

Draft Framework of Proof of Concept

Signalling security and certificate-based calling line identification authentication

ITU Roundtable “Implementing ITU Standards for Combating Fraudulent Communications”, 9 October 2026, New Delhi, India

<https://itu.int/go/RT-CFC>

Moderator: Assaf Klinger, Vaulto Technologies

1 Summary

This document describes a draft of indicative framework of a Proof of Concept (PoC) on certificate-based authentication of calling line identification (CLI), based on Recommendations ITU-T Q.3057, ITU-T Q.3062 and ITU-T Q.3063, the associated protocol amendments, and determined draft new Recommendation ITU-T Q.3070.

The aim of this document is to introduce the indicative framework aligned with ITU-T guidelines which may be useful for information and discussion with the stakeholders at the ITU Roundtable “Signalling security and certificate-based calling line identification authentication” (New Delhi, India) on 9 October 2026.

The PoC can be based on two complementary tracks:

- **Track A — certificate-based calling line identification authentication.** Implementation and execution of defined test scenarios, including between independently developed implementations, against procedures that are specified at clause level in Recommendations in force or determined. The purpose is to produce interoperability evidence, measurements of operational impact, and a record of the questions that implementation raises.
- **Track B — signalling security gateway capability.** Demonstration of detection and mitigation capability against the threat categories and mitigation framework of Recommendation ITU-T Q.3066, and structured capture of what implementations do. The purpose is to establish, from implementation evidence, the material from which detailed signalling security gateway requirements and associated test specifications can be developed. Detailed requirements for the signalling security gateway have not yet been developed, and Track B does not assess conformance.

ITU-T Q.3066 identifies authenticity validation of signalling messages as one of the four pillars of its mitigation framework, and Track A specifies the mechanism by which that validation is performed; one scenario exercises the junction between them directly.

2 Background

Calling line identification spoofing continues to enable fraud at scale, and to defeat mitigation measures that depend on the identity presented with a call being reliable. ITU-T Study Group 11 has developed a set of standards which apply digital public-key certificates to the international signalling interconnect environment:

- **[ITU-T Q.3057] (2020)** specifies the architecture, the functional entities and the reference points, and establishes the trusted signalling certification authority as trust anchor.
- **[ITU-T Q.3062] (2022)** specifies the signalling procedures and protocols, including the security association, the structure of protected messages and the digital signature algorithms.
- **[ITU-T Q.3063] (2022), with Corrigendum 1 (2023)** specifies the architecture and procedures of calling line identification authentication: certificate generating, call request initiating and certificate verification, together with the corresponding presentation procedures.
- **[ITU-T Q.763] Amendment 7, [ITU-T Q.931] Amendment 2 and [ITU-T Q.1902.3] Amendment (2023)** specify the protocol extensions carrying the certificate, the signature and the authentication result.
- **Draft new Recommendation [ITU-T Q.3070] (ex Q.TSCA)**, determined by ITU-T Study Group 11 at its meeting in Geneva, 14–22 July 2026, specifies the requirements for verification of information elements in

certificate signing requests, the issuance of end-entity and certification authority certificates, and the cross-border trust anchor certificate list.

- **Draft Recommendation [ITU-T E.1122]**, determined by ITU-T Study Group 2, specifies the complementary governance framework for the registration authority anchor and for cross-border sharing of trust anchor certificate information.

The specification base is therefore substantially established. What is missing is deployment experience: implementations that have been exercised against one another, measurements of the operational effect, and the practical knowledge that only implementation produces. Standardization work in this area — in particular the development of test specifications and the finalization of the Recommendations still in progress — depends on that experience.

Because the framework is specified in ITU-T Recommendations rather than in a regional scheme, the same certificates, procedures and protocol parameters apply in any jurisdiction that adopts it, and the cross-border trust mechanism is designed so that adoption in one jurisdiction extends the reach of adoption in another. An implementation developed for this proof of concept is therefore applicable wherever the framework is taken up.

[ITU-T A Suppl. 2] records that proof-of-concept activity is used by standards development organizations to determine the feasibility of a concept, technology or solution, or to verify that it functions as intended and in accordance with the features defined in standards under development, and that this may significantly help ITU standardization activities to understand whether a solution is viable and to advance the work items under study. That is precisely the position here.

3 PoC description

Under **Track A**, the following points need to be verified:

- 1) **Implementations** of one or more of the functions defined by the framework — originating and terminating signalling security gateway, certification authority, trusted signalling certification authority, registration authority functions, and supporting network entity or test functions;
- 2) **Execution of the defined test scenarios**, individually and, importantly, between independently developed implementations;
- 3) **Reported results**, including negative and inconclusive results, and including the choices implementers made where the Recommendations do not determine them;

Under **Track B**, the following points need to be verified:

- 1) **Demonstration of signalling security gateway capability** against the four threat categories classified in ITU-T Q.3066 — single-request, multi-request within a single protocol, multi-protocol, and cross-generational — across SS7, Diameter, GTP, SIP and 5G environments;
- 2) **A structured description of what the implementation does**, covering the detection methods applied, the mitigation pillars supported, and the assets protected, so that returns from different participants can be read together;
- 3) **Proposed requirement material** — for each capability described, what the implementer considers the corresponding requirement should say. This is the principal output of Track B and the reason it is being run;

And under both tracks:

- 1) **Sponsoring administrations and regulators** willing to support the activity in their jurisdiction, including by arranging test trust anchor or registration authority functions or by making test numbering resources available;
- 2) **Test laboratory and academic participation** providing environments, traffic generation, capture and measurement.

Proposals for Track B are not required to identify an interoperability partner, and no conformance statement of any kind results from participation in either track.

4 Scope

4.1 Track A — certificate-based calling line identification authentication

Track A covers certificate-based authentication of calling line identification between security domains, and the certificate and trust-distribution mechanisms on which it depends. In summary, this comprises:

- issuance of end-entity and certification authority certificates, including verification of the information elements in certificate signing requests, and the transition from a provisional to a validated end-entity certificate;
- construction and validation of certification paths under a trust anchor, within and across security domains;
- establishment of security associations between signalling security gateways and construction of protected messages;
- the calling line identification authentication procedures — certificate generating, call request initiating and certificate verification — and the associated presentation procedures;
- encoding, transport and validation of the ISUP certificate, signature and authentication indicator parameters, and behaviour of intermediate exchanges on receipt of them;
- certificate lifecycle handling, including renewal and revocation;
- submission, distribution and validation of the cross-border trust anchor certificate list, and cross-jurisdiction certification path validation using it;
- interoperability between independently developed implementations of the above.

4.2 Track B — signalling security gateway capability

Track B covers the capability of a signalling security gateway to detect and mitigate signalling attacks, described against the framework of Recommendation ITU-T Q.3066. In summary, this comprises:

- the deployment position of the gateway and the interfaces and protocols it covers;
- detection across the four categories of signalling attack classified in ITU-T Q.3066;
- the detection methods applied — unauthenticated message detection, allow-list enforcement, heuristic analysis, anomaly detection and cross-protocol consistency checking;
- coverage of the four pillars of the ITU-T Q.3066 mitigation framework, and the actions applied per security domain;
- protection of the assets classified in ITU-T Q.3066;
- the junction with Track A — consumption of a signature validation result as an input to detection and to policy, and behaviour where deployment among interconnect partners is partial;
- operational characteristics under load, and failure behaviour;
- structured capture of what the implementer considers the corresponding requirement should say.

4.3 Out of scope

Out of scope in both tracks are: conformance assessment of a signalling security gateway against detailed requirements, which do not yet exist; governance, designation, licensing or audit of certification and registration authorities; regulatory, policy, legal and commercial questions; certification of any kind; and any use of live subscriber traffic or personal data. Track A does not extend to protection of signalling other than that carrying calling line identification; Track B is not so limited, since the ITU-T Q.3066 threat model is not confined to calling line identification.

Participants that also operate session initiation protocol environments may, on a voluntary basis, exercise interworking with a SIP domain and report the results as input to the ongoing work on draft Recommendations [ITU-T Q.CSSIWF] and [ITU-T Q.SSP4SIP].

The complete scope, the functional requirements and the full scenario definitions for both tracks are to be developed in other documents.

5 Who may participate, and in what role

Because the activity is conducted outside ITU-T, participation is **not restricted to the ITU membership**. Any entity will be able to take part — ITU Member States, Sector Members, Associates and Academic Institutions, and equally entities that are not members of ITU.

Role	Suited to	What it involves
Administration or regulator	Member States; national regulatory authorities	Supporting the activity in the jurisdiction; where feasible, arranging test trust anchor or registration authority functions and test numbering resources; receiving the results
Implementing participant, Track A	Operators and communications service providers; equipment and software suppliers; certification authority and trust service providers	Contributing one or more functions; executing the applicable scenarios; pairing with at least one independently developed implementation; reporting results
Implementing participant, Track B	Suppliers of signalling security gateways, signalling firewalls and related systems; operators running such systems	Demonstrating detection and mitigation capability against the ITU-T Q.3066 framework; describing that capability in the common structure; returning proposed requirement material. No interoperability partner is required
Test laboratory or academic participant	Test laboratories; research institutions; universities	Providing test environments, traffic generation, capture and measurement; executing scenarios on behalf of a pairing
Observer	Any eligible entity	Receiving interim and final reports; no implementation contributed; not named in the results

6 What participation involves

Participants contributing an implementation are invited to:

- 1) inform Study Group 11 what they intend to do, stating the track or tracks, the functions to be contributed, and the Recommendations and clauses concerned;
- 2) prepare a short implementation description before beginning, so that the results can be interpreted;
- 3) execute the scenarios they have chosen and record the results, including negative and inconclusive results;
- 4) in Track A, exercise its implementation against at least one independently developed implementation; in Track B, return proposed requirement material for each capability described;
- 5) take part in coordination among the participants, at whatever frequency the participants themselves agree; and
- 6) share the results with ITU-T Study Group 11, on the basis described at clauses 8.6 and 10.

None of this is a condition of participation, and nothing here is enforceable by ITU-T. They are the things that make the activity useful to the participants and to the study group alike.

7 Phases and indicative timeline

Timings are indicative and expressed relative to the issuance of the Call of PoC (T0).

Phase	Indicative period	What happens
0 — Announcement and registration	T0 to T0 + 3 months	Notifications received; participants, tracks and roles confirmed

Phase	Indicative period	What happens
1 — Scoping and test plan consolidation	T0 + 2 to T0 + 4 months	Scenario set confirmed for each track; interoperability pairings agreed; test trust arrangement established; Track B demonstration profiles agreed
2 — Certificate issuance and trust establishment (<i>A</i>); capability demonstration (<i>B</i>)	T0 + 4 to T0 + 7 months	Track A: certificate issuance and certification path scenarios. Track B: deployment declaration and detection across the four threat categories
3 — Protected signalling and CLI authentication (<i>A</i>); mitigation and requirements capture (<i>B</i>)	T0 + 6 to T0 + 11 months	Track A: protected signalling and CLI authentication scenarios; measurements. Track B: mitigation coverage, the junction with Track A, operational characteristics, requirements capture
4 — Cross-border trust distribution and multi-party operation	T0 + 10 to T0 + 15 months	Cross-border trust anchor list scenarios; multi-party and robustness scenarios
5 — Consolidation and standardization feedback	T0 + 14 to T0 + 17 months	Results consolidated across both tracks; report and contributions prepared, including the material from which detailed signalling security gateway requirements could be developed

Interim findings are reported to each ordinary ITU-T Study Group 11 meeting occurring during the period, so that they reach the study group as they arise. The phases are indicative and are a matter for the participants; a participant may join at any point.

8 What ITU-T asks in return

The Guidelines identify the information that is most useful to share. Participants are invited to cover, so far as they are able:

- the results of the activity;
- how it was performed — a description of the activity, the testing or PoC methods used, the test equipment, the schedule, and who coordinated it;
- where it has been, or is going to be, conducted;
- how the results should be handled in order to submit contributions that advance ongoing work items and improve the quality of the Recommendations;
- any other activity identified in the same area, and the scope for cooperation and work-sharing with it.

The report template published with the PoC description is arranged to cover these points, so that a completed report can serve as the basis of a contribution with little further work.

9 What the results will be used for

- A consolidated PoC report submitted to ITU-T Study Group 11.
- A record of implementation questions and divergent interpretations, as the basis for considering corrigenda or amendments to the Recommendations concerned.
- Input to the draft Supplement providing an implementation guideline framework.
- Candidate input to work on test specifications for certificate-based calling line identification authentication.
- From Track B: a consolidated picture of what deployed and available signalling security gateways detect and mitigate, described against the ITU-T Q.3066 framework, and the proposed requirement material returned by participants — together forming the evidence base for a new work item on detailed signalling security gateway requirements and associated test specifications.
- A published summary of results.

10 References

Reference	Title
ITU-T A Suppl. 2 (2022)	Guidelines on interoperability experiments and proof-of-concept events — the basis on which this activity is conducted
ITU-T Q.3057 (2020)	Signalling requirements and architecture for interconnection between trustable network entities
ITU-T Q.3062 (2022)	Signalling procedures and protocols for enabling interconnection between trustable network entities in support of existing and emerging networks
ITU-T Q.3063 (2022), Cor. 1 (2023)	Signalling procedures of calling line identification authentication
ITU-T Q.763 (1999) Amd. 7 (2023)	Extensions for the support for the calling line identification authentication
ITU-T Q.931 (1998) Amd. 2 (2023); ITU-T Q.1902.3 Amd. (2023)	Extensions for the support for the calling line identification authentication
ITU-T Q.731.3 (2019)	Calling line identification presentation
draft ITU-T Q.3070 (ex Q.TSCA)	Requirements for issuing end-entity and certification authority certificates for enabling trustable signalling interconnection between network entities — determined, SG11, Geneva, 14–22 July 2026
draft ITU-T E.1122 (ex E.RAA4Q.TSCA)	A Registration Authority Anchor for the purposes of supporting secure signalling – determined, SG2, Geneva, 9-11 September 2026
ITU-T Q.3066 (2026)	Principles for detection and mitigation of signalling attacks in telecommunication networks
ITU-T X.509 (2019)	The Directory: public-key and attribute certificate frameworks
ITU-T QSTR-SS7-DFS (2019)	SS7 vulnerabilities and mitigation measures for digital financial services transactions

Further information on ITU-T activities on signalling security is available at <https://itu.int/go/SIG-SECURITY>. Information on ITU-T Study Group 11 is available at <https://itu.int/go/tsg11>.

Annex A —Indicative Notification of intent and PoC outline which may be used by ITU-T SG11

Annex A contains draft application form to be completed by PoC participants.

A.1 PoC team

Field	Response
PoC project name	
Lead entity — name and country	
ITU membership category (Member State / Sector Member / Associate / Academia / other)	
Main point of contact — name, role, electronic mail address	
Coordinator of the activity — name and entity, where different from the point of contact	
Where the activity will be conducted — location or locations, and whether laboratory, pre-production or distributed	

Field	Response
Operator or communications service provider participants	
Supplier participants	
Certification authority or trust service provider participants	
Test laboratory or academic participants	
Sponsoring administration or regulator, where applicable	
Additional participants	

A.2 PoC goals

State each goal the team intends to achieve and the Recommendation and clause to which it maps. At least one goal is required.

#	Goal	Recommendation and clause addressed
1		
2		
3		

A.3 Role, functions and scenarios

Field	Response
Track or tracks (A / B / both)	
Role sought (sponsoring administration or regulator / implementing participant / test laboratory or academic participant / observer)	
Functions to be contributed F1 originating gateway · F2 terminating gateway · F3 certification authority · F4 trusted signalling certification authority · F5 registration authority functions · F6 network entity or exchange emulation · F7 test and measurement · F8 signalling security gateway detection and mitigation (Track B)	
Scenario groups to be executed <i>Track A:</i> A certificate issuance · B protected signalling · C CLI authentication · D cross-border trust distribution · E robustness and interoperability <i>Track B:</i> F signalling security gateway capability (F1–F9)	
Signalling environments available (ISUP / DSS1 / BICC / other)	
SIP environment available for the optional exploratory activity (yes / no)	
Intended interoperability partner, or request to be paired by the coordination (<i>Track A only</i>)	
Attack traffic profiles intended for the group F demonstrations (<i>Track B only</i>)	
Test environment (laboratory / pre-production) and connectivity arrangement intended	
Test numbering resources available, and their source	

A.4 Implementation description

Field	Response
Recommendations and clauses to be implemented, or — in Track B — the clauses of ITU-T Q.3057 and ITU-T Q.3066 against which capability will be described	
Options selected where the Recommendations offer a choice	
Signature algorithm and hash function selected, and the basis for the selection	
Certificate profile and representation to be used	
Known limitations, or clauses not implemented	
Equipment and software, with versions	

A.5 Timeline

Milestone	Target date
Activity start	
<i>Track A</i> : certificate issuance and trust establishment scenarios complete	
<i>Track A</i> : first interoperability exercise with an independently developed implementation	
<i>Track A</i> : protected signalling and CLI authentication scenarios complete	
<i>Track A</i> : cross-border trust distribution scenarios complete, where applicable	
<i>Track B</i> : detection scenarios F1 to F5 complete	
<i>Track B</i> : mitigation, junction and operational scenarios F6 to F8 complete	
<i>Track B</i> : requirements capture return under F9	
Interim report	
Final PoC report	

A.6 Additional information (optional)

Field	Response
Constraints affecting participation (connectivity, numbering resources, scheduling, other)	
Attributed reporting agreed in principle? (yes / no — reporting without attribution requested)	
Expected contribution to ITU-T work	
Other activity known to you in the same area, and any scope for cooperation or work-sharing with it	
Any other information	