Lawful Interception Assurance Fieldbook

Lawful Interception Assurance Fieldbook

Independent educational material about public technical standards, lawful governance, defensive architecture, interoperability, and assurance. It is not legal advice and contains no operational interception instructions.

\newpage

Roadmap, scope, and the safety boundary

Lawful interception (LI) is a legally authorized, targeted capability for obtaining communications data under applicable law. The engineering problem is not simply moving data. It is proving that every action had authority, stayed inside scope, preserved integrity, reached the approved recipient, expired on time, and can be audited without exposing sensitive material.

> **Safety boundary:** this chapter teaches lawful, governed system design from public standards. It does not provide operational targeting, activation, decryption, surveillance-evasion, or covert collection instructions.

The mental model

Concept	Plain meaning	Control that must travel with it
Authority before capability	A valid legal mandate is the root permission for every technical action	Technology cannot repair a missing or invalid legal basis
Targeted and bounded	Identifiers, services, jurisdiction, and time are explicitly limited	Broad or ambiguous scope must stop before activation
Separation of duties	No one person can authorize, configure, collect, and erase evidence alone	Dual control and independent review reduce misuse
Data minimization	Collect and retain only what the mandate and law permit	Collateral and out-of-scope data need defined handling

Concept	Plain meaning	Control that must travel with it
End-to-end assurance	Correctness covers authorization through delivery, expiry, and audit	A working interface is not proof of a lawful system
Standards with national profiles	ETSI and 3GPP provide interoperable technical building blocks	National law and profiles decide what is actually permitted

Apply it as a controlled workflow

1. Start with law, jurisdiction, competent authority, and an accountable policy owner.
2. Translate the mandate into a machine-checkable scope without changing its legal meaning.
3. Map administration, collection, mediation, delivery, receipt, expiry, and audit as separate responsibilities.
4. Attach controls and evidence to every state transition.
5. Test denial, expiry, duplication, loss, clock error, and insider misuse before production.
6. Reconcile the closed case and prove de-provisioning and retention outcomes.

Evidence to demand

- A standards applicability matrix with publication date, version, national profile, and owner.
- A trace from legal authority to approved technical scope and controlled lifecycle state.
- Independent audit evidence that excludes communication content from ordinary operational logs.
- Named stop conditions for invalid, expired, conflicting, or technically unsafe requests.

Failure to reason about

A platform can be technically available yet legally unusable. If an authorization expires while a delivery queue is delayed, the design must know which already-lawful records may complete delivery, which new collection must stop, and who resolves ambiguity. The answer belongs in policy, state machines, and tested evidence—not operator memory.

Feynman check

Explain LI as a sealed, timed delivery job: a judge or competent authority supplies the permission; the provider verifies the label; machines collect only the named parcel; an approved recipient signs for it; the job stops at expiry; auditors can later prove each step.

\newpage

Law, rule of law, necessity, and jurisdiction

Standards describe technical interfaces; they do not create legal power. The applicable legal framework defines who may issue an authorization, for which offences or purposes, with what necessity and proportionality tests, within which territory, and under which oversight, notification, retention, and remedy rules.

> **Safety boundary:** this chapter teaches lawful, governed system design from public standards. It does not provide operational targeting, activation, decryption, surveillance-evasion, or covert collection instructions.

The mental model

Concept	Plain meaning	Control that must travel with it
Legal basis	The statute, court order, or other lawful instrument permitting action	Record source, status, and jurisdiction; do not infer it
Competent authority	The body legally allowed to issue or validate the mandate	Verify authority independently from request content
Necessity	The action must address a legitimate need that less intrusive means cannot satisfy	Technical convenience is not necessity
Proportionality	Intrusion must be limited relative to purpose and harm	Scope growth needs renewed authority
Jurisdiction	Law and authority are territorially and organizationally bounded	Roaming, cloud regions, and cross-border delivery complicate it
Oversight and remedy	Independent review and challenge mechanisms constrain power	Audit must support meaningful review

Apply it as a controlled workflow

1. Maintain a jurisdiction register owned by legal and compliance specialists.
2. Validate issuing authority, dates, signatures, purpose, target scope, service, and territory.
3. Resolve conflicts of law before technical provisioning.
4. Encode only approved fields; preserve the original authoritative instrument separately.
5. Require renewed approval for amendments, extensions, or new identifiers.
6. Route legal uncertainty to a stop-and-escalate path.

Evidence to demand

- Legal sign-off and validation timestamps are immutable and independently reviewable.
- No technical activation can exist without a live authorization reference.

- Cross-border paths have an explicit legal-assistance basis and approved receiving authority.
- Policy tests reject missing, future, expired, revoked, and overlapping-invalid mandates.

Failure to reason about

A subscriber travels, the service is operated in one country, the cloud workload runs in another, and the requesting authority is in a fourth. A hostname or data-center location cannot decide jurisdiction. The organization needs a legal determination and an approved cross-border mechanism before delivery.

Feynman check

Standards are the shape of the locked box. Law decides who may ask for the box, what may go inside, where it may travel, and when it must be destroyed.

\newpage

Stakeholders, responsibilities, and separation of duties

LI spans public authority, law-enforcement monitoring, communications providers, service owners, vendors, operators, security, privacy, and independent oversight. Architecture should make decision rights and prohibited combinations visible.

> **Safety boundary:** this chapter teaches lawful, governed system design from public standards. It does not provide operational targeting, activation, decryption, surveillance-evasion, or covert collection instructions.

The mental model

Concept	Plain meaning	Control that must travel with it
LEA	The legally empowered law-enforcement authority	Its request still requires the applicable authorization
LEMF	The law-enforcement monitoring facility that receives authorized handover	Only approved destinations and staff may receive
CSP/NWO/SvP	Provider roles operating network or communications services	Responsibility follows real control, not labels
ADMF	Administration function managing authorized LI state	It must not silently broaden scope
POI	Point that observes authorized service events or communication material	It acts only from controlled provisioning

Concept	Plain meaning	Control that must travel with it
MF/DF	Mediation/delivery functions that normalize and send handover	They must preserve correlation, integrity, and isolation

Apply it as a controlled workflow

1. Create a RACI for authorization validation, provisioning approval, operations, receipt, audit, incident response, and deletion.
2. Identify toxic combinations such as one operator creating, approving, activating, and suppressing audit.
3. Implement dual control for high-risk state transitions.
4. Use separate privileged identities, work queues, and cryptographic trust for each role.
5. Make emergency access time-bound, visible, and post-reviewed.
6. Test staff departure, role change, supplier support, and compromised administrator scenarios.

Evidence to demand

- Privileged access reviews show purpose, approver, duration, and actual use.
- No shared administrative accounts or reusable operator credentials.
- Vendor support cannot view target scope or communication material by default.
- Oversight can reconstruct decisions without needing production superuser access.

Failure to reason about

A database administrator can modify case mappings and also erase audit logs. Even if this was created for operational convenience, it defeats independent accountability. Split authorities, make audit append-only outside the operational trust domain, and exercise detection.

Feynman check

Think of a bank vault: one person has the request, another checks it, a different machine opens only the named box, and a separate recorder watches the process.

\newpage

LI, lawful disclosure, preservation, and e-evidence

Related processes are often confused. LI generally concerns targeted, authorized acquisition while communication activity occurs. Lawful disclosure (LD) concerns data already held by a provider.

Preservation freezes eligible stored data against deletion. European e-evidence mechanisms define structured cross-border orders and communication between authorities and service providers. Their legal bases, timing, data categories, and interfaces differ.

> **Safety boundary:** this chapter teaches lawful, governed system design from public standards. It does not provide operational targeting, activation, decryption, surveillance-evasion, or covert collection instructions.

The mental model

Concept	Plain meaning	Control that must travel with it
Lawful interception	Authorized acquisition associated with ongoing service activity	Use LI lifecycle and handover controls
Lawful disclosure	Authorized request and delivery of stored provider data	Search only eligible repositories and date ranges
Preservation	Temporary protection of specified existing data from normal deletion	It is not permission to disclose
Production order	Authority to provide specified stored data under applicable law	Validate scope and recipient independently
Emergency request	A special urgent legal path where law permits it	Urgency does not remove validation or later review
e-Evidence interface	Structured exchange supporting EU cross-border orders	It does not itself decide legal validity

Apply it as a controlled workflow

1. Classify the incoming instrument before selecting any technical workflow.
2. Determine data category, creation time, location, retention state, and legal availability.
3. Keep preservation, search, review, disclosure, and live interception state separate.
4. Use the matching ETSI family and national profile.
5. Record partial availability, lawful rejection, and deadline handling explicitly.
6. Close with delivery receipt, retention decision, and audit reconciliation.

Evidence to demand

- The case record states whether the workflow is LI, LD, preservation, or e-evidence.
- Preserved data cannot be disclosed merely because it is held.
- A live intercept cannot silently become a historical-data fishing exercise.
- Metrics separate legal deadlines from technical service levels.

Failure to reason about

An authority sends a preservation order for messages that may otherwise expire. The provider freezes the specified stored items. It must not start live collection or release the items until a valid production authority arrives.

Feynman check

LI watches a permitted future stream; disclosure retrieves permitted stored pages; preservation puts a legal bookmark on existing pages; none of these permissions automatically includes the others.

\newpage

The functional reference model

A reference model lets legal, network, platform, and receiving teams discuss responsibility without tying the design to one vendor. The essential flow is authorization administration, controlled observation, mediation, delivery, receipt, and evidence.

> **Safety boundary:** this chapter teaches lawful, governed system design from public standards. It does not provide operational targeting, activation, decryption, surveillance-evasion, or covert collection instructions.

The mental model

Concept	Plain meaning	Control that must travel with it
HI1	Administrative or warrant-related handover information	Keep it distinct from intercepted material
HI2	Intercept-related information (IRI) handover	Preserve event semantics, timing, and correlation
HI3	Content of communication (CC) handover	Apply the highest confidentiality and minimization controls
X1	Internal administration interface	Provision only approved scope; authenticate both ends
X2	Internal delivery of IRI toward mediation	Detect gaps, duplicates, and version mismatch
X3	Internal delivery of CC toward mediation	Isolate high-volume sensitive flows

Apply it as a controlled workflow

1. Draw roles first, then interfaces, then products.
2. Mark legal, administrative, provider-network, mediation, and LEA trust zones.

3. Label each data class and allowed direction.
4. Separate control-plane and delivery-plane failure models.
5. Map every logical role to deployment, owner, keys, logs, and recovery.
6. Validate the model against each supported service technology.

Evidence to demand

- A data-flow diagram names every boundary and data classification.
- IRI and CC are distinguishable through storage, transport, access, and retention.
- An interface inventory records version, national profile, endpoint owner, and certificate authority.
- No monitoring facility is reachable from general provider networks.

Failure to reason about

If one mediation service handles both administrative records and content with the same database, identity, and log sink, a compromise crosses every boundary. Logical labels do not create isolation; deployment and authority must enforce it.

Feynman check

HI means the provider hands something to the approved authority. X means provider systems talk internally. The numbers tell whether it is administration, event information, or communication content.

\newpage

The lifecycle: authorization to closure

The safest design is a finite state machine whose transitions require explicit evidence. A case should not be a set of scripts or tickets. It should have controlled states, allowed actors, validation rules, deadlines, and irreversible audit events.

> **Safety boundary:** this chapter teaches lawful, governed system design from public standards. It does not provide operational targeting, activation, decryption, surveillance-evasion, or covert collection instructions.

The mental model

Concept	Plain meaning	Control that must travel with it
Received	A request entered controlled intake	No provisioning yet
Validated	Authority, scope, dates, and jurisdiction passed review	Validation evidence is immutable

Concept	Plain meaning	Control that must travel with it
Approved	Required internal dual control completed	Approvers cannot be the requesting operator
Provisioned	Authorized scope reached relevant functions	Activation acknowledgements are reconciled
Active	Permitted observations may be produced	Continuous expiry and scope checks remain
Closed	Collection stopped and post-case duties completed	Closure includes de-provisioning and retention outcome

Apply it as a controlled workflow

1. Normalize the request without discarding the signed original.
2. Validate authority and translate bounded scope.
3. Run dual approval and conflict checks.
4. Provision with an idempotent case operation and collect acknowledgements.
5. Monitor completeness, scope, health, and expiry without exposing payload.
6. Stop, de-provision, reconcile, record receipt, and execute retention policy.

Evidence to demand

- Every state transition has actor, reason, time source, prior state, and authorization reference.
- Repeated requests are idempotent and do not create duplicate collection.
- Expiry is enforced autonomously even when control systems are unavailable.
- Closure reports unresolved gaps, incidents, delivery receipts, and deletion holds.

Failure to reason about

A maintenance outage hides the expiry scheduler. Collection continues after legal end time. Availability engineering must include lawful stop behavior: local expiry enforcement, monotonic state, protected time, and an alarm that does not depend on the failed control plane.

Feynman check

A case behaves like a train with gated stations. It cannot jump from request to collection, and at the final station every carriage must stop and be counted.

\newpage

Handover interfaces: HI1, HI2, and HI3

The handover model separates administrative information from intercepted event information and communication content. This separation supports least privilege, different throughput and confidentiality needs, and independent receipt and reconciliation.

> **Safety boundary:** this chapter teaches lawful, governed system design from public standards. It does not provide operational targeting, activation, decryption, surveillance-evasion, or covert collection instructions.

The mental model

Concept	Plain meaning	Control that must travel with it
HI1 administration	Conveys warrant/case lifecycle information as defined by applicable profile	Do not mix legal documents with payload channels
HI2 IRI	Conveys metadata or service events related to the authorized target	IRI can itself be highly sensitive
HI3 CC	Conveys authorized communication content	Strongest isolation, capacity, and access controls apply
Correlation	Lets receiving systems relate authorized IRI and CC	Identifiers must not collide, leak, or be rewritten unpredictably
Sequencing	Represents order and detects discontinuity	Transport order is not always service-event order
Receipt	Confirms accepted delivery or reports a bounded error	A network send is not proof of usable receipt

Apply it as a controlled workflow

1. Classify each handover object as administrative, IRI, CC, or control.
2. Select the applicable ETSI/3GPP and national profile.
3. Define correlation, time, sequencing, error, and retry semantics at contract level.
4. Provision endpoints and trust separately from target data.
5. Test volume, loss, duplicate, reordering, failover, and invalid-version behavior.
6. Reconcile source, mediation, and receiver counts using privacy-safe evidence.

Evidence to demand

- Interface conformance results are tied to exact schema and profile versions.
- Delivery health reveals gaps without putting content into telemetry.

- Backpressure and outage policy are agreed by provider and receiving authority.
- Administration cannot expose communication content to case-management users.

Failure to reason about

A delivery function reconnects after outage and retransmits a window. Without stable object identity and receiver-side duplicate handling, the same material may be counted twice. Without bounded replay, records may be lost. The contract must define both.

Feynman check

HI1 says what authorized job exists. HI2 carries the allowed activity notes. HI3 carries allowed communication material. Separate doors help each kind of parcel receive the right protection.

\newpage

ETSI TS 103 120: warrant information interface

ETSI TS 103 120 specifies an electronic interface for warrant-related information between an authorized organization and a communications provider. It supports structured establishment and management of authorized actions. The standard improves interoperability; it does not validate the law or replace national approval.

> **Safety boundary:** this chapter teaches lawful, governed system design from public standards. It does not provide operational targeting, activation, decryption, surveillance-evasion, or covert collection instructions.

The mental model

Concept	Plain meaning	Control that must travel with it
Structured warrant information	Machine-readable administrative data for controlled processing	The signed legal source remains authoritative
Object lifecycle	Creation, modification, cancellation, and status can be represented	Only permitted transitions are accepted
Tasking information	Bounded technical scope derived from authority	Translation must be independently checked
Acknowledgement/status	Makes processing outcome visible	Avoid revealing provider internals or target data unnecessarily
National extensions	Jurisdiction-specific parameters where standardized	Version and interpretation need bilateral agreement

Concept	Plain meaning	Control that must travel with it
Schema validation	Rejects malformed or incompatible messages	Syntactic validity is not legal validity

Apply it as a controlled workflow

1. Pin the published TS 103 120 edition and the applicable national profile.
2. Validate transport peer, message signature, schema, freshness, and replay protection.
3. Perform legal and authority validation outside the wire parser.
4. Map the accepted object into a controlled case lifecycle.
5. Return bounded status without leaking sensitive topology.
6. Audit amendments, cancellations, and conflicts against the original authority.

Evidence to demand

- Interoperability tests cover create, amend, reject, revoke, duplicate, and expired cases.
- A schema-valid but unauthorized request is denied before provisioning.
- Message and case identifiers remain stable across retries.
- National extensions are documented, tested, and rejected when unknown.

Failure to reason about

An incoming object is perfectly valid XML or ASN.1 but names an issuing body outside the configured authority set. The parser succeeded; the request must still stop. Conformance and authorization are separate controls.

Feynman check

TS 103 120 gives two trusted offices a common form and envelope. It does not decide whether the person filling the form has legal permission.

\newpage

ETSI TS 103 221-1: X1 administration

The X1 interface is the provider-internal administration path between a central administration function and LI functions. It carries controlled provisioning and lifecycle state, not a license for local components to invent scope.

> **Safety boundary:** this chapter teaches lawful, governed system design from public standards. It does not provide operational targeting, activation, decryption, surveillance-evasion, or covert

> collection instructions.

The mental model

Concept	Plain meaning	Control that must travel with it
Central administration	One governed source coordinates authorized technical state	Avoid uncontrolled local tasking
Provisioning	Distributes the minimum parameters needed by a function	Do not send legal documents or unrelated identifiers
Function discovery/capability	Administration understands supported features and status	Capability must not silently downgrade safeguards
Acknowledgement	Each function reports applied state	Success is reconciled across the whole path
Keepalive/status	Detects control-path health	Health does not prove correct target scope
De-provisioning	Removes authorized state promptly at end	Local expiry is a safety backstop

Apply it as a controlled workflow

1. Inventory every X1-controlled function and assign stable identity.
2. Authenticate and authorize both sides with narrow service credentials.
3. Send idempotent versioned desired state with effective and expiry times.
4. Collect positive and negative acknowledgements and reconcile drift.
5. Keep target parameters out of generic infrastructure telemetry.
6. Exercise control-plane outage, rollback, revocation, and stale-node recovery.

Evidence to demand

- Desired and observed state can be compared without exposing content.
- A newly restored node cannot reactivate expired state.
- Unknown fields, versions, and functions fail safely.
- Certificate rotation does not require bypassing peer authentication.

Failure to reason about

A function restores from an old snapshot containing an active task. If it trusts local disk instead of authoritative current state and expiry, it can resume unlawful collection. Boot must reconcile signed/authorized state before observation.

Feynman check

X1 is the provider’s private control line. It tells approved internal machines exactly which bounded job exists and when it ends.

\newpage

ETSI TS 103 221-2: X2 and X3 delivery

X2 and X3 define provider-internal delivery paths for IRI and CC toward mediation/delivery functions. They create a clean boundary between service-specific observation and standardized handover processing.

> **Safety boundary:** this chapter teaches lawful, governed system design from public standards. It does not provide operational targeting, activation, decryption, surveillance-evasion, or covert collection instructions.

The mental model

Concept	Plain meaning	Control that must travel with it
X2	Internal transfer of intercept-related information	Preserve event identity, timestamps, and scope
X3	Internal transfer of content of communication	Isolate throughput and confidentiality
POI identity	Identifies the producing function and trust context	Do not confuse network identity with target identity
Mediation input	Receives service-specific objects for normalization	Reject incompatible or unauthorized inputs
Sequence/gap handling	Detects missing, late, or duplicate delivery	Define recovery rather than hiding counters
Flow control	Protects functions during congestion	Dropping policy must be explicit and reportable

Apply it as a controlled workflow

1. Define supported service profiles and data classifications per interface.
2. Bind producer identity to approved administration state.
3. Validate object, scope reference, time, and anti-replay attributes.
4. Separate X2 and X3 queues, keys, capacity, and access.
5. Normalize only what the downstream profile requires.
6. Reconcile production, mediation acceptance, and handover delivery.

Evidence to demand

- Load tests use synthetic data and cover receiver slowdown and failover.
- Gap and duplicate alarms expose counts and identifiers, never payload.
- A producer cannot send for a case it was not provisioned to serve.
- Mediation preserves source evidence and transformation version.

Failure to reason about

During congestion, CC traffic fills a shared queue and delays IRI status records. Separate resource pools and declared priorities prevent one data class from hiding another’s completeness evidence.

Feynman check

X2 carries allowed event notes from service machinery; X3 carries allowed content. Mediation checks, labels, and safely prepares both for the outside handover.

\newpage

ETSI TS 101 671: foundational handover model

ETSI TS 101 671 is a foundational handover specification that established concepts still visible in later work. It is important for vocabulary, legacy interoperability, and understanding HI2/HI3, but implementers must verify whether a newer technology-specific or IP-delivery specification applies.

> **Safety boundary:** this chapter teaches lawful, governed system design from public standards. It does not provide operational targeting, activation, decryption, surveillance-evasion, or covert collection instructions.

The mental model

Concept	Plain meaning	Control that must travel with it
Foundational model	Provides common LI handover concepts and terminology	Do not assume old edition equals current profile
Legacy interoperability	Supports installed systems and historical national profiles	Migration and coexistence require testing
IRI/CC separation	Distinguishes event information from communication content	Both remain sensitive
Handover semantics	Defines receiver-facing behavior and information	Service-specific standards may refine it

Concept	Plain meaning	Control that must travel with it
National parameters	Allows jurisdiction-specific information	Uncontrolled variation harms interoperability
Migration mapping	Relates legacy objects to modern delivery frameworks	Mapping must preserve meaning and evidence

Apply it as a controlled workflow

1. Identify why TS 101 671 is referenced in the applicable profile.
2. Pin edition and dependencies rather than relying on the title.
3. Map each required concept to the selected current delivery family.
4. Document semantic differences and unsupported legacy fields.
5. Run bilateral conformance and regression tests.
6. Plan retirement where current profiles supersede legacy paths.

Evidence to demand

- The architecture marks the standard as foundational, active-by-profile, or superseded.
- Legacy translation is versioned and reversible for audit.
- No silent default fills legally material fields.
- Receiver acceptance is demonstrated with synthetic fixtures.

Failure to reason about

A vendor says its product is “101 671 compliant” but cannot name the edition, national profile, or supported services. The claim is not testable. Demand a precise conformance statement and evidence matrix.

Feynman check

This standard is an older map many newer maps learned from. Keep it when the road still uses it, but check the latest route before driving.

\newpage

ETSI TS 102 232 series: IP handover and service-specific details

The TS 102 232 family provides a common IP-based delivery framework plus service-specific details (SSDs). Part 1 defines general HI2/HI3 IP handover aspects. Other parts specialize messaging, internet

access, Layer 2, IP multimedia, PSTN/ISDN, and mobile-service material. Implementations select only the parts applicable to the authorized service and national profile.

> **Safety boundary:** this chapter teaches lawful, governed system design from public standards. It does not provide operational targeting, activation, decryption, surveillance-evasion, or covert collection instructions.

The mental model

Concept	Plain meaning	Control that must travel with it
Part 1	Common IP handover envelope, delivery, and control concepts	Pin the current published edition
Part 2	Service-specific details for messaging services	Service semantics and provider capability matter
Part 3	Service-specific details for internet access services	Identity-to-access binding is time-sensitive
Part 4	Service-specific details for Layer 2 services	Avoid assuming Layer 3 visibility
Parts 5–7	IP multimedia, PSTN/ISDN, and mobile-service details	Choose by actual service and network generation
Profile composition	Part 1 plus one or more SSDs and national parameters	Mixed versions require explicit compatibility

Apply it as a controlled workflow

1. Inventory offered services and identify applicable SSD parts.
2. Pin Part 1, SSD, common-parameter, and external dependency editions as one profile.
3. Define supported information classes and transformations at a conceptual level.
4. Validate delivery security, sequencing, error, keepalive, and availability behavior.
5. Run synthetic interoperability tests with the receiving facility.
6. Repeat testing whenever one part or national profile changes.

Evidence to demand

- A bill of standards records every composed version and dependency.
- Unknown service payloads are quarantined, not guessed.
- Performance testing covers high-volume CC and bursty IRI separately.
- Transformation logs contain version and outcome, not communication material.

Failure to reason about

Provider and receiver both claim TS 102 232 compliance, but one uses a newer Part 1 with an older mobile SSD and different national parameters. Family-level labels hide incompatibility. Pin and test the exact profile tuple.

Feynman check

Part 1 is the shipping box. The SSD parts describe how different kinds of permitted service material fit inside. The receiver and sender must agree on the exact box instructions.

\newpage

ETSI TS 103 280: the common-parameter dictionary

TS 103 280 centralizes common LI and disclosure parameters used across ETSI TC LI specifications. A shared dictionary reduces contradictory definitions, but only when every interface pins compatible editions and national extensions.

> **Safety boundary:** this chapter teaches lawful, governed system design from public standards. It does not provide operational targeting, activation, decryption, surveillance-evasion, or covert collection instructions.

The mental model

Concept	Plain meaning	Control that must travel with it
Common dictionary	One authoritative definition for reused parameters	Names alone do not ensure semantic agreement
Version alignment	Interfaces agree which dictionary edition applies	Independent upgrades can break decoding
Enumerations	Controlled values prevent free-text ambiguity	Unknown values need safe behavior
Identifiers	Consistent cases, parties, endpoints, and locations can correlate	Minimize and classify identifiers
Time representation	Events can be compared across systems	Clock source, zone, precision, and uncertainty matter
National extension	Approved jurisdiction-specific additions	Extension namespaces and ownership must be governed

Apply it as a controlled workflow

1. Create a dependency graph from each interface standard to TS 103 280.
2. Pin dictionary versions in build, schema registry, and conformance fixtures.
3. Define safe handling for unknown optional and mandatory values.
4. Normalize time and identity only through reviewed mappings.
5. Track national extensions as controlled products.
6. Regression-test producers and receivers before rollout.

Evidence to demand

- Schema compatibility checks run in CI and bilateral qualification.
- Time synchronization quality and drift are monitored without payload.
- Identifier formats are validated but never used as sole legal authority.
- Extension ownership, documentation, and expiry are visible.

Failure to reason about

A location field changes precision in a dictionary update. The wire still parses, but policy decisions and downstream interpretation differ. Semantic compatibility tests must go beyond successful decoding.

Feynman check

TS 103 280 is the shared dictionary. If two systems use different editions, the same word may no longer mean exactly the same thing.

\newpage

3GPP TS 33.126: LI requirements

TS 33.126 is the modern 3GPP requirements specification. It describes what LI support must achieve across provisioning, detection, capture, delivery, and de-provisioning while protecting LI information and limiting access to authorized personnel.

> **Safety boundary:** this chapter teaches lawful, governed system design from public standards. It does not provide operational targeting, activation, decryption, surveillance-evasion, or covert collection instructions.

The mental model

Concept	Plain meaning	Control that must travel with it
Stage 1 requirements	States service needs and required outcomes	It is not a deployment recipe
Provisioning	Authorized parameters reach appropriate functions	Least information and independent approval apply
Detection	Relevant service activity is recognized under authorization	No collection outside active scope
Capture	Authorized IRI or CC is made available	Preserve service semantics and integrity
Delivery	Material reaches the approved mediation/LEMF path	Secure, timely, complete, and accountable
De-provisioning	LI state is removed at end	Expiry must survive control-plane failure

Apply it as a controlled workflow

1. Translate each applicable requirement into architecture responsibility.
2. Map requirement to function, interface, owner, threat, and evidence.
3. Resolve national options and service applicability.
4. Design negative behavior for unauthorized, unsupported, and expired state.
5. Exercise lifecycle transitions under network-function scaling and failover.
6. Maintain traceability when release or service capability changes.

Evidence to demand

- A requirements compliance matrix links each clause-level obligation to tests.
- Only authorized personnel and workloads can access LI management information.
- Scaling does not duplicate or omit lifecycle state.
- De-provisioning is proven across every relevant network function.

Failure to reason about

A cloud-native network function autoscaling event creates a new instance. If authorized state propagation is late, service events may be missed; if stale bootstrap state is used, scope may be exceeded. Requirements must drive secure, consistent instance lifecycle.

Feynman check

33.126 says what the mobile system must accomplish safely. Later specifications explain architecture and protocol details.

\newpage

3GPP TS 33.127: architecture and functions

TS 33.127 is the Stage 2 architecture specification for modern 3GPP LI. It allocates responsibilities among administration, points of interception, mediation/delivery, and receiving functions across mobile-system services.

> **Safety boundary:** this chapter teaches lawful, governed system design from public standards. It does not provide operational targeting, activation, decryption, surveillance-evasion, or covert collection instructions.

The mental model

Concept	Plain meaning	Control that must travel with it
Stage 2	Turns requirements into logical functions and reference points	Products may combine roles only with preserved controls
ADMF	Administers authorized LI state	Protect from service-plane and ordinary operations
POI	Observes relevant authorized information in a network function or service	Bind output to current provisioning
MF/DF	Mediates and delivers IRI or CC	Transformation must be traceable
LEMF	Authorized receiving environment	Endpoint and jurisdiction are verified
Service coverage	Architecture applies across defined 5G/EPS/IMS services	Capability claims must name the release and service

Apply it as a controlled workflow

1. Select the 3GPP release and supported service set.
2. Map logical functions to real network functions, vendors, and responsibility.
3. Draw control, IRI, and CC flows with trust boundaries.
4. Define state propagation, correlation, scaling, and failover.
5. Test roaming, slicing, service chaining, and mixed-release conditions conceptually.
6. Keep a release-aware architecture decision and conformance record.

Evidence to demand

- Each logical function has an accountable owner and least-privilege identity.
- Co-located functions retain separate authorization and audit boundaries.
- Topology change cannot orphan active lawful state.
- Unsupported services fail visibly rather than appearing compliant.

Failure to reason about

A vendor appliance combines ADMF and mediation for simplicity. This can be acceptable only if access, data, logging, key, approval, and failure boundaries still enforce separation. A box boundary is not a control boundary.

Feynman check

33.127 assigns jobs: who manages the lawful task, where allowed service information is observed, who prepares it, and where it is received.

\newpage

3GPP TS 33.128: protocols and procedures

TS 33.128 is the Stage 3 protocol-and-procedure specification. Engineering teams need to understand its role, version dependencies, conformance, and security properties. This fieldbook intentionally does not reproduce wire-level tasking or collection procedures.

> **Safety boundary:** this chapter teaches lawful, governed system design from public standards. It does not provide operational targeting, activation, decryption, surveillance-evasion, or covert collection instructions.

The mental model

Concept	Plain meaning	Control that must travel with it
Stage 3	Defines interoperable protocol behavior for Stage 2 functions	Use the normative specification under controlled access
Procedure state	Messages implement authorized lifecycle and delivery behavior	State machines reject impossible transitions
Encoding/schema	Structured objects support interoperability	Parsing success is not authorization
Error behavior	Peers can report bounded failures	Errors must not leak target or topology details

Concept	Plain meaning	Control that must travel with it
Security association	Peers authenticate and protect transport	Key lifecycle and endpoint authorization are separate
Release compatibility	Protocol edition aligns with architecture and requirements	Mixed releases need a tested profile

Apply it as a controlled workflow

1. Pin matching 33.126, 33.127, and 33.128 release versions.
2. Build an abstract state/conformance model without production target data.
3. Validate peer identity, authorization, replay resistance, and schema before state change.
4. Use synthetic fixtures for positive and negative interoperability tests.
5. Fuzz parsers and test resource exhaustion in isolated assurance environments.
6. Promote only signed, reviewed protocol implementations with rollback.

Evidence to demand

- Conformance results identify exact release, options, and national profile.
- Malformed inputs cannot bypass authorization or exhaust privileged systems.
- Secrets and sensitive parameters are absent from ordinary logs and crash dumps.
- Protocol upgrade has dual-version, rollback, and reconciliation evidence.

Failure to reason about

A protocol parser accepts a valid message after the related case was revoked because authorization was checked only when the session opened. Every state-changing procedure must evaluate current authorization, not just transport authentication.

Feynman check

33.128 is the detailed grammar for approved machines. Knowing grammar does not grant permission to start the conversation.

\newpage

Legacy 3GPP TS 33.106, 33.107, and 33.108

The older 33.106/107/108 family remains important for legacy GSM, UMTS, EPS, and IMS deployments and for understanding historical handover. New designs should determine whether the modern 33.126/127/128 family applies, whether legacy coexistence is required, and how national profiles bridge them.

> **Safety boundary:** this chapter teaches lawful, governed system design from public standards. It does not provide operational targeting, activation, decryption, surveillance-evasion, or covert collection instructions.

The mental model

Concept	Plain meaning	Control that must travel with it
33.106	Legacy LI requirements	Do not use its title alone to claim modern 5G coverage
33.107	Legacy architecture and functions	Map actual supported network generation
33.108	Legacy handover interface	Coordinate with ETSI IP-delivery profiles
Coexistence	Old and new functions operate during migration	Prevent duplicate or missing handover
Semantic mapping	Equivalent concepts are related across families	Do not invent equivalence where meaning changed
Retirement	Legacy support is removed with receiver agreement	Inventory consumers and active legal obligations first

Apply it as a controlled workflow

1. Inventory network generations, services, and receiver profiles.
2. Classify each legacy standard as required, transitional, or retired.
3. Define one authority for task state across old and new paths.
4. Use synthetic dual-path comparison and reconciliation.
5. Cut over by bounded service cohort with rollback.
6. Prove no active cases, dependencies, or legal retention duties remain before removal.

Evidence to demand

- The standards matrix distinguishes legacy and modern families.
- Dual delivery cannot create unexplained duplicates.
- Migration preserves correlation and evidence.
- Retired endpoints, keys, and privileges are actually removed.

Failure to reason about

A 5G core supports modern procedures while an IMS voice service still relies on legacy handover. Declaring the whole network “5G compliant” hides the mixed profile. Model capability by service, function, and release.

Feynman check

Old and new mobile roads can coexist. Draw which service uses which road, make one traffic controller authoritative, and retire the old road only after every traveler is accounted for.

\newpage

5G SBA, slicing, roaming, and service evolution

5G replaces many fixed appliances with service-based, virtualized, and dynamically scaled functions. Network slicing, roaming, non-public networks, edge services, and changing identity associations add lifecycle and correlation complexity. LI controls must follow the service without becoming visible to general orchestration or tenants.

> **Safety boundary:** this chapter teaches lawful, governed system design from public standards. It does not provide operational targeting, activation, decryption, surveillance-evasion, or covert collection instructions.

The mental model

Concept	Plain meaning	Control that must travel with it
SBA	Network functions interact through service-based interfaces	LI control remains isolated from general APIs
Network slice	Logical service partitions share physical platform	Tenant isolation does not automatically isolate LI
Roaming	Home and visited networks share service responsibility	Jurisdiction and handover responsibility are explicit
Dynamic NF	Instances scale, move, and restart	Authorized state is consistent and expires safely
Edge deployment	Service processing occurs nearer users	Trust, time, keys, and reachability span sites
Identity association	Identifiers change across service events	Correlation must be lawful, bounded, and time-aware

Apply it as a controlled workflow

1. Map service ownership and LI responsibility for home, visited, edge, and tenant domains.
2. Keep LI administration outside ordinary discovery and observability surfaces.
3. Define secure state distribution for ephemeral instances.
4. Model lawful correlation across identifier changes without broad data pooling.
5. Test slice movement, roaming changes, failover, and delayed state.

6. Reassess coverage when 3GPP releases or service topology change.

Evidence to demand

- New instances cannot emit until current authorized state and time are proven.
- General orchestrator users cannot infer case existence.
- Roaming matrices name legal and technical delivery responsibility.
- Scaling, draining, and rolling upgrades have completeness reconciliation.

Failure to reason about

A network function is rescheduled to an edge zone whose certificate trust and time service are stale. The platform may serve ordinary traffic, but its LI path must fail safely and alert without revealing case information.

Feynman check

In 5G, the machines move and multiply. The lawful permission must reach exactly the right current machines, remain secret from ordinary operators, and disappear everywhere on time.

\newpage

Cloud, NFV, containers, and multi-tenancy

Cloud-native LI separates a provider control plane, service-plane points, mediation, evidence, and operations across software-defined infrastructure. Shared platforms can improve resilience but create insider, metadata leakage, snapshot, backup, and jurisdiction risks.

> **Safety boundary:** this chapter teaches lawful, governed system design from public standards. It does not provide operational targeting, activation, decryption, surveillance-evasion, or covert collection instructions.

The mental model

Concept	Plain meaning	Control that must travel with it
NFV/CNF	Network functions run as software on shared infrastructure	Platform admins are a new trust domain
Control-plane isolation	LI administration uses dedicated identities, networks, and policy	Namespace labels alone are insufficient

Concept	Plain meaning	Control that must travel with it
Secret workload identity	Functions authenticate without shared static credentials	Rotation and revocation must not reveal target state
Ephemeral compute	Instances are replaceable and stateless where possible	Sensitive buffers, crash dumps, and disks still need handling
Multi-tenancy	Infrastructure serves many customers or operators	Case metadata must not cross tenant or support boundaries
Data residency	Processing and backups stay in approved locations	Autoscaling and disaster recovery can move data

Apply it as a controlled workflow

1. Create separate trust zones for provider platform, LI control, observation, mediation, and audit.
2. Use dedicated workload identities, network policy, encrypted storage, and narrow operator roles.
3. Disable or govern snapshots, debugging, memory dumps, and support access.
4. Keep case details out of labels, metrics, traces, billing, and general logs.
5. Test node loss, rescheduling, backup, restore, region failover, and forensic acquisition.
6. Prove deletion and key retirement across active, backup, and replicated stores.

Evidence to demand

- Cloud control-plane logs can be reviewed without revealing target identifiers.
- Platform support cannot attach debuggers to sensitive workloads by default.
- Residency policy is enforced in placement and restore workflows.
- A compromised tenant cannot infer LI activity through shared resource side channels.

Failure to reason about

An autoscaler metric is named with a case identifier. A general cloud operator cannot read content but can infer who is under surveillance. Treat metadata as sensitive and use opaque operational identifiers.

Feynman check

Cloud computers are rented rooms in a huge building. Locks, keys, cleaners, cameras, backup storage, and emergency moves all need rules—not just the application door.

\newpage

IRI, CC, correlation, identity, and time

IRI and CC must remain semantically correct and correlatable without creating an uncontrolled identity warehouse. Time, sequence, target identity, network identity, and case identity are distinct. Precision, clock quality, and uncertainty matter.

> **Safety boundary:** this chapter teaches lawful, governed system design from public standards. It does not provide operational targeting, activation, decryption, surveillance-evasion, or covert collection instructions.

The mental model

Concept	Plain meaning	Control that must travel with it
IRI	Authorized information about communication-related events	It may be as sensitive as content
CC	Authorized communication content	Access and retention are tightly limited
Correlation identifier	Links related objects within permitted scope	Opaque, unique, and bounded
Target identifier	A legally authorized identity or selector	Do not broaden through unapproved association
Network/service identity	Operational identifier used by a service	Association may change over time
Trusted time	Comparable timestamps with known quality	Record source, precision, and drift

Apply it as a controlled workflow

1. Classify every field by purpose, authority, sensitivity, and retention.
2. Define legal rules for identity association and disassociation.
3. Generate correlation identifiers that do not reveal target identity.
4. Use protected time sources and monitor drift.
5. Preserve sequence and uncertainty during transformation.
6. Reconcile gaps and duplicates without inspecting payload.

Evidence to demand

- The data model distinguishes case, target, service, communication, and delivery identities.
- Clock quality is part of acceptance evidence.
- Correlation works across failover and retry without global reusable identifiers.
- Out-of-scope identity associations are rejected or quarantined.

Failure to reason about

A dynamic IP address was assigned to one subscriber, then another. If time precision or session boundaries are wrong, material can be attributed to the wrong person. Correlation requires authoritative, time-bounded association—not an address alone.

Feynman check

A name tag, room number, parcel number, and delivery receipt number are different. Mixing them can give the right parcel to the wrong person.

\newpage

Mediation, transformation, and delivery assurance

Mediation converts technology-specific output into the authorized handover profile while preserving meaning, provenance, ordering, and evidence. Delivery assurance proves more than connectivity: it addresses acceptance, gaps, duplicates, backlog, delay, and safe recovery.

> **Safety boundary:** this chapter teaches lawful, governed system design from public standards. It does not provide operational targeting, activation, decryption, surveillance-evasion, or covert collection instructions.

The mental model

Concept	Plain meaning	Control that must travel with it
Normalization	Maps service-specific objects into agreed handover form	Never silently invent missing meaning
Provenance	Records source function and transformation version	Keep operational evidence payload-free
Validation	Checks profile, scope reference, structure, and policy	Malformed authorized data is still unsafe
Delivery queue	Buffers bounded receiver or network interruption	Capacity and expiry behavior are explicit
Receipt/reconciliation	Compares sent, accepted, rejected, and replayed objects	Transport ACK is not semantic acceptance
High availability	Preserves service through component failure	Failover must not duplicate or widen scope

Apply it as a controlled workflow

1. Define an immutable transformation specification per input/output version pair.
2. Validate authorization reference and current lifecycle state at intake.
3. Separate IRI and CC processing, storage, keys, and capacity.
4. Use bounded durable queues with sequence and duplicate protection.
5. Exchange privacy-safe receipts and reconcile counts.
6. Test replay, partial acceptance, receiver outage, and disaster recovery.

Evidence to demand

- Every output can be traced to source and transformation version.
- Unmappable objects are quarantined with visible case impact.
- Backlog age and lawful timing thresholds alert before data loss.
- Failover/replay tests show complete-once semantic outcomes where required.

Failure to reason about

A mediation upgrade changes how an optional field is represented. Both formats parse, but receiver analytics interpret them differently. Canary synthetic traffic and semantic golden fixtures catch the issue before production.

Feynman check

Mediation is a careful translator and courier. It must not change the story, lose pages, copy pages twice, or deliver to the wrong reader.

\newpage

Security architecture, trust, cryptography, and keys

LI systems are high-value targets for criminals, hostile states, insiders, and extortion. Security must protect confidentiality, integrity, authenticity, availability, accountability, and secrecy of case existence. Cryptography supports these properties but does not replace authorization or operational discipline.

> **Safety boundary:** this chapter teaches lawful, governed system design from public standards. It does not provide operational targeting, activation, decryption, surveillance-evasion, or covert collection instructions.

The mental model

Concept	Plain meaning	Control that must travel with it
Zero-trust access	Every user/workload action is authorized from identity and context	Network location alone is insufficient
Mutual authentication	Both interface peers prove approved identity	Certificate validity is not endpoint authorization
Encryption	Protects data in transit and at rest	Keys, metadata, memory, and endpoints remain
Key management	Generates, stores, rotates, revokes, and destroys keys	Separate duties and hardware protection where justified
Integrity/signature	Detects unauthorized modification and supports provenance	Canonicalization and trust anchors matter
Threat modeling	Finds misuse and attack paths across trust boundaries	Repeat when topology or standards change

Apply it as a controlled workflow

1. Inventory assets including case existence, target scope, content, keys, audit, and availability.
2. Model external, insider, supply-chain, and shared-infrastructure threats.
3. Assign preventive, detective, containment, recovery, and oversight controls.
4. Use narrow identities and just-in-time privileged access.
5. Rotate trust without disabling validation or losing delivery.
6. Run compromise, key loss, forged request, exfiltration, and denial exercises with synthetic data.

Evidence to demand

- No secret, identifier, or payload appears in general logs, tickets, metrics, or crash reports.
- Key use is policy-bound and independently audited.
- Software provenance, signing, dependency, and update controls protect the supply chain.
- Emergency access is time-bound, dual-approved where possible, and reviewed.

Failure to reason about

A valid TLS client certificate belongs to a decommissioned receiver. Cryptography succeeds, but authorization should fail because the endpoint is no longer approved. Maintain an independent endpoint registry and rapid revocation.

Feynman check

Encryption is an armored van. You still need a real court order, the right driver, the right destination, a route, and a receipt.

\newpage

Audit, accountability, and chain of custody

Audit should allow independent reviewers to reconstruct who did what, under which authority, to which system state, and with what outcome. Chain of custody preserves provenance and integrity across acquisition, transformation, delivery, receipt, storage, and authorized use.

> **Safety boundary:** this chapter teaches lawful, governed system design from public standards. It does not provide operational targeting, activation, decryption, surveillance-evasion, or covert collection instructions.

The mental model

Concept	Plain meaning	Control that must travel with it
Audit event	A structured record of a consequential control action	Exclude content and minimize target details
Append-only evidence	Past events cannot be silently rewritten	Protect against privileged administrators
Provenance	Links output to source and transformation history	Identifiers must be stable and scoped
Integrity proof	Detects alteration of records or delivered objects	Protect trust anchors and verification procedures
Custody transfer	Records accountable handover between controlled parties	Network transmission alone is not custody
Independent oversight	Reviewers can test legality and control effectiveness	They need sufficient context without unnecessary exposure

Apply it as a controlled workflow

1. Define the minimum audit schema for authorization, lifecycle, access, change, delivery, and deletion.
2. Send evidence to a separately administered append-only store.
3. Use protected time and sequence and detect missing audit intervals.
4. Bind transformations and deliveries to versioned provenance.
5. Provide narrow oversight queries and sealed-case review.

6. Test administrator tampering, log outage, delayed upload, and evidence restoration.

Evidence to demand

- Auditors can reconstruct lifecycle without opening communication content.
- Privileged users cannot disable logging unnoticed.
- Custody records show sender, approved receiver, time, object range, and acceptance outcome.
- Audit retention and legal holds are distinct from intercepted-material retention.

Failure to reason about

An operator deletes an embarrassing failed provisioning event from the primary database. A separately controlled, cryptographically linked audit stream reveals the gap and preserves the original event.

Feynman check

Audit is the sealed diary of the process. It should tell who opened which authorized door and when, without copying what was inside the room.

\newpage

Privacy, minimization, collateral data, retention, and deletion

Lawful authority does not remove privacy engineering. Systems should minimize identifiers and fields, isolate collateral data, restrict use, enforce time and purpose, and prove retention or deletion outcomes under applicable law.

> **Safety boundary:** this chapter teaches lawful, governed system design from public standards. It does not provide operational targeting, activation, decryption, surveillance-evasion, or covert collection instructions.

The mental model

Concept	Plain meaning	Control that must travel with it
Purpose limitation	Data is used only for the authorized purpose	Analytics and product reuse are prohibited by default
Data minimization	Only necessary authorized information is processed	Schema availability does not equal permission

Concept	Plain meaning	Control that must travel with it
Collateral data	Information about non-target parties may appear in communication	Handle under national law and strict access
Retention schedule	Material and audit evidence have governed lifetimes	Different classes may have different rules
Legal hold	Authorized preservation overrides normal deletion temporarily	Hold scope and release are controlled
Deletion proof	Data and keys are removed across copies and backups as required	A database row deletion is incomplete

Apply it as a controlled workflow

1. Create a field-level purpose, authority, sensitivity, and retention inventory.
2. Minimize at the earliest reliable boundary.
3. Separate operational evidence from intercepted material.
4. Enforce access by case, role, purpose, and time.
5. Propagate expiry, hold, and deletion across queues, replicas, caches, and backups.
6. Run regular data-location and deletion verification.

Evidence to demand

- No LI material enters ordinary analytics, AI training, or troubleshooting datasets.
- Retention jobs fail closed and alert on unresolved copies.
- Backups have documented expiry, restore-time controls, and re-deletion behavior.
- Access reports support oversight of collateral-data handling.

Failure to reason about

A support engineer copies a failed delivery payload into a ticket. The ticketing system now has different users, region, backup, and retention. Use synthetic diagnostics, opaque object references, and controlled evidence access instead.

Feynman check

Permission to open one sealed letter does not permit copying it into the office notebook, training a robot on it, or keeping it forever.

\newpage

Reliability, capacity, time, monitoring, and operations

LI reliability is unusual: availability must coexist with lawful stop, confidentiality, integrity, completeness, and non-disclosure of case existence. Operations need privacy-safe indicators and rehearsed recovery.

> **Safety boundary:** this chapter teaches lawful, governed system design from public standards. It does not provide operational targeting, activation, decryption, surveillance-evasion, or covert collection instructions.

The mental model

Concept	Plain meaning	Control that must travel with it
Service objective	A measurable target for lifecycle and delivery behavior	Do not optimize uptime while violating scope
Capacity model	Sizes IRI bursts, CC bandwidth, queues, and recovery	Use tail and catch-up demand
Failure domain	A component group that can fail together	Replicas need independent power, network, keys, and control
Protected time	Reliable clocks support authorization and evidence	Monitor drift and holdover
Privacy-safe telemetry	Shows health without target or payload data	Opaque IDs and aggregation are still sensitive
Runbook/game day	Practiced response for failure and compromise	Use synthetic cases and dual control

Apply it as a controlled workflow

1. Model normal, peak, receiver outage, catch-up, and disaster-recovery workloads.
2. Set objectives for provisioning, de-provisioning, gap detection, delivery delay, and recovery.
3. Design independent capacity and queues for administration, IRI, CC, and audit.
4. Monitor clocks, certificates, versions, backlog, rejection, gap, duplicate, and expiry state.
5. Exercise loss, corruption, control outage, receiver outage, and regional failure.
6. Reconcile after every exercise or incident and update architecture.

Evidence to demand

- Dashboards reveal actionable health without case details.

- Receiver outage cannot cause unbounded storage or unlawful post-expiry collection.
- Recovery tests include key access and audit continuity.
- On-call access is just-in-time and every sensitive action is reviewed.

Failure to reason about

A receiver is unavailable for twelve hours. A queue sized for one hour fills. The system needs an agreed policy for admission, protected storage, notification, recovery priority, and lawful timing—not an improvised deletion or hidden drop.

Feynman check

Reliable means the right permitted parcel arrives safely and on time, and the machine stops when permission ends. It does not mean collecting forever.

\newpage

Conformance, interoperability, testing, and assurance

Standards compliance is a specific, testable claim: edition, profile, options, services, national extensions, and evidence. Conformance tests one implementation against a specification; interoperability tests two real implementations together; assurance also tests security, failure, operations, and legal-control integration.

> **Safety boundary:** this chapter teaches lawful, governed system design from public standards. It does not provide operational targeting, activation, decryption, surveillance-evasion, or covert collection instructions.

The mental model

Concept	Plain meaning	Control that must travel with it
Conformance statement	Names supported standards, versions, options, and exceptions	Avoid vague 'ETSI compliant' labels
Schema test	Checks structural encoding and constraints	Does not prove semantics or authorization
Interoperability test	Proves sender and receiver behavior together	Use synthetic non-production cases
Negative test	Exercises malformed, unauthorized, stale, duplicate, and unsupported input	Safe rejection is a feature

Concept	Plain meaning	Control that must travel with it
Security assurance	Tests implementation and deployment against threats	Include supply chain and privileged operations
Regression suite	Prevents version or vendor change from breaking established behavior	Golden fixtures need governance

Apply it as a controlled workflow

1. Build a standards and national-profile applicability matrix.
2. Define requirements traceability and a synthetic test corpus.
3. Test lifecycle, data classes, transformation, sequencing, errors, and receipts.
4. Run bilateral interoperability and high-volume/failure scenarios.
5. Perform parser, privilege, isolation, logging, and supply-chain assurance.
6. Sign the exact release artifact and archive results and exceptions.

Evidence to demand

- Every claim maps to a current test and immutable build artifact.
- Production content and real target identifiers never enter test environments.
- Known deviations have legal/security owners, compensating controls, and expiry.
- Upgrade approval includes rollback and mixed-version evidence.

Failure to reason about

A product passes schema tests but retries a partially accepted batch without stable identity, producing duplicates. Interoperability and failure tests expose behavior that a static validator cannot.

Feynman check

Spelling every word correctly does not prove two people understand the same story. Conformance checks spelling; interoperability and assurance check the conversation and its safety.

\newpage

Retained data and lawful disclosure: TS 102 657 and TS 103 705

ETSI TS 102 657 addresses request and delivery of retained data. TS 103 705 defines data structures for lawful disclosure. These support controlled search and handover of provider-held data; actual retention

duties and eligible categories come from applicable law, not the standard.

> **Safety boundary:** this chapter teaches lawful, governed system design from public standards. It does not provide operational targeting, activation, decryption, surveillance-evasion, or covert collection instructions.

The mental model

Concept	Plain meaning	Control that must travel with it
Retained data	Provider data lawfully held under normal or mandated retention	Do not create data merely because a request might arrive
Request interface	Structured query under a validated disclosure authority	Bound scope, time, service, and data categories
Response	Available authorized records plus status or lawful refusal	Distinguish none found from not held or not permitted
103 705 structure	Common data structures for disclosure	Pin edition and national profile
Search provenance	Records sources, query version, and processing outcome	Do not expose unrelated data in audit
Partial result	Explicitly reports limits, gaps, or unavailable data	Never fabricate completeness

Apply it as a controlled workflow

1. Validate disclosure authority independently from the query syntax.
2. Map requested categories to governed provider systems and retention state.
3. Search only approved fields, services, identities, and time window.
4. Review, minimize, package, and validate the result.
5. Deliver to the approved recipient and record receipt.
6. Apply post-delivery retention, hold, and deletion policy.

Evidence to demand

- The system distinguishes not found, not held, legally unavailable, and technical failure.
- Queries cannot traverse unrelated customer or analytics repositories.
- Data lineage proves source and transformation.
- Retention policy is documented independently from disclosure capability.

Failure to reason about

A request asks for two years of data, but policy lawfully retains only six months. The system returns the eligible available window with an accurate status; it does not imply records were lost or expand retention

retroactively.

Feynman check

Disclosure asks the provider for permitted pages already on its shelf. The catalog must say what is actually held, and the request cannot search every room.

\newpage

e-Evidence, cross-border exchange, and ETSI TS 103 462 ILHI

Cross-border legal cooperation adds requesting and responding authorities, differing national formats, time limits, secure channels, and legal-assistance decisions. ETSI TS 103 462 defines an inter-LEMF handover interface (ILHI). ETSI TS 104 144 supports interfaces for the EU e-Evidence Regulation. Technical interoperability never overrides jurisdiction or legal review.

> **Safety boundary:** this chapter teaches lawful, governed system design from public standards. It does not provide operational targeting, activation, decryption, surveillance-evasion, or covert collection instructions.

The mental model

Concept	Plain meaning	Control that must travel with it
Requesting/responding LEMF	Authorities exchange approved material across an inter-LEMF path	Each side keeps its legal responsibility
ILHI	Standardized inter-LEMF transport and interworking	Bilateral agreement and secure trust are required
Interworking function	Maps local formats to agreed cross-border format	Preserve provenance and report transformation
e-Evidence order	Structured cross-border order to a service provider	Validate authority, service, deadlines, and remedies
Conflict of law	Duties in different jurisdictions may conflict	Stop and escalate; do not solve in code
Delivery country	Recipient and onward handling are jurisdiction-bound	Routing must match approved legal path

Apply it as a controlled workflow

1. Identify requesting, responding, provider, and receiving legal roles.
2. Validate the cooperation instrument and any grounds for refusal or escalation.
3. Pin ILHI/e-evidence versions and bilateral profiles.
4. Establish approved endpoints, trust anchors, and interworking mappings.
5. Test receipt, delay, partial availability, translation, and onward-custody evidence.
6. Close both sides with aligned status and retention outcomes.

Evidence to demand

- Cross-border routing cannot be changed by ordinary network failover.
- Original and transformed representations remain linked and integrity-protected.
- Legal deadlines are visible separately from technical latency.
- Unknown national extensions stop safely.

Failure to reason about

A disaster-recovery route would send cross-border handover through an unapproved country. Ordinary network resilience would violate legal routing. Use policy-aware route constraints and a controlled unavailable state.

Feynman check

Cross-border exchange is like two courts using different forms. A trusted translator can align the forms, but only the law decides whether the package may cross the border.

\newpage

Incident response, insider threats, and continuous assurance

LI incident response must protect affected people, investigations, legal duties, and the integrity of oversight. Teams need sealed escalation, independent evidence, containment that respects active authorizations, and recovery that does not silently lose or widen collection.

> **Safety boundary:** this chapter teaches lawful, governed system design from public standards. It does not provide operational targeting, activation, decryption, surveillance-evasion, or covert collection instructions.

The mental model

Concept	Plain meaning	Control that must travel with it
Insider threat	Authorized access is misused or accumulated	Behavior, dual control, rotation, and independent audit matter
Security incident	Confidentiality, integrity, availability, or authority may be compromised	Use a restricted but accountable response channel
Legal incident	Action may exceed or lack authority	Stop, preserve evidence, and escalate immediately
Containment	Limits ongoing harm	Do not destroy evidence or hide delivery impact
Recovery	Restores a known-good authorized state	Revalidate every active case and endpoint
Lessons and assurance	Controls evolve from verified causes	Do not expose case details in broad postmortems

Apply it as a controlled workflow

1. Define severity and escalation for unauthorized access, overcollection, undercollection, leakage, tampering, and outage.
2. Preserve independently controlled evidence and protected time.
3. Contain compromised identities, keys, components, and routes.
4. Coordinate legal, security, privacy, provider, and authorized authority roles.
5. Restore from a clean build and revalidate live authorized state.
6. Notify and remediate as law requires, then test the corrective controls.

Evidence to demand

- Incident responders use synthetic or minimized views unless content access is necessary and approved.
- A compromised administrator cannot erase the evidence needed to investigate.
- Recovery reports exactly which periods, services, or cases may be affected.
- Exercises include malicious insiders and supply-chain compromise.

Failure to reason about

A privileged engineer queries case metadata without operational need. The system should detect unusual purpose-free access, preserve evidence outside their control, revoke access, and initiate restricted review—even if no content was opened.

Feynman check

A powerful system needs a fire alarm that even the key-holder cannot silence. When it rings, responders protect people, preserve the truth, and rebuild only from proven permission.

\newpage

Real-life governed scenario: Northstar Mobile

Northstar Mobile is a fictional communications provider operating mobile, fixed-IP, and messaging services. A competent authority submits a court-approved order concerning one subscriber identifier, two named services, and a precise 72-hour period. The example is intentionally non-operational: it explains governance, architecture, assurance, and evidence without target activation or collection instructions.

1. Intake and independent validation

The warrant interface receives a signed administrative object over an approved peer relationship. Schema validation passes, but that is only the first gate. A legal specialist verifies the issuing authority, jurisdiction, dates, named services, target identifiers, and any special limits against the authoritative order. A second authorized reviewer approves the technical translation.

The signed order is preserved separately. The case system stores a minimal, opaque case reference and a bounded technical scope. General service desks, cloud administrators, and product teams cannot see the target or case.

2. Architecture decision

Northstar maps the request through these controlled responsibilities:

```
validated authority → administration → approved points of interception

points → X2 IRI / X3 CC → mediation → HI2 / HI3 → approved LEMF

independent audit ← every consequential state transition
```

The administration function is the sole source of desired state. Each relevant function has a dedicated workload identity and acknowledges the versioned state. Functions also enforce expiry locally, so a control-plane outage cannot extend the authorization.

3. Standards profile

The service profile pins the applicable published ETSI TS 103 120 warrant interface, TS 103 221 internal interfaces, TS 103 280 common dictionary, and TS 102 232 delivery parts. Mobile services additionally pin

one coherent 3GPP 33.126/33.127/33.128 release. National parameters are treated as a separately versioned profile. “ETSI compliant” is not accepted without this tuple.

4. Controlled activation evidence

The platform records:

- approval identities and times;
- authority reference and approved scope hash;
- desired-state version and effective/expiry time;
- which eligible functions accepted or rejected the state;
- software, schema, certificate, and profile versions;
- gap, duplicate, backlog, and delivery-receipt counters;
- every privileged access and change.

It does not put target identifiers, communication content, or legal documents in normal logs, dashboards, traces, tickets, or cloud labels.

5. Delivery and assurance

IRI and CC use separate mediation pools, queues, keys, and access policies. Mediation validates the active case reference and transforms only to the pinned handover profile. Synthetic fixtures already proved version compatibility with the approved LEMF.

During the case, a receiver link is unavailable for 18 minutes. Bounded queues retain already authorized objects. Privacy-safe counters alert both controlled operations teams. On recovery, stable identity and sequence allow replay and duplicate handling. Source, mediation, and receiver totals reconcile; no operator opens payload to perform the check.

6. Expiry and closure

At the legal end time, every point independently stops new observation. The administration function sends de-provisioning and reconciles acknowledgements. Queued objects are handled according to the agreed legal policy for material lawfully acquired before expiry. No new collection occurs.

The closure report records final delivery status, gaps, incidents, privileged access, de-provisioning evidence, and the applicable retention or legal hold. Target-scope working data is deleted from operational systems when permitted. Audit evidence remains for the separately governed oversight period.

What the architect must defend

1. **Authority:** no action exists without valid current authorization.
2. **Scope:** identifiers, services, jurisdiction, and time are bounded.
3. **Isolation:** administrative, IRI, CC, and audit domains have distinct trust.

4. **Correctness:** versioned state, identity, time, sequence, and transformation make gaps and duplicates visible.
5. **Availability:** failure recovery never becomes permission to overcollect.
6. **Privacy:** data and metadata are minimized and ordinary operators cannot infer case existence.
7. **Accountability:** independent reviewers can reconstruct the lifecycle.
8. **Closure:** expiry, de-provisioning, retention, and deletion are proven.

Architecture review checklist

- Is the legal authority validated by a role independent of technical intake?
- Can any one person create, approve, activate, receive, and erase a case?
- Are standards and national profiles pinned to exact published versions?
- Does every function enforce current scope and local expiry?
- Are IRI and CC isolated in transport, processing, storage, and access?
- Can the platform detect missing, duplicate, late, or rejected objects?
- Do telemetry and support systems avoid target and content data?
- Are receiver outage and cross-border failover policies agreed in advance?
- Can a restored or newly scaled function prove current authorization?
- Can closure prove that all active state was removed?

Glossary and abbreviations

Term	Plain meaning
ADMF	Administration Function that controls approved LI state
CC	Content of Communication
CSP	Communications Service Provider
DF	Delivery Function
ETSI	European Telecommunications Standards Institute
HI1	Administrative/warrant-related handover information
HI2	Handover of Intercept Related Information
HI3	Handover of Content of Communication
ILHI	Inter-LEMF Handover Interface
IRI	Intercept Related Information
LEA	Law Enforcement Agency/Authority
LEMF	Law Enforcement Monitoring Facility
LD	Lawful Disclosure of stored data

Term	Plain meaning
LI	Lawful Interception
MF	Mediation Function
NF / CNF / VNF	Network Function / cloud-native / virtualized network function
NWO	Network Operator
POI	Point of Interception
RD	Retained Data
SBA	5G Service-Based Architecture
SSD	Service-Specific Details in the TS 102 232 family
SvP	Service Provider
TS	Technical Specification
X1	Provider-internal LI administration interface
X2	Provider-internal IRI delivery interface
X3	Provider-internal CC delivery interface

Published standards snapshot

This snapshot was verified against official ETSI and 3GPP catalog pages on **5 August 2026**. Standards evolve: an implementation or procurement decision must re-check the primary catalog, dependencies, national profile, and publication status.

Family	Published/status snapshot	Role and use
ETSI TS 101 331	V1.8.1 (2021-07)	Foundational LEA requirements; verify national applicability
ETSI TS 101 671	Verify current applicable edition/profile	Generic/foundational handover, often relevant to legacy profiles
ETSI TS 102 232-1	V3.37.1 (2026-05)	Common IP delivery handover; compose with applicable SSD parts
ETSI TS 102 657	V2.6.1 (2025-08)	Request/delivery of retained data, not live LI
ETSI TS 103 120	V1.23.1 (2026-05)	Warrant information interface; a newer draft does not replace the published edition
ETSI TS 103 221-1	V1.20.1 (2025-05)	X1 provider-internal administration
ETSI TS 103 221-2	V1.9.1 (2025-08)	X2/X3 provider-internal IRI/CC delivery

Family	Published/status snapshot	Role and use
ETSI TS 103 280	V2.18.1 (2026-03)	Common parameter dictionary and shared dependency
ETSI TS 103 462	V1.3.1 (2026-03)	Inter-LEMF Handover Interface
ETSI TS 103 705	V1.6.1 (2026-05)	Data structures for lawful disclosure
ETSI TS 104 144	V1.4.1 (2026-05)	EU e-Evidence Regulation interface
3GPP TS 33.126	Release 19 V19.3.0 snapshot	Modern mobile LI requirements
3GPP TS 33.127 / .128	Release 19 V19.5.0 status snapshot	Architecture/functions and Stage 3 protocols/procedures
3GPP TS 33.106 / .107 / .108	Release-aligned legacy family	Use where the legacy service profile requires
3GPP TS 33.129-1 / -2	Draft/status work in the checked report	Emerging security-assurance work; do not present as stable published guidance without re-checking

Official primary sources

- ETSI Technical Committee Lawful Interception
- ETSI TC LI Terms of Reference
- ETSI TS 103 120 work programme
- ETSI TS 103 221-1 V1.20.1
- ETSI TS 103 221-2 V1.9.1
- ETSI TS 103 280 published editions
- ETSI TS 102 657 V2.6.1
- ETSI TS 103 462 V1.3.1
- ETSI TS 101 331 V1.8.1
- 3GPP 33-series specification index
- 3GPP specification status report

Final Feynman challenge

Explain the complete Northstar case without using an acronym: who grants permission, who checks it, how the provider gives each machine only the necessary bounded job, how event information and content stay separated, how the approved authority receives it, how gaps are found without reading content, how the job stops on time, and how an independent reviewer proves the whole story later.

\newpage