

ITU-T STUDY GROUP 11

From standards to deployment

Signalling security and certificate-based calling line
identification authentication for combating fraudulent communications

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

What this presentation covers

1

The problem

Why calling line identification can be falsified, and why measures at the network edge have not closed it

2

The framework

What ITU-T Q.3057, Q.3062 and Q.3063 specify, and what goes on the wire

3

The trust layer

Certificate issuance under determined draft Q.3070, and cross-border trust distribution

4

Status

What is in force, what is determined, what is still under development

5

The gap

Why deployment has not followed specification

6

The response

A two-track Proof of Concept — the Call itself is announced at the close of the session

Calling line identification can be falsified

Consumers

Scam and robocalls that present a familiar or trusted number, defeating call blocking and screening

Financial services

Impersonation of banks and digital financial service providers in social engineering and account takeover

Institutions

Impersonation of public authorities and enterprises, eroding the reliability of voice as a channel

“Signalling System No. 7 was originally designed for operator management on the assumption that anyone connected to the SS7 network was trustable. In the current network environment however, more and more untrusted devices ... are appearing that interconnect to a PLMN/PSTN. As a result, calling line identification spoofing is particularly effective at defeating call blockers.”

Recommendation ITU-T Q.3063 (2022), Summary

The assumption that broke

The original assumption

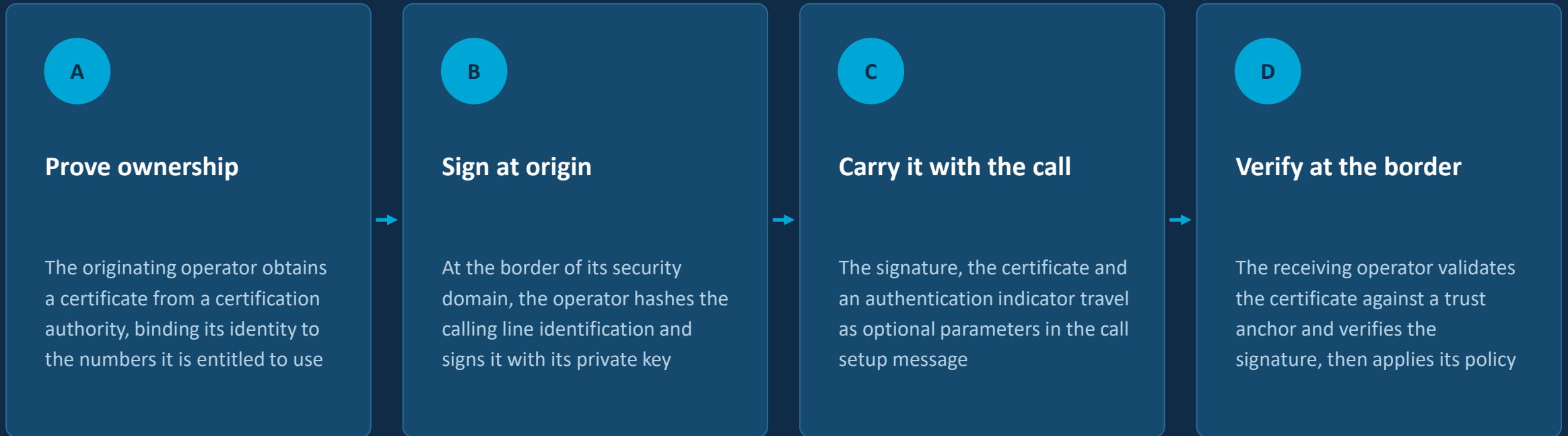
- Signalling interconnect segregated from public networks
- Connectivity available only to licensed operators
- A small, mutually known set of interconnect partners
- Consequently, no authentication applied on the network-to-network interface

The environment today

- PABX, call centres and VoIP access systems interconnect with PSTN and PLMN
- Access through SIP, SS7, GTP, Diameter and HTTP interfaces
- Over-the-top services, digital financial services and eSIM broaden the perimeter
- The interface carries no evidence of who asserted the identity

Measures applied at the receiving edge — blocking, screening, labelling — act on an identity they cannot verify. Authentication must travel with the call.

The idea, in one slide



Everything that follows is the detail of how these four steps are specified — and of the trust arrangements that make step D possible between operators that have no prior relationship.

What the framework makes possible

For consumers and the wider economy

- A call arrives carrying evidence of who asserted the identity it presents
- Fraud that depends on impersonating a bank, an enterprise or a public authority loses its principal instrument
- Voice becomes usable again as a channel for banking, public services and customer contact

For administrations

- A measure that acts on international inbound traffic, not only on domestic origination
- Interoperable with neighbouring jurisdictions without bilateral negotiation
- Each jurisdiction retains control over which trust anchors it recognizes
- Enforcement and consumer-protection action supported by verifiable evidence

For operators

- Policy is applied per interconnect partner, so deployment can begin with a single partner
- Network entities are unchanged; the function sits at the border of the security domain
- Transit networks are not required to implement anything

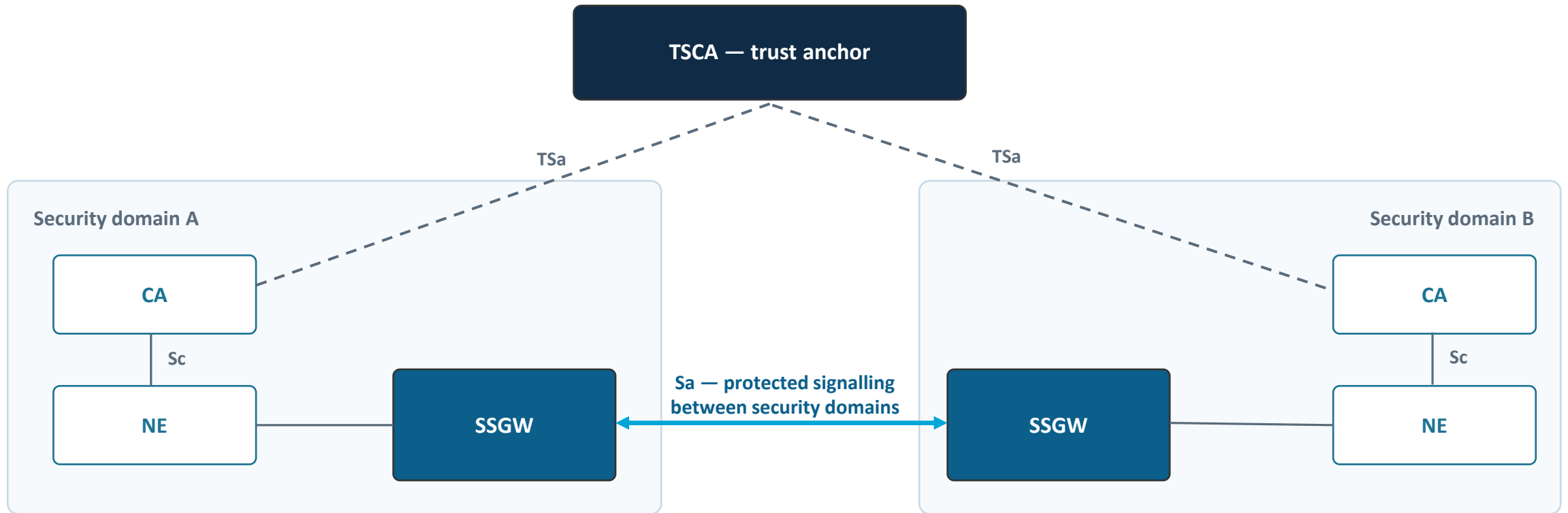
And because the mechanism is specified in ITU-T Recommendations rather than in a regional scheme, one implementation is applicable across markets. The same certificates, procedures and protocol parameters apply irrespective of which administration adopts them first — and the cross-border trust arrangement is designed so that adoption in one jurisdiction extends the reach of adoption in another.

The standards, and how they fit together

Governance	draft E.1122 (ITU-T SG2)	Registration authority anchor; assignment and cross-border sharing of trust anchor information
Certificates	draft Q.3070 (ex Q.TSCA) — determined July 2026	Verification of information elements in certificate requests; issuance of end-entity and CA certificates; cross-border trust anchor certificate list
Procedures	Q.3062 (2022) · Q.3063 (2022) + Cor.1 (2023)	Security associations and protected messages; the three CLI authentication processes and the presentation procedures
Protocol	Q.763 Amd.7 · Q.931 Amd.2 · Q.1902.3 Amd. (2023)	Certificate, signature and authentication indicator parameters carried in the call setup message
Architecture	Q.3057 (2020)	Functional entities, reference points, trust models, and the trusted signalling certification authority as trust anchor

Context: ITU-T Q.3066 (2026), detection and mitigation of signalling attacks. · Under development: Q.CSSIWF and Q.SSP4SIP, for SIP environments.

ITU-T Q.3057 — architecture and reference points



Functional entities: certification authority (CA) · trusted signalling certification authority (TSCA) · signalling security gateway (SSGW) · network entity (NE).

The SSGW may be standalone or integrated with a network entity and does not affect message routing.

ITU-T Q.3062 — what a protected message looks like



Both the security header and the security payload are sent in cleartext and are added by the originating SSGW.

Security association

- Created by each SSGW for every peer SSGW it exchanges with
- Identified by the SAI, derived from the peer global title (SS7) or the peer FQDN (IPX)
- Carries the algorithm identifier, the gateway certificate and an expiry time in UTC

Security header

- Security association identifier, concatenated with a time variant parameter
- The TVP is a 32-bit timestamp used for replay protection
- A message is accepted only if the timestamp falls within the acceptance window

Signature algorithms

- Identified by a DSA identifier carried in the security association
- DSA-0 — no signature applied; the payload is omitted
- DSA-1 — elliptic curve digital signature algorithm, P-384 curve, SHA-256 hash
- Identifiers 2 to 15 are not yet assigned

How an operator obtains a certificate

1

Request

The certification authority of a communications service provider sends a provisional certificate request to the TSCA, carrying its identity information elements

2

Automated check

The TSCA validates the information submitted in the request, the information exchanged contains the provider's registration with its governing telecommunication regulator according to applicable law

3

Provisional certificate (optional)

On success, the TSCA generates and returns an X.509 certificate signed by its private key, with the end entity denoted by the realm FQDN of the provider

4

Full validation

The TSCA completes verification of the identity information through its full validation process

5

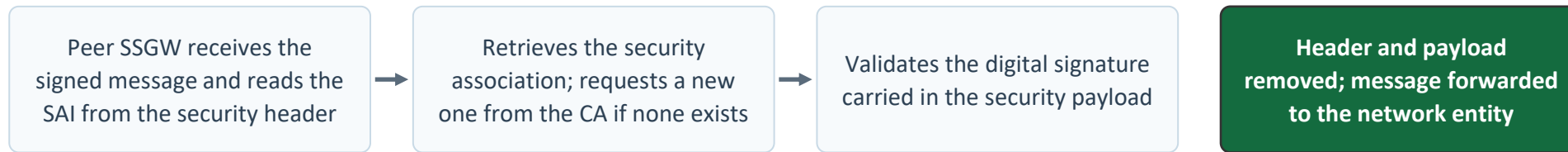
Validated certificate

The TSCA issues a validated CA certificate to the operator's CA; the operator's certification authority acknowledges it and begins using it to sign security associations using end-entity certificates

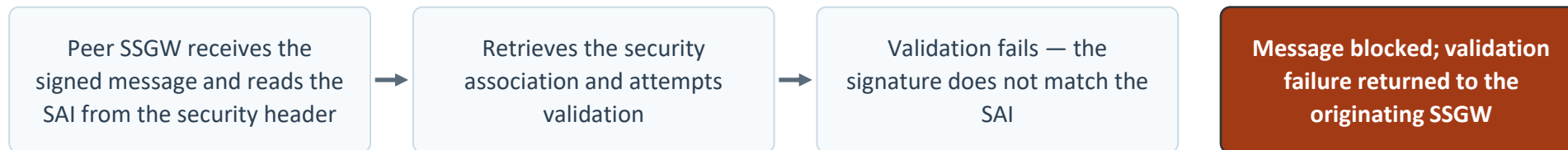
ITU-T Q.3062 clause 10.1.2 and Annex A; ITU-T Q.3057 clause 9.2.1. The requirements for what must be verified, and how, are specified in determined draft ITU-T Q.3070.

What happens when a protected message arrives

Signature validates



Signature does not validate



The security policy of the receiving SSGW determines what happens next: whether unsigned traffic from a domain is blocked, and what action applies when validation fails. Policy is defined per security domain — which is what makes incremental deployment possible.

ITU-T Q.3063 — calling line identification authentication

1

Certificate generating

clause 7.1

The gateway generates a key pair and authenticates to the certification authority over the Sc reference point. A challenge exchange demonstrates possession of the private key. The certification authority then signs the public key together with the identification ownership information, producing a calling line identification certificate (CLIC).

2

Call request initiating

clause 7.2

On receiving an initial address message, the outgoing gateway analyses the routing information, extracts the calling line identification from the BICC or ISUP parameters, computes its hash, signs the hash with its private key, and attaches the signature and the certificate to the message as optional parameters.

3

Certificate verification

clause 7.3

The incoming gateway checks whether the certificate is valid, expired or revoked; verifies the signature against the calling line identification; and, where the checks succeed, removes the added parameters and forwards the message to the destination exchange.

Certificates may be based on the ITU-T X.509 format, and the calling line identification carried in the certificate is based on the international ITU-T E.164 format.

What actually goes on the wire

Three new optional parameters are added to the initial address message. Corresponding extensions exist for DSS1 (ITU-T Q.931 Amd. 2) and for BICC (ITU-T Q.1902.3 Amd.).

Certificate

clause 3.107 · code 1001 0000

- Version of the encoded public-key certificate
- Serial number assigned to the certificate
- Expiry time, in seconds since 1970-01-01 UTC
- Public-key algorithm and key length
- The public key being certified

Length: 41 octets or more

Signature

clause 3.108 · code 1001 0001

- Signature algorithm — including sha256WithRSAEncryption, sha384WithRSAEncryption, dsa-with-sha256 and ecdsa-with-SHA256
- Length
- The signature value

Length: 66 octets or more

CLI authentication indicator

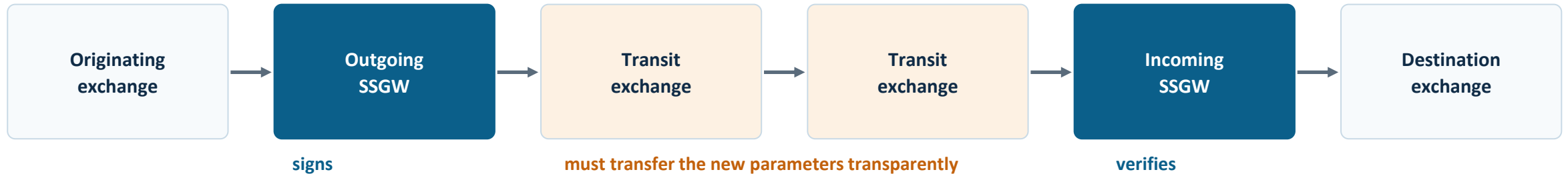
clause 3.109 · code 1001 0010

- Bit A — 0 indicates successful authentication; 1 indicates unsuccessful authentication
- Bits B to H are spare

Length: 3 octets

All three parameters are optional in the initial address message, which is what permits a network that has not implemented the extensions to continue operating unchanged.

The incremental deployment question



What the Recommendations specify

- The extended message includes a parameter compatibility information parameter, instructing transit exchanges to transfer the added parameters transparently to the next exchange
- Transit exchanges apply the compatibility procedures of ITU-T Q.764 clause 2.9.5.3.2 and ITU-T Q.1902.4 clause 13.4.4.2 on receipt of unrecognized parameters

What is not yet known

- How exchanges actually deployed today behave on receipt of these parameters — across vendors, generations and configurations
- Whether the parameters survive real international transit paths intact
- This is a question of observation, not of specification. It is one of the reasons a proof of concept is needed

Draft ITU-T Q.3070 — determined in July 2026

Requirements for issuing end-entity and certification authority certificates for enabling trustable signalling interconnection between network entities

Certificate request verification

Requirements for verifying the information elements presented in a certificate signing request, and for the issuance of provisional and validated end-entity certificates

Identity information

A recommended set of verifiable identifiers: legal name, security domain names, place of legal establishment, responsible registration authority, official registration identifier, business address and authorized contact

Cross-border trust anchor list

A signed list, structured as a JSON web token, carrying for each entry the country codes concerned, the trust anchor certificate, and the locations of the certification authority list and the revocation list

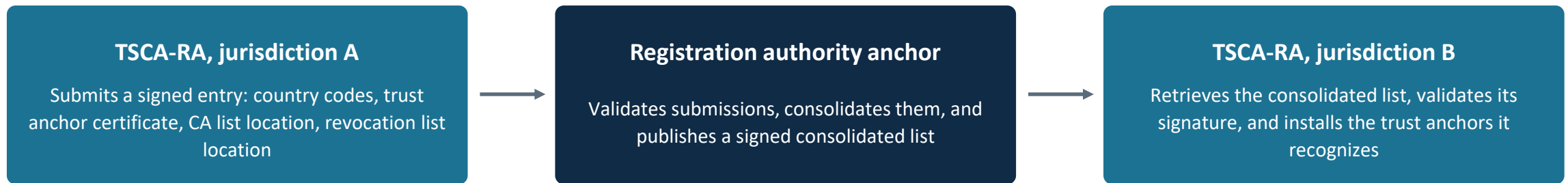
Revocation and assignment records

Signalling requirements for retrieval of assignment record information and for revocation updates, so that a revoked certificate ceases to be accepted

Determined by ITU-T Study Group 11 at its meeting in Geneva, 14–22 July 2026, and communicated to ITU-T Study Group 2 and ITU-T Study Group 17.

Trust across borders

An operator in one jurisdiction must be able to validate a signature produced under a trust anchor in another, without a prior bilateral relationship.



How the list is protected

- Structured as a JSON web token, signed as a JSON web signature
- The protected header identifies the algorithm and the location of the signing certificate over HTTPS
- A sequence number increments with each publication, so a recipient can detect a missed update
- Validity fields bound the period during which the list is to be relied upon

What it preserves

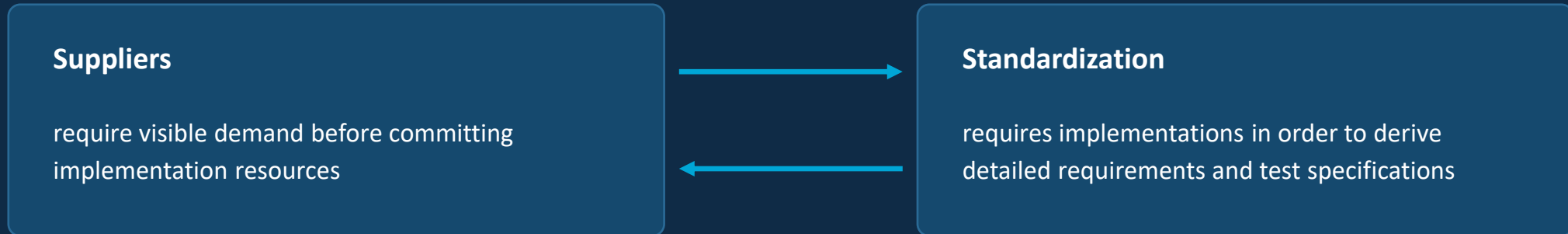
- Each jurisdiction retains control over which trust anchors it recognizes — the list distributes information, it does not compel recognition
- Each jurisdiction retains control over how certification authorities are appointed within it
- The governance arrangements sit in draft ITU-T E.1122, determined by ITU-T Study Group 2

Where the standards stand today

Reference	Title	Status	Date
ITU-T Q.3057	Signalling requirements and architecture for interconnection between trustable network entities	In force	04/2020
ITU-T Q.3062	Signalling procedures and protocols for enabling interconnection between trustable network entities	In force	09/2022
ITU-T Q.3063	Signalling procedures of calling line identification authentication (Cor. 1, 07/2023)	In force	09/2022
ITU-T Q.763 Amd. 7 Q.931 Amd. 2 · Q.1902.3 Amd.	Extensions for the support for the calling line identification authentication	In force	12/2023
ITU-T Q.3066	Principles for detection and mitigation of signalling attacks in telecommunication networks	In force	01/2026
draft ITU-T Q.3070	Requirements for issuing end-entity and certification authority certificates	Determined	07/2026
draft ITU-T E.1122	Registration authority anchor — governance framework (ITU-T Study Group 2)	Determined	08/2026
draft ITU-T Q.CSSIWF	Certificate based secure signalling interworking function, VoIP to legacy PSTN/ISDN	In development	—
draft ITU-T Q.SSP4SIP	Secure signalling procedures for the session initiation protocol	In development	—

The specification base is substantially in place. What is missing is deployment.

Why deployment has not followed



The way out is to build against the requirements that already exist

Rather than completing detailed requirements first and implementing afterwards, produce implementations and interoperability evidence against the determined and in-force text, and use what is learned to complete the specification.

Eight questions the Proof of Concept is designed to answer

These arise from reading the Recommendations against one another. They are points where an implementer must presently make a choice — and where different implementers may choose differently.

1

Algorithm and hash

Q.3057 clause 9.5 indicates ECDSA with SHA-384; Q.3062 Table 9-1 defines DSA-1 as ECDSA P-384 with SHA-256; Q.763 Amd. 7 lists ecdsa-with-SHA256 among the assigned codes

2

Certificate encoding

Q.3063 describes the certificate using X.509 syntax; Q.763 Amd. 7 clause 3.107 defines a compact parameter carrying version, serial, expiry, algorithm and public key

3

Signature coverage

The signature is computed over the hash of the calling line identification, while acceptance is also conditioned on the called party number being correct

4

Replay protection

Q.3062 provides a time variant parameter for replay protection; the Q.3063 procedure has no mandatory equivalent element

5

Hash function

The hash function applied to the calling line identification is not mandated by Q.3063 clause 7.2

6

Reference point implementation

The implementation of the Sa and TSa reference points is not defined by Q.3057 and Q.3062

7

Policy structure

Security policy is specified in Q.3057 clause 9.3 and referenced in Q.3063; the practical structure required during incremental deployment is not defined

8

Transit behaviour

Whether deployed intermediate exchanges transfer the new optional parameters transparently

What we are asking of you today

Administrations and regulators

- Describe the situation in your jurisdiction and the measures you currently apply
- Tell us what would need to be in place before deployment could be considered
- Indicate whether you would support, host or observe a proof of concept

Operators

- Tell us what implementation would involve in your network, and what the obstacles are
- Identify the interconnection relationships that would be most valuable to exercise
- Consider participating in a future PoC

Suppliers

- Tell us what you would need in order to commit implementation resources
- If you build signalling security gateways: Track B asks you to demonstrate what you already detect and mitigate — and to tell us what the requirement should say
- If you build certificate or signalling infrastructure: Track A asks for an implementation and an interoperability partner

ITU-T STUDY GROUP 11

Thank You

Signalling security and certificate-based calling line
identification authentication for combating fraudulent communications

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