

Proof of Concept Framework

Signalling security and certificate-based calling line identification authentication

ITU roundtable · India Mobile Congress 2026
New Delhi, India · 9 October 2026

Why a Proof of Concept, and why now

The standards are substantially in place

Five Recommendations in force; ITU-T Q.3070 determined in July 2026; three more under development

Deployment experience is not

No implementations exercised against one another; no measurements of operational impact; no evidence base for the requirements still to be written

That gap is what blocks both sides

Suppliers commit where they see demand; standardization needs implementations in order to write detailed requirements and test specifications

ITU-T A Suppl. 2 records that a proof of concept is used to determine the feasibility of a solution, or to verify that it functions as intended and in accordance with the features defined in standards under development — and that this helps ITU understand whether a solution is viable and advance the work items under study.

That is exactly the position here: the specification work is largely done, and what remains is to find out what implementation teaches us.

Two tracks

Track A

Certificate-based CLI authentication

- Procedures specified at clause level in Recommendations in force or determined
- Implement, execute defined scenarios, and exercise against an independently developed implementation
- Produces interoperability evidence, measurements, and a record of implementation questions
- Feeds Q2/11, and test specification work in Q16/11

Track B

Signalling security gateway capability

- ITU-T Q.3057 gives a high-level SSGW description; ITU-T Q.3066 gives threat model, detection methods and mitigation pillars — as principles
- Demonstrate capability against the four Q.3066 threat categories; describe it in a common structure
- No interoperability partner required; conformance is not assessed, because the requirements do not yet exist
- Produces the evidence base for detailed SSGW requirements and test specifications

The two are one activity, not two. ITU-T Q.3066 names authenticity validation of signalling messages as one of its four mitigation pillars — and Track A is the mechanism that supplies it. One scenario exercises that junction directly.

How the PoC is conducted

1	Outside ITU-T	The activity is carried out outside ITU-T, on a voluntary basis.
2	Participants govern themselves	Participants make rules of their own, appoint their own coordinator, and agree their own schedule. ITU-T is in no way involved in that rule-making
3	Open, including to non-members	Because the activity sits outside ITU-T, it may involve entities that are not ITU-T members. Membership affects only who can carry a contribution into the study group
4	Notification, not application	Inform Study Group 11 what you plan to do, so the group knows what is happening and where, and can put parties in touch. Nothing is assessed, scored, compared or refused
5	The description is offered, not imposed	Scope, scenarios, measurements and templates are there so the activity need not be designed from nothing. Adopt, adapt or replace them — just record what you did

Supplement 2 to the ITU-T A-series Recommendations — Guidelines on interoperability experiments and proof-of-concept events (12/2022)

Indicative timeline



Timings are indicative and relative to the issuance of the Call. The phases are a matter for the participants: they may be compressed, extended or reordered, and a participant may join at any point. Interim findings reach each ordinary Study Group 11 meeting during the period.

Who can take part, and how

Sponsoring administration or regulator Member States and national regulatory authorities	Support the activity in your jurisdiction; where feasible arrange test trust anchor or registration authority functions and test numbering resources; receive the results	
Implementing participant, Track A Operators, suppliers, certification and trust service providers	Contribute one or more functions; execute the scenarios; pair with an independently developed implementation; report results	
Implementing participant, Track B Suppliers of signalling security gateways and firewalls; operators running them	Demonstrate what you already detect and mitigate; describe it in the common structure; say what the requirement should be. No partner required	
Test laboratory, academia, or observer Test laboratories, research institutions, universities, any eligible entity	Provide environments, traffic generation and measurement — or simply receive the interim and final reports	
Open to Any entity able to contribute, including non-members of ITU	Conducted Outside ITU-T — voluntary, self-governed, self-supporting	Endorsement None — no ITU approval, certification or ranking of any implementation

What ITU-T asks in return

Two things, and they are the whole of it.

1

Contributions

That participants submit contributions to ITU-T Study Group 11 based on the results, so that ongoing work items can be advanced and the quality of the Recommendations improved — for example by proposing text changes to remove ambiguities

2

Information sharing

That participants share as much information as possible at study group meetings: the results; how the activity was performed, with methods, equipment, schedule and coordinator; where it was conducted; how the results should be handled to produce contributions; and any other activity in the same area

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

Contributions to Study Group 11 are submitted by ITU-T members. A participant that is not a member is encouraged to work with one.

HOW TO TAKE PART

The announcement is coming

Open to

ITU members and any other interested party

Inform SG11

a notification, not an application. Nothing is assessed or refused

How

Complete the outline published with the Call and send it to ITU

Basis

Conducted outside ITU-T, self-governed and self-supporting

Full description

Scope, functions, scenarios, measurements, participation model and report template, published with the Call

itu.int/go/tsg11 · itu.int/go/SIG-SECURITY