



Tunnel Sovereign

---

SOVEREIGN COMMUNICATION AUTHORITY

# Controlled Evaluation Brief

---

Encryption protects the communication. Tunnel Sovereign governs the authority to communicate.

AVAILABLE FOR CONTROLLED EVALUATION

THIS BRIEF SETS OUT

What the product controls · What Tunnel Command does not require · Which platforms are implemented · What evidence exists today · What a Controlled Evaluation involves, and what it cannot establish

---

Sovereign Inc.

Delaware, United States

[tunnelsovereign.com](https://tunnelsovereign.com)

PUBLIC DOCUMENT · REVISION 1.1 · SEPTEMBER 2026

## 01 • THE PROBLEM

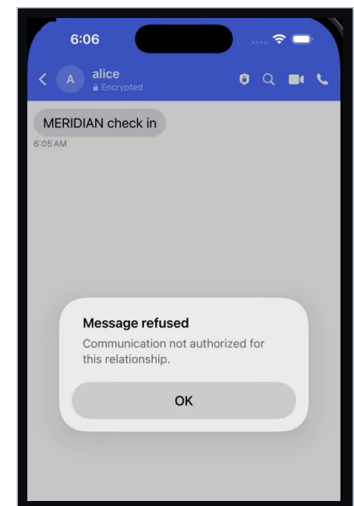
# Encryption can protect the message. It does not decide whether the communication should still be authorized.

Secure messaging answers one question well: can anyone else read this? It does not answer the question an organization is accountable for — should this endpoint still be able to send it at all?

A secure messenger protects content while the endpoint remains valid, and that validity is the assumption underneath it. The endpoint holds keys, the keys work, and the application does what the person holding it asks. That assumption is exactly what fails in the situations an organization has to plan for: a handset that leaves the perimeter, an operator no longer cleared for a task, a partner relationship that has ended, an operation that is over, an authority that should have expired weeks ago. None of those is an encryption failure. The cryptography is working precisely as designed.

## SIX QUESTIONS ENCRYPTION DOES NOT ANSWER

|              |                                                                    |
|--------------|--------------------------------------------------------------------|
| DEVICE       | Is this endpoint currently authorized?                             |
| RELATIONSHIP | May this person communicate with that person?                      |
| DIRECTION    | Does a grant one way create a grant the other way?                 |
| CAPABILITY   | Does authority to send a message include authority to send a file? |
| MISSION      | Is the operation this communication belongs to still active?       |
| TIME         | Has the authority lease expired?                                   |



The refusal is the product's own, on the endpoint's own screen. Recorded from the demonstration published at [tunnelsovereign.com/demo](https://tunnelsovereign.com/demo).

## THE ENDPOINT THAT STAYS ONLINE

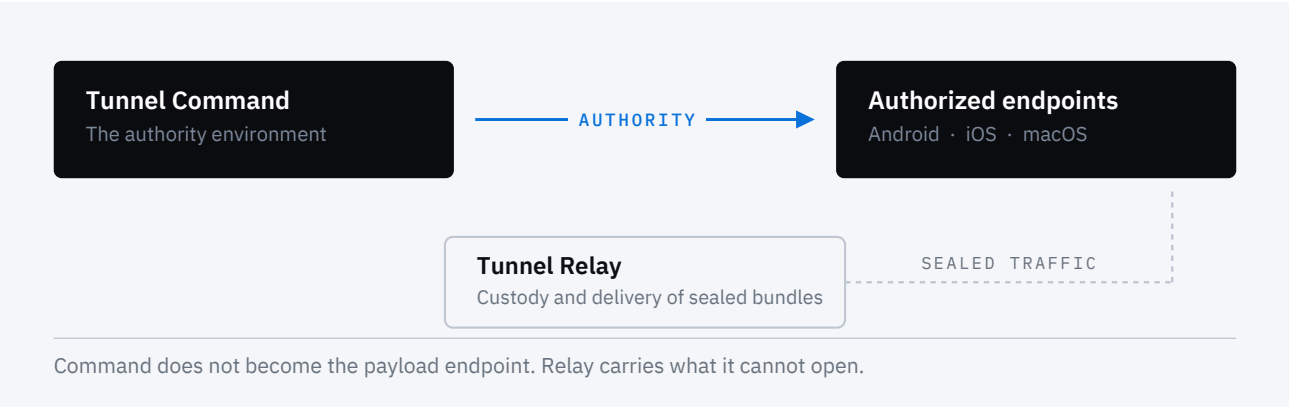
A device is lost, or the person holding it is compromised. The application is still installed, still enrolled, still online, and its keys still work. Tunnel Sovereign withdraws the authority. The endpoint stays online, and the software on it refuses what it may no longer do.

Nothing is wiped, destroyed, hidden, or replaced with a decoy. No remote destruction is claimed, and no reach over an endpoint that is disconnected: residual authority is bounded by the last signed lease, which is a real bound an operator plans for. What changes is the authority, not the device.

## Possession does not imply authority.

# A sovereign communication authority.

Tunnel Sovereign is an authority plane over secure communication. It governs whether a communication is permitted at all — from which device, with whom, in which direction, under which mission, with which capability and for how long — without becoming the endpoint that reads it.



## Command authorizes. Relay delivers. Authorized endpoints read.

### ONE PLATFORM, FOUR COMPONENTS

|                |                                                                                                                                                                                                      |
|----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| TUNNEL COMMAND | The authority environment, native on desktop. Enrollment, principals and devices, missions, relationships, capabilities, leases, freeze and revoke states, transport and retention policy.           |
| TUNNEL MOBILE  | The operator endpoint, native on mobile. Content is encrypted and decrypted on the endpoint, and credentials are bound to the device.                                                                |
| TUNNEL RELAY   | Delivery infrastructure, managed or customer-held, on Linux, private cloud, on-premises or isolated. Sealed bundles are held, scheduled, forwarded and expired. It holds no payload decryption keys. |
| SECURE CORE    | The shared foundation resident in Mobile, Command and Relay, and the reason the three enforce one authority model rather than three.                                                                 |

### MESSENGER AND SOVEREIGN

Tunnel Messenger is the communication plane: an operating secure messaging application, and the lineage this product comes from. Tunnel Sovereign is the authority plane that governs whether a communication is permitted at all.

Sovereign is not the messenger renamed. The Messenger user population is not a Sovereign deployment, a Sovereign customer base or evidence of Sovereign traction, and it is not presented as any of those here or on the website.

### THE UNIT THAT TIES THE PLATFORM TOGETHER

Everything the platform carries is a Secure Mission Bundle: a transport-independent encrypted package that carries its own authorization, its own policy and its own expiration. The relay reads the outer envelope in order to carry, schedule and expire the bundle, and does not hold the keys required to open the sealed section.

## The transport may change. The authority does not.

03 · AUTHORITY IN OPERATION

# Four grants, and what each one does not imply.

A grant names a source principal, a destination principal, one capability and one direction. It is absolute rather than relative: everything not granted is refused. Each behavior below is visible in the published demonstration.

## 01 Directional authority

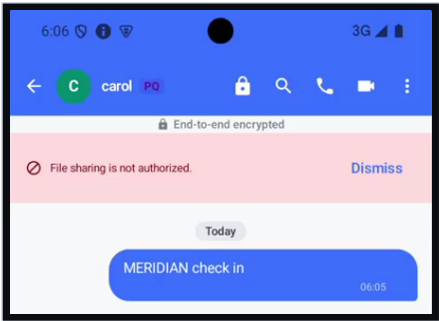
A relationship grant runs one way. `alice → carol`, capability `MESSAGE`, direction `A_TO_B`, gives carol no authority to reply. The reverse leg is a separate grant, issued separately, and until it exists the reply is refused.

| RELATIONSHIPS — WHO MAY SAY WHAT, TO WHOM, IN WHICH DIRECTION |   |       |            |           |                  |
|---------------------------------------------------------------|---|-------|------------|-----------|------------------|
| FROM                                                          |   | TO    | CAPABILITY | DIRECTION | MISSION          |
| alice                                                         | → | carol | MESSAGE    | A_TO_B    | mission_595a3684 |
|                                                               |   |       |            |           | ACTIVE           |

Tunnel Command — relationships. One capability, one direction.

## 02 Capability separation

Authority to send a message is not authority to send a file. Each capability is granted, and refused, on its own. The endpoint states the refusal in its own words, at the moment the operator tries to use what they do not hold.



Tunnel Mobile on Android — the file capability is not granted.

## 03 Mission control

A mission moves from `ACTIVE` to `SUSPENDED` in one action at Command, and governed operations stop across every endpoint under it. Resuming restores authority the way it left, with no restart, reinstallation or re-enrollment.

| MISSIONS         |                    |           |       |         |
|------------------|--------------------|-----------|-------|---------|
| MISSION          | NAME               | STATUS    | EPOCH | MEMBERS |
| mission_595a3684 | OPERATION MERIDIAN | SUSPENDED | 1     | 3       |

Tunnel Command — OPERATION MERIDIAN, suspended.

## 04 Time-bound authority

Authority can be issued to expire. A lease carries a sequence and a remaining term; when it ends, the authority ends with it and no operator has to act. This brief describes the mechanism. A lease is not shown lapsing in the published recording, and it is not claimed to be.

Every refusal shown on this page is the product's own, generated by the application on the endpoint. Nothing in these frames is a mockup, a composite or a reordering: each is a frame of the demonstration published at [tunnelsovereign.com/demo](https://tunnelsovereign.com/demo).

## 04 • BEYOND MESSAGING

## The same authority model, applied to protected digital assets.

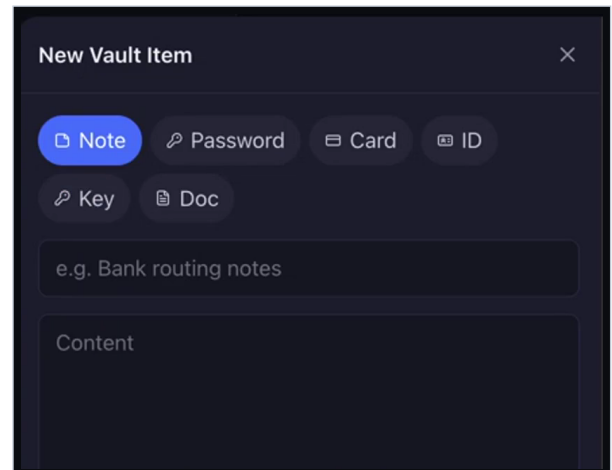
Vault holds material an operator needs and an organization is accountable for: notes, passwords, cards, identity documents, keys and documents. It is governed by the authority plane that governs communication, which is why it belongs to this product rather than to a separate one.

### WHAT IS IMPLEMENTED TODAY

The authority plane covers the vault path on the Android endpoint and the Vault on the macOS desktop endpoint. Content is sealed on the endpoint. Tunnel Command does not receive protected Vault content and does not hold the keys required to open it.

### STANDING GOVERNS ACCESS

While the governing standing is valid, the protected operation proceeds. When that standing changes — a mission suspended at Command, or a duress state declared on an endpoint where duress is implemented — Vault refuses access and says so.



The desktop endpoint on macOS — a new Vault item. Notes, passwords, cards, identity documents, keys and documents.

### WHY THE REFUSAL IS UNINFORMATIVE

The refusal wording is deliberately the same across causes. A refusal that revealed which cause produced it would tell whoever is holding the device what the operator had just done.

### STANDING, AND WHAT FOLLOWS FROM IT

#### STANDING VALID

The protected operation proceeds.

#### STANDING CHANGED

Vault refuses access, and says so.

A standing changes when a mission is suspended at Command, or when a duress state is declared on an endpoint where duress is implemented.

### WHAT THIS SECTION DOES NOT CLAIM

- Nothing here is a claim about recovery of Vault material, about offline behavior beyond the bound stated on the previous page, or about sharing semantics between principals.
- Duress is implemented on Android. iOS and macOS do not have it, and the demonstration says so.
- Duress performs no wipe, destruction, concealment, decoy or anti-forensics. That is deliberate: destruction under coercion converts a coercion event into permanent data loss decided by whoever applied the coercion.

# What Tunnel Command governs, and what it does not require.

The question a security buyer asks first is what an administrator can see. The answer is structural: Command holds what governing authority requires, and does not require what reading the communication would require.

COMMAND GOVERNS

- Enrollment, and the single-use invitation that is the only way in
- Principal and device state, including device binding
- Presence, and the authority generation each endpoint currently holds
- Missions, and their operational status
- Relationships — who may communicate with whom, in which direction
- Capabilities, granted one at a time
- Authority leases, and their expiry
- Freeze, revoke and duress states
- Governance events
- One-time pre-key health

COMMAND DOES NOT REQUIRE

- Message content
- Protected Vault content
- Payload keys
- Endpoint private keys

Tunnel Relay reads the outer envelope in order to carry, schedule and expire a sealed bundle. It does not hold the keys required to open the sealed section.

This is a statement about what the control plane needs in order to work. It is not a claim that an administrator can observe nothing. Governing authority requires knowing who is enrolled, which endpoints exist, who may reach whom, with which capability and under which mission — and Command holds exactly that. What it does not require, and does not receive, is the content of the communication it authorizes.

| ENDPOINTS            |                                             |                   |                |                            |                 |                            |                           |                           |                                     |
|----------------------|---------------------------------------------|-------------------|----------------|----------------------------|-----------------|----------------------------|---------------------------|---------------------------|-------------------------------------|
| WHO                  | DEVICE / PLATFORM                           | ENROLMENT         | BINDING        | PRESENCE                   | AUTHORITY       | MISSION                    | LEASE                     | CAPABILITIES              | OPK HEALTH                          |
| alice<br>b28baea5... | android<br>app 2.4-staging · contract 1.0.1 | BOUND<br>SOFTWARE | BOUND<br>alice | ONLINE<br>last seen 4s ago | SYNCED<br>gen 8 | mission_595a3604<br>ACTIVE | ACTIVE<br>seq 1 · in 168m | FILE, MESSAGE, VOICE_NOTE | OK<br>100 unused · uploaded 13m ago |
| carol<br>acff5e69... | ios<br>app 2.4 · contract 1.0.1             | BOUND<br>SOFTWARE | BOUND<br>carol | ONLINE<br>last seen 3s ago | SYNCED<br>gen 6 | mission_595a3604<br>ACTIVE | ACTIVE<br>seq 1 · in 170m | none                      | OK<br>98 unused · uploaded 11m ago  |
| dave<br>a83cb709...  | macos-desktop<br>app 2.0.0 · contract 1.0.1 | BOUND<br>SOFTWARE | BOUND<br>dave  | ONLINE<br>last seen 4s ago | SYNCED<br>gen 5 | mission_595a3604<br>ACTIVE | ACTIVE<br>seq 1 · in 171m | none                      | OK<br>97 unused · uploaded 10m ago  |

Tunnel Command — the endpoint record. Enrollment, binding, presence, authority generation, mission, lease, capabilities and pre-key health. There is no column for what was said.

THREE QUESTIONS, ANSWERED STRUCTURALLY

Can an administrator read a message?

Command does not receive message content, and does not hold the keys that would open it. It authorizes; it does not decrypt.

Can an administrator open a Vault item?

Protected Vault content is sealed on the endpoint. Command does not receive it.

What does the relay see?

The outer envelope it needs in order to carry, schedule and expire a bundle. Not the sealed section.

# Implementation is not evidence. This page separates them.

Tunnel Sovereign operates across Android, iOS and macOS. Assurance evidence is platform-specific: physical verification currently covers Device Authority on one Android handset model and the operator ceremony at Command, while physical acceptance of the application path is tracked separately and remains outstanding.

| PLATFORM | AUTHORITY PLANE – IMPLEMENTED                                                                 | DEMONSTRATED                                                                                       | PHYSICAL EVIDENCE                                                                           |
|----------|-----------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------|
| Android  | Authority plane on the application's real send, file, voice-note, call, room and vault paths. | Automated and adversarial evidence, and an end-to-end run in a controlled development environment. | Device Authority only, on one handset model. The application path awaits physical evidence. |
| iOS      | Authority plane integrated on the operator endpoint.                                          | End-to-end run in a controlled development environment, on the iOS Simulator.                      | Open. Physical evidence for iOS remains to be established.                                  |
| macOS    | Authority plane integrated on the desktop endpoint, including Vault.                          | End-to-end run in a controlled development environment, on a local build.                          | Open. Physical evidence for macOS remains to be established.                                |

HOW TO READ THIS TABLE

Implemented means production-intended code exists on the path described. Demonstrated means automated, adversarial or controlled end-to-end evidence supports the behavior; it is not physical endpoint verification. Physical evidence means the property was demonstrated on real hardware, through the path it describes. A property climbs this ladder by acquiring a different kind of evidence, never by becoming more important.

PLATFORM PARITY IS NOT CLAIMED

The duress state is implemented on Android; iOS and macOS do not have it. The published demonstration runs the iOS endpoint on the iOS Simulator, and the recording says so on screen. Nothing in this brief asserts feature parity or evidence parity across the three platforms, and the table above is the authority on which is which.

Full current evidence register, property by property: [tunnelsovereign.com/assurance](https://tunnelsovereign.com/assurance)

THE PUBLISHED DEMONSTRATION

This demonstration shows the current application and control-plane behavior of the real product. It is not physical acceptance evidence: physical assurance is tracked separately, by scope and by platform, in Assurance. The recording runs 1 minute 43 seconds and is published at [tunnelsovereign.com/demo](https://tunnelsovereign.com/demo).

This table describes what exists today. It is not a roadmap, it carries no dates, and no state on it is promoted in anticipation of work that has not been done.

# Where the evidence stands.

Device Authority and the operator ceremony are physically verified within stated scopes. Physical acceptance of the application path is outstanding, and external assessment remains open.

THE EVIDENCE LADDER

|                     |                                                                                                               |
|---------------------|---------------------------------------------------------------------------------------------------------------|
| DESIGNED            | The architecture exists. Implementation evidence is not yet sufficient.                                       |
| IMPLEMENTED         | Production-intended code exists on the path the property describes.                                           |
| VERIFIED            | Automated and adversarial evidence supports the property. This is not physical endpoint verification.         |
| PHYSICALLY VERIFIED | Demonstrated on real hardware, through the path the property describes, under controlled evidence conditions. |
| EXTERNALLY ASSESSED | Examined by an independent qualified third party. Nothing on this page has reached this state.                |

THE PUBLIC ASSURANCE SUMMARY, IN THREE SCOPES

Device Authority: physically verified, on Android, one handset model

A device identity is a P-256 key generated in the Android Keystore, non-exportable, hardware-backed where the platform allows, with attestation-chain verification. Bind, reconnect, reboot, rotate, revoke and post-revoke refusal were demonstrated on real hardware. The scope is one handset model, which makes it a demonstration rather than a device compatibility matrix. iOS and macOS carry their own evidence state, which Assurance sets out platform by platform.

Human Authority: physically verified, at Command

An operator authenticating with a physical hardware security key, producing a Command session that carries an authority role and is recorded in a verifying audit chain. It proves the operator step, and only that step. The device key, the organization root and every payload key sit outside its scope, as does any endpoint capability.

Physical acceptance of the application path: outstanding

Two-endpoint acceptance of the application path remains outstanding on every platform, reboot persistence awaits physical execution, and the duress gesture and its canary delivery are pending. This class of evidence is tracked separately from automated and controlled-environment verification, and it is not claimed until it exists. Independent external assessment remains open for every property on this page.

EXTERNAL ASSESSMENT – NOT YET COMPLETED

No property described in this brief has been examined by an independent qualified third party. Every test suite behind it was written by the implementation's own authors. Sovereign Inc. holds no certification, accreditation or government operating approval, and represents none anywhere.

ASSESSMENT AND APPROVAL – CURRENT STATE

|                                            |      |                                 |                 |
|--------------------------------------------|------|---------------------------------|-----------------|
| Independent security evaluation            | OPEN | Penetration assessment          | OPEN            |
| Cryptographic implementation review        | OPEN | Certification and accreditation | OPEN            |
| Government operating approval              | OPEN | CNSA 2.0                        | GAP, QUANTIFIED |
| Reproducible builds and production signing | OPEN | Export-control classification   | UNDER REVIEW    |

Every statement on this page is generated from the source behind [tunnelsovereign.com/assurance](https://tunnelsovereign.com/assurance) which carries the register in full, property by property, with the limit stated beside each one.

## 08 • THE EVALUATION

# What a Controlled Evaluation is.

A bounded environment in which a qualified organization exercises the current authority model against the real application clients and observes the control-plane behavior — under a scope, a duration and a set of questions agreed in writing before it begins.

## THE EVALUATION ENVIRONMENT

- An isolated evaluation environment, on a separate tenant.
- Officer authentication at Command with a physical hardware security key.
- The current Android, iOS and macOS application paths.
- Authority granted, changed and withdrawn from Tunnel Command during the evaluation.
- Tunnel Relay operated separately from Tunnel Command.
- Governance and evidence observations against the criteria agreed in scoping.
- No dependency on the production Tunnel Messenger service.

## THE ORGANIZATION PROVIDES

- An evaluation owner who can make the deployment decision.
- A technical contact for the environment and the devices.
- The devices and the network conditions the evaluation runs under.
- The questions the evaluation has to answer, in writing.

## HOW AN EVALUATION RUNS

### 01 SCOPING

What the evaluation must answer, who the evaluators are, which environment it runs in, and what evidence would satisfy the risk owner.

### 02 DEPLOYMENT

A dedicated deployment configured for the agreed scope, in the environment the evaluation requires.

### 03 OPERATION

Your operators use the platform under conditions you set: your devices, your compartments, your links, your degradation scenarios.

### 04 TECHNICAL REVIEW

Architecture and trust-boundary sessions with your evaluators, with an engineer present.

### 05 FINDINGS

A written record of what was configured, what was exercised, what was observed and what remains open.

## SOVEREIGN INC. PROVIDES

- The evaluation deployment for the agreed scope.
- An architecture and trust-boundary briefing, with an engineer present.
- Deployment support through installation and enrollment.
- A findings review and a written outcome against the agreed criteria.

### A CONTROLLED EVALUATION IS NOT PHYSICAL ACCEPTANCE

An application and control-plane evaluation establishes how the product behaves. It does not by itself produce physical device acceptance evidence, an independent security assessment or a certification. Those are separate milestones, tracked separately, and this brief does not merge them.

## WHAT AN ORGANIZATION HOLDS AT THE END

|                                   |                                                                                                    |
|-----------------------------------|----------------------------------------------------------------------------------------------------|
| <b>A documented outcome</b>       | Findings against the criteria agreed before the evaluation began, not criteria written afterwards. |
| <b>A procurement record</b>       | A scope, an acceptance criterion and a delivery against it.                                        |
| <b>A security findings review</b> | Anything found is routed through a security reporting process rather than a slide.                 |
| <b>A decision, either way</b>     | On a known date. An evaluation that cannot conclude is a failed evaluation.                        |

## 09 • SCENARIOS

# Eight exercises a technical evaluator can run.

Scope is agreed in the scoping session. These are the exercises organizations most often want to see, and each produces an observation rather than an impression.

## 01 Account is not authority

### EXERCISE

Enroll and bind an endpoint, then withhold every governed authority.

### EXPECTED OBSERVATION

The endpoint is enrolled and online and is authorized for nothing. Governed operations are refused on the endpoint's own screen.

## 03 Capability separation

### EXERCISE

Grant MESSAGE and withhold FILE; attempt a file; then grant FILE and repeat.

### EXPECTED OBSERVATION

The file is refused, then the same file moves, with nothing changed on the endpoint except its authority.

## 05 Mission suspension

### EXERCISE

Suspend the mission at Command, exercise governed operations, then resume it.

### EXPECTED OBSERVATION

Governed operations across the endpoints under that mission refuse. Resuming restores authority with no re-enrollment.

## 07 Duress on the endpoint

### EXERCISE

On Android, where duress is implemented, declare duress from the endpoint and attempt governed operations.

### EXPECTED OBSERVATION

Governed operations and Vault refuse, in wording that does not disclose the cause. Command holds the endpoint in duress. Nothing is wiped, hidden or destroyed.

## 02 Directional relationship

### EXERCISE

Grant  $A \rightarrow B$  for one capability, and leave  $B \rightarrow A$  ungranted.

### EXPECTED OBSERVATION

A reaches B. B is refused when it tries to reply, until a separate grant is issued.

## 04 Live authority withdrawal

### EXERCISE

Keep the endpoint online and withdraw one relationship capability at Command.

### EXPECTED OBSERVATION

Everything else the endpoint holds is untouched. The withdrawn operation is refused the next time it is attempted.

## 06 Vault under authority

### EXERCISE

Exercise a protected Vault operation under valid standing, change the governing standing, and repeat.

### EXPECTED OBSERVATION

The operation proceeds, then is refused, in wording that does not disclose which change produced it.

## 08 Restart and persistence

### EXERCISE

Restart the application after an authority change, and attempt the operation again.

### EXPECTED OBSERVATION

The refusal is still there and Command still holds the same state. Authority does not resurrect by restarting.

### WHAT THESE EXERCISES ARE NOT

These are application and control-plane exercises. Passing them establishes how the product behaves; it is not physical acceptance evidence, and this brief does not present it as such. Physical acceptance of the application path is outstanding on every platform, and is tracked as its own item on the public assurance register.

## 10 • BOUNDARIES

# What an evaluation can establish, and what it cannot.

An evaluation that states its boundary is worth more than one that does not. This page is that boundary, and it is the same one used when the findings are written.

## CAN HELP ESTABLISH

depending on the scope agreed in advance

- Correctness of authority transitions
- Control-plane behavior across Android, iOS and macOS
- Relationship directionality
- Capability separation
- Mission suspension and resumption behavior
- Lease and policy behavior
- Governance observations against the agreed criteria
- The confidentiality boundary at Command
- Integration fit with the organization's environment

## DOES NOT BY ITSELF ESTABLISH

these are separate milestones

- External certification or accreditation
- An independent security assessment
- Production-scale capacity
- Universal device compatibility
- Complete physical acceptance across every platform
- Regulatory approval
- Government operating authorization

## KNOWN LIMITS AND NON-CLAIMS

|                            |                                                                                                                                                                                                                                                                                           |
|----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Assurance</b>           | No completed external assessment. No certification and none in progress: not certified, not accredited, not listed under any scheme, and no approval for classified information is represented.                                                                                           |
| <b>Physical evidence</b>   | Physical acceptance of the application path is outstanding on Android, iOS and macOS alike, and reboot persistence awaits physical execution. This class of evidence is tracked separately from automated and controlled-environment verification, and it is not claimed until it exists. |
| <b>Reach</b>               | No remote destruction is claimed, and no control over an endpoint that is unreachable. Withdrawal cannot reach a disconnected endpoint; residual authority is bounded by the last signed lease.                                                                                           |
| <b>Duress</b>              | Duress performs no wipe, destruction, concealment, decoy or anti-forensics, by design. It refuses access and tells the authority that duress was entered, and nothing about why.                                                                                                          |
| <b>Governance receipts</b> | Receipts are signed and minimal, but the receipt signing key is software-protected in application-private storage. Receipts are not hardware-attested.                                                                                                                                    |
| <b>CNSA 2.0</b>            | A quantified gap. The suite is ML-KEM-768 with Ed25519; National Security Systems require ML-KEM-1024 and ML-DSA-87, so a parameter migration is required.                                                                                                                                |
| <b>Build integrity</b>     | Reproducible builds and production signing are open, and are identified internally as the highest-value outstanding security work.                                                                                                                                                        |
| <b>Export control</b>      | Referred for specialist review. No export classification is asserted.                                                                                                                                                                                                                     |
| <b>Commercial</b>          | No customer, contract, pilot, operational deployment or design partner is claimed, and no customer-operated sovereign deployment has been delivered. When one exists and can be named, it will be named.                                                                                  |

A security product that cannot state its own boundaries has been marketed rather than engineered. This page is the boundary, and it is published in full, property by property, on the assurance register.

# Tell us what the evaluation has to prove.

Qualification is a conversation rather than a form. The scoping session establishes what the evaluation must answer, who will assess it and what evidence would satisfy the risk owner.

WHAT TO INCLUDE IN A FIRST MESSAGE

- The organization, and the risk owner who can make the deployment decision.
- The intended use case.
- The platforms and endpoints in scope.
- The deployment environment: managed, or infrastructure you hold.
- The success criteria the evaluation has to meet.
- A technical sponsor for the environment and the devices.

**Request a Controlled Evaluation**  
[tunnelsovereign.com/evaluation](https://tunnelsovereign.com/evaluation)

**Watch the demonstration**  
[tunnelsovereign.com/demo](https://tunnelsovereign.com/demo)

SOVEREIGN INC.

|                   |                                                                                    |
|-------------------|------------------------------------------------------------------------------------|
| Legal entity      | Sovereign Inc.                                                                     |
| Jurisdiction      | Delaware, United States                                                            |
| Product           | Tunnel Sovereign                                                                   |
| Category          | Sovereign Communication Authority                                                  |
| Leadership        | Francesco Tripepi, Founder and Chief Executive Officer                             |
| Stage             | Available for Controlled Evaluation                                                |
| Written enquiries | <a href="mailto:enterprise@tunnelsovereign.com">enterprise@tunnelsovereign.com</a> |

Company identity, in full: [tunnelsovereign.com/company](https://tunnelsovereign.com/company)

Evaluations are conducted on unclassified material. Do not submit classified information, operational secrets, credentials or other sensitive material through the website or in initial correspondence. Handling of any sensitive material within an evaluation is agreed beforehand, in writing, under the customer's own procedures.

Product configurations, integrations and operational capabilities are delivered according to customer requirements, deployment environment, validation scope and applicable authorization. No approval for classified information is represented.

ABOUT THIS DOCUMENT

This is a public document. Its assurance statements are generated from the same source as the public assurance register, so the two cannot diverge. A materially revised edition carries a new revision number, and the edition in hand is identified on the cover.