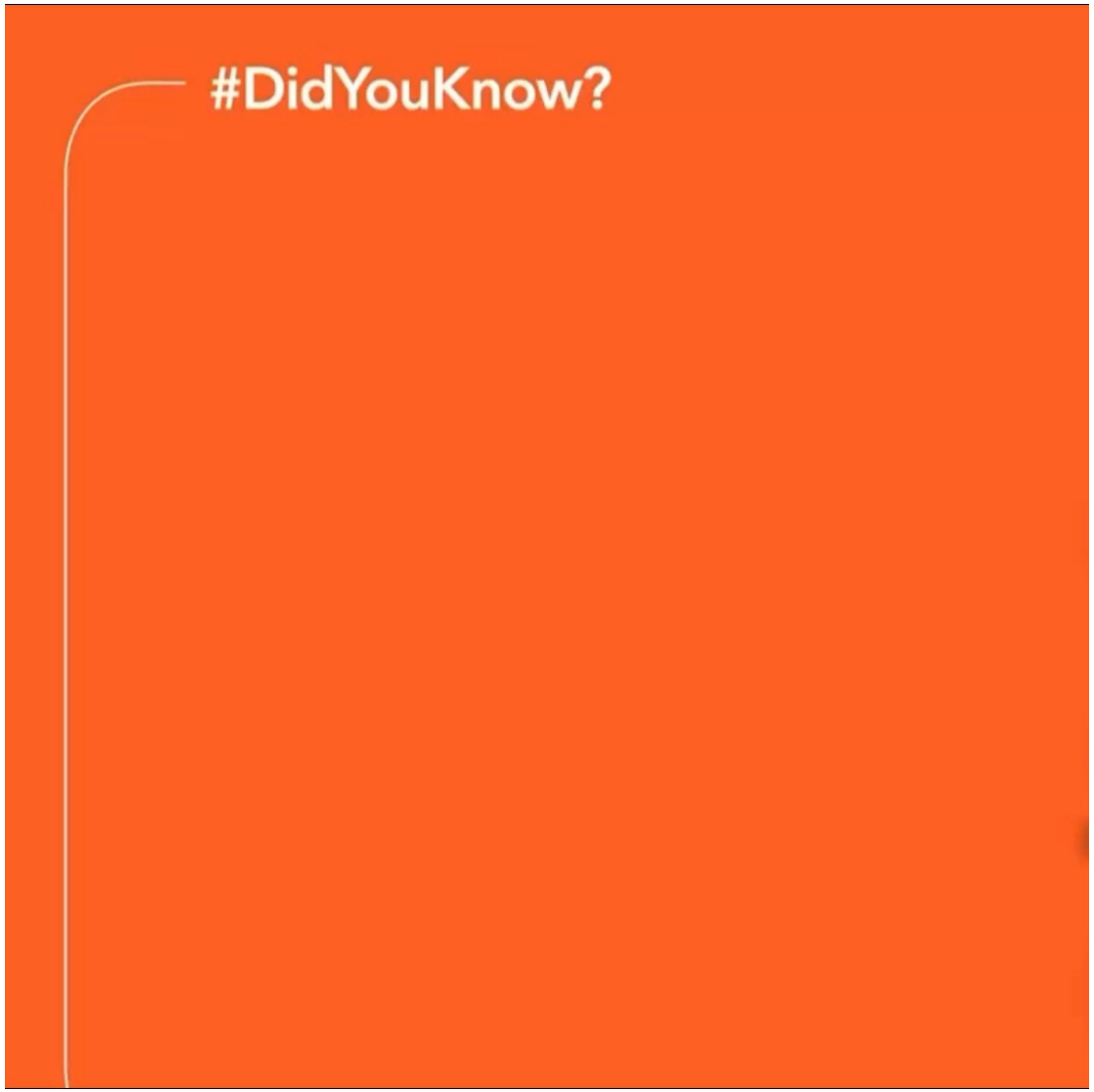
OBJECTIVES

- **Raise awareness** of the growing threats posed by fraudulent communications.
- **Present current ITU initiatives related to digital public-key certificates for authenticating CLI.**
- **Facilitate international collaboration** among stakeholders to address this global issue.



CONCLUSION

- This approach can be deployed globally issuing digital certificates to be recognized by all operators (**scalable solution**)
- **ITU-T SG11 completed the required protocol-related part** and working on requirements for verification of information elements in certificate signing requests (Q.TSCA)
- **ITU-T SG2 is developing Registration Authority Assignment criteria to issue digital public certificates for use by Q.TSCA**
- **ITU organizes workshop "Securing Telephone Networks: Toward collaborative approach for combating fraudulent communications using Digital Certificate"** to be held in Geneva on 17 November 2025 b2b with SG11 meeting (17-26 November 2025)



CONTACTS

Denis ANDREEV
Advisor of ITU-T SG11, TSB/ITU

denis.andreev@itu.int
tsbsg11@itu.int

https://itu.int/go/SIG-SECURITY
https://itu.int/go/tsg11
https://linkedin.com/in/denis-andreev-ict