ORBITX

The Secure Orbital Fabric

A technical white paper on non-territorial storage, pure-space routing, and a cryptographic root of trust that never touches Earth.

Architecture · Claim elements · Data flows · Use cases

August 2026

Confidential — distributed to qualified counterparties.

1. Abstract

Orbital compute is no longer a research program. Power, cooling, and land constraints on Earth are pushing inference and training into space. That migration is incomplete if the data those systems consume and produce still depends on terrestrial networks, terrestrial key management, and terrestrial jurisdiction.

This paper describes the OrbitX Secure Orbital Fabric: five interlocking space systems that together provide (i) air-gapped, multi-petabyte-class storage (design target) that never faces a ground terminal directly for user files; (ii) a high-orbit routing backbone (network satellites at ≥ 2,000 km, MEO or GEO) whose inter-satellite leg never takes a terrestrial long-haul hop; (iii) an intermediary LEO overlay that cross-straps RF bands and decongests ground networks (preferred embodiment: without demodulating through a station); (iv) a near-continuous dump path for Earth-observation and other high-inclination collectors; and (v) onboard generation and inter-satellite distribution of cryptographic keys, with no ground-facing transponder on the key node.

The architecture is designed as a substrate, not as a competitor to orbital GPU fleets. Pure-compute constellations still need a place to put weights, training sets, classified archives, and outputs, and a way to move that data without exposing it to the public internet or to a foreign (or even domestic) data-center statute. The Fabric is that layer. It can be flown as an OrbitX service or licensed as a technical stack.

The design is grounded in granted U.S. patents covering each layer. Patent numbers are cited as technical references. This paper is a description of the system, not a corporate history.

2. The incomplete orbital stack

2.1 What compute-in-orbit does not solve

Placing accelerators in orbit solves energy and thermal envelopes. It does not solve four adjacent problems that determine whether orbital compute is usable for the workloads that actually need it — sovereign, regulated, and high-integrity data.

- Storage. Model weights, training corpora, sensor archives, and classified stores still live in buildings. Those buildings have jurisdictions, cooling plants, and attack surfaces.
- Routing. Most satellite paths still hairpin through a ground station and a terrestrial backbone. The long-haul hop is the exposure.
- Collection windows. Polar and high-inclination Earth-observation spacecraft can dump only when they see a dish. The orbit is mostly dark to the network.
- Keys. Even “encrypted in space” systems typically mint and rotate keys in a room on Earth. Compromise of that room compromises the constellation.

2.2 Design requirement

A complete orbital information system therefore needs a storage plane that cannot be subpoenaed or raided as a terrestrial facility; a routing plane whose default path is space; a way to use existing RF fleets without rebuilding them; a dump path that is open for most of an observation orbit; and a cryptographic root that is generated and distributed where the ciphertext lives. Those five requirements map onto the five layers in §4.

3. Design principles

- Indirect-only storage. Storage satellites neither accept nor transmit data files directly to or from terrestrial terminals. The only legal path is ground terminal → communications satellite (typically GEO) → storage satellite, and the reverse.
- Space is the primary path. Ground-to-ground, ground-to-orbit, and orbit-to-orbit sessions stay on the fabric. Terrestrial long-haul is not the default.
- Isolation is architectural, not procedural. Air-gap is enforced by antenna geometry, transponder absence, and routing rules — not by a policy overlay on an internet-connected node.
- Redundancy is orbital, not rack-level. Files are fragmented and recorded across multiple satellites and multiple orbital planes. Retrieval is simultaneous through the optical mesh.
- Keys never touch Earth. Generation, wrapping, rotation, and distribution of the root occur onboard. Subsequent ciphertext can remain on the fabric for its entire life.
- Leverage existing fleets. The overlay is designed to sit on top of heterogeneous GEO and LEO assets — frequency translation and decongestion in space — rather than requiring a green-field rebuild of global RF capacity.
- Modular growth. Nodes can be added, retired, or isolated as private sub-constellations without redesigning the protocol of the ring.

4. Five-layer architecture

The Fabric is a stack, not a menu. Each layer is independently useful; the security and operational properties compound when they are flown together.

Layer	Function	Reference

01 Orbital Storage	LEO radiation-hardened store; optical ISL mesh; no direct ground file path	US 9,602,580 B2 US 10,218,431 B2
02 Secure Global Backbone	GEO / high-MEO equatorial ring; end-to-end space routing	US 12,355,547 B2
03 Cross-Strap & Decongestion	LEO relay ring; in-space band conversion; peak-traffic offload	US 10,958,335 B2
04 Earth-Observation Highways	Intermediate mesh; 50–80% dump window; approved delivery	US 11,040,786 B2
05 Pure-Space Key Generation	Onboard HSM / TRNG; ISL-only key distribution; no ground RF	US 12,407,505 B1

4.1 Orbital Storage Layer

US 9,602,580 B2 (2017) · US 10,218,431 B2 (2019 continuation)

A constellation of low-Earth-orbit data-storage satellites, preferably in low-inclination or equatorial planes at roughly 700–900 km (claims cover altitudes below 2,000 km), is interconnected by a continuous optical inter-satellite mesh. Each storage node is a radiation-shielded, solar-powered platform with processors, mass storage, batteries, and communications arrays. The constellation is sized as a multi-petabyte-class system and can grow by adding nodes rather than resizing a single vehicle.

The governing constraint is isolation. Storage satellites are not permitted to accept or transmit data files directly to or from terrestrial terminals. A ground facility reaches storage only through a communications satellite — typically geostationary — that acts as a gateway. The same rule applies on retrieval. That single architectural decision removes the storage plane from terrestrial jurisdiction, from internet routing, and from the class of attacks that begin with a public address.

Claim elements (storage and transfer)

- Indirect-only access path: ground terminal → GEO (or other) communications satellite → LEO storage satellite, and the reverse. Direct ground-to-storage file transfer is excluded.
- Continuous optical ISL mesh so that any storage satellite can retrieve data stored on any other storage satellite, including after a node failure. The ring is self-healing.
- File fragmentation with redundant recording across at least two storage satellites and at least two orbital planes. Fragments are retrieved simultaneously and reassembled at the authorized gateway.
- De-duplication prior to recording, to conserve mass, power, and downlink.
- Radiation shielding surrounding the storage elements, with processors and power (solar arrays plus batteries) sized for continuous operation.

- Optional sub-orbital nodes — airships, high-altitude platforms, or floating data centers — as additional hops in the same isolation doctrine, not as substitutes for the orbital store.
- Private or dedicated storage satellites (or private sub-constellations) for tenants that require physical, not merely logical, isolation.

Operationally this is Data Security as a Service: an information plane independent of the public internet and of conventional leased lines. Because data never lands on the terrestrial infrastructure of an unintended jurisdiction, the layer is a direct answer to data-localization statutes, foreign surveillance of undersea cables, and conventional data-center raid or subpoena. The store is physically above every terrestrial network.

4.2 Secure Global Backbone

US 12,355,547 B2 (2025)

A plurality of network satellites in MEO or GEO — each at least 2,000 km above sea level — are fully interconnected by laser or RF inter-satellite links. The resulting loop is a continuous global communications backbone. This is a high-orbit door, not a low-Earth mega-constellation mesh. Any point on Earth that can see a node, and any satellite in any orbit that can close a link to a node, can reach any other such point without a terrestrial long-haul hop on the inter-satellite leg.

This layer is the always-on routing core of the Fabric. Storage (§4.1) hangs below it. Earth-observation highways (§4.4) deliver into it. Key nodes (§4.5) publish onto it. Cross-strap relays (§4.3) offload into it. The backbone is deliberately sparse and high: coverage and persistence, not mass storage.

Claim elements (secure global network)

- End-to-end space paths for ground-to-ground, ground-to-orbit, and orbit-to-orbit sessions. The primary path does not traverse a terrestrial backbone.
- Elimination of ground-based nodes as a required hop, reducing exposure to snooping, hacking, and multi-hop latency.
- Time-windowed access controls: a session may be valid only inside a defined interval, independent of cryptographic validity.
- Encrypted ledgers for authenticity of traffic and of configuration changes on the ring.
- Anomaly detection on unexpected sources, times, or frequencies, with the option to raise an alert or to drop the path.
- Modular expansion: additional satellites may be added to the ring; older nodes may be retired or repositioned without collapsing the mesh.
- Compatibility with laser crosslinks and with traditional RF transponders, so hosted payloads and dedicated vehicles can coexist.

Because the ring sits at or above 2,000 km, a small number of vehicles produces continuous coverage of the populated Earth. LEO storage and LEO relays then provide density and capacity underneath a stable high-altitude core.

4.3 Cross-Strap and Decongestion Overlay

US 10,958,335 B2 (2021)

A modular LEO ring — or a multi-plane set of rings — of relatively simple, single-band or limited-band relay satellites forms continuous communication loops around the Earth. These intermediaries exist to do two jobs that existing GEO fleets do poorly: translate between RF bands without a ground demodulation hop, and move peak traffic off a congested ground station onto an off-peak station via space.

Cross-strapping in this design is performed in orbit. A Ku-band uplink can leave as Ka, K, or C without being brought to a teleport, demodulated, re-modulated, and sent back up. The relay does not have to be a full processing satellite; the claim set is deliberately cheap and expandable. Capacity is added by adding simple nodes, not by replacing the GEO fleet the overlay sits on.

Claim elements (intermediary network)

- In-space frequency translation and band conversion (Ku, Ka, K, C, and mixed) without a requirement to demodulate through a ground station.
- Local network decongestion: non-latency-sensitive or overflow traffic is taken off an overloaded ground station and delivered to an off-peak station through the space ring.
- Path optimization across heterogeneous satellite assets — the overlay is an intelligent traffic engineer, not a parallel internet.
- A low-cost, modularly expandable topology. Nodes are relays, not full storage or full gateway vehicles.
- Continuous loop geometry so that a packet entering the ring can leave it at any later longitude.

The commercial implication is that incumbent GEO operators become more useful, not obsolete. The Fabric does not ask them to rip out transponders. It gives those transponders a space-side way to change band and to shed peak load.

4.4 Earth-Observation Continuous Routing

US 11,040,786 B2 (2021)

Polar and high-inclination Earth-observation satellites traditionally store onboard and dump when they pass a ground station. For a spacecraft that never loiters over a dish, that window is a small fraction of the orbit. The result is latency measured in hours, pressure on onboard recorders, and a political constraint: the only places that can receive the take are the places that have built stations.

An intermediate LEO mesh — preferably equatorial or otherwise complementary to the collector’s inclination — takes the dump almost anywhere in the pass. The mesh then routes the data to an approved GEO or high node, and from there either to a jurisdiction-controlled ground station or directly into the Orbital Storage Layer for sovereign archival and, later, edge analysis. Claims target fifty to eighty percent of the collector’s orbit as a live transfer window.

Claim elements (EO information routing)

- An intermediate LEO relay network that is visible to polar / high-inclination collectors for a majority of the orbit.
- Near-continuous downlink in place of pass-limited dumps, enabling live monitoring and streaming classes of product, not only delayed archive.
- Delivery only to pre-approved ground stations. Jurisdiction is a routing rule, not a post-processing hope.
- Direct feed into the secure orbital store, so the collection event and the archive event can be the same event.
- Reduction or elimination of the requirement to build a planetary ground-station network in order to achieve low-latency EO.

The same path serves SIGINT, missile-warning, weather, and other high-inclination sensors. Anything that currently waits for a dish is a candidate for the highway.

4.5 Pure-Space Key Generation

US 12,407,505 B1 (2025)

The last terrestrial attack surface in an otherwise air-gapped space system is key management. If session keys, wrapping keys, or the root of trust are minted in a ground HSM and uplinked, then the ground HSM is the system. This layer removes that surface.

Dedicated or multi-role satellites generate encryption keys entirely onboard, using only space-based hardware and software — hardware security modules, true random-number generators, and credential stores that never leave the vehicle. Key satellites have no ground-facing transponders for the key function. Distribution is inter-satellite only, onto the optical or RF mesh of the Fabric. Subsequent ciphertext never needs to leave space.

Claim elements (key-generating satellite)

- Onboard generation of symmetric keys (AES-256 class and equivalents) and of asymmetric key pairs, from space-resident entropy.
- Zero ground exposure of the cryptographic root: no key-export path to a terrestrial terminal.
- ISL-only distribution to peer satellites, gateways, and (where authorized) to storage nodes that will wrap objects at rest.
- Endpoint validation against onboard credential stores.
- Key rotation, session management, and hot-standby / backup key satellites so that loss of a vehicle does not lose the root.
- The option for all subsequent encrypted traffic to remain entirely on the space network for the life of the data.

Combined with indirect-only storage and space-primary routing, this produces a system in which the bits, the path, and the keys are all off the planet. That is the closed form of the air-gap.

5. Integrated data flows

The five families are designed to interlock. A representative set of flows:

5.1 Sovereign object store

A tenant encrypts an object under a wrapping key that was minted on a key satellite and delivered over ISL to the authorized GEO gateway. The gateway never holds the root; it holds a session. The object is fragmented, de-duplicated, and recorded across at least two LEO storage satellites in at least two planes. Retrieval is the reverse: simultaneous fragment pull across the optical mesh, reassembly at the gateway, delivery to the same (or another authorized) ground terminal. At no point does a storage satellite speak files to Earth. At no point does a fragment sit in a terrestrial data center of an unintended jurisdiction.

5.2 Continuous collection into archive

A polar EO or SIGINT collector dumps to the intermediate LEO highway for the majority of its orbit. The highway hands the take to the GEO backbone, which either (a) delivers immediately to a pre-approved ground station or (b) writes through to the orbital store under keys that never touched Earth. Collection window and archive window collapse into one.

5.3 Peak-load offload across an incumbent fleet

A GEO operator's Ka-band beam is saturated at a particular longitude. Non-latency-sensitive traffic is accepted by a LEO cross-strap node, translated in space, carried along the ring, and delivered to an off-peak station or to another transponder in another band. No teleport demodulation is required for the translation hop. The incumbent fleet did not have to be replaced; it became more efficient.

5.4 Orbital compute, OrbitX underneath

A third-party GPU constellation trains or infers in orbit. Weights, corpora, and outputs do not return to a terrestrial object store. They land in the Fabric: stored under space-minted keys, moved on the backbone, and — where the tenant requires it — never downlinked at all. OrbitX is not the accelerator. OrbitX is the store, the path, and the root those accelerators run on.

5.5 Properties that only appear at full stack

- True air-gapped / non-territorial storage and transfer. Isolation is a consequence of antenna rules and of the Outer Space operating environment, not of a software policy. Spacecraft remain on a national registry under the Outer Space Treaty.
- Continuous sensor harvest plus immediate secure archival or edge analysis.
- Intelligent traffic engineering across existing GEO fleets without ground intermediaries for band change.
- Zero-trust key management generated and distributed purely in orbit.
- A clean path to hybrid nodes: radiation-tolerant accelerators co-located with LEO storage, so the object and a bounded inference over it never leave the vehicle.

6. Security properties

6.1 Threats the architecture is built to refuse

- Internet-path compromise. There is no public-internet path to a storage node. Files do not traverse leased lines.
- Ground-station as pivot. A compromised dish can at most speak to a gateway under time-windowed, keyed rules. It cannot enumerate the store. Key nodes do not listen to ground RF.
- Jurisdictional seizure of a data center. There is no building that holds the corpus. Fragments live on vehicles in more than one plane.
- Cable tap / foreign intercept of long-haul. The primary path does not use the long-haul.
- Key-ceremony compromise. The root is not in a cage in a city. Rotation and standby are orbital.
- Single-vehicle loss. Fragmentation across satellites and planes, plus a self-healing optical ring, plus backup key nodes, are the availability story.

6.2 What remains a terrestrial problem

Authorized ground terminals still exist. They are the human and enterprise edge: a SCIF, a sovereign gateway, a bank's uplink. The Fabric does not pretend those facilities are invulnerable. It pretends they are the only terrestrial objects in the threat model, and it makes them replaceable — another authorized terminal, another longitude, another nation — without moving the corpus. Time-windowed access and anomaly detection on the backbone are the controls that sit in front of those terminals.

6.3 Tenancy and isolation

Logical tenancy (keys, namespaces, time windows) is the default. Physical tenancy is an offered mode: a dedicated storage satellite or a private sub-constellation for a sovereign or regulated customer that requires isolation at the vehicle, not at the record. Both modes use the same backbone, the same key doctrine, and the same optical mesh protocols.

7. Use cases

7.1 Sovereign and defense cloud

A classified or "black" store that never lands on foreign — or even domestic — terrestrial networks. Continuous EO and SIGINT dump into that store. Command-and-control and data exchange among deployed forces, ships, aircraft, and satellites without depending on a vulnerable ground infrastructure. Keys that cannot be lifted from a ground station. Private vehicles for the highest isolation tier.

7.2 Hyperscale AI and orbital compute

Pure-compute constellations still need a place to put weights, training sets, and outputs. The Fabric is the complementary storage and transfer layer — not a competitor to GPU fleets, the substrate they run on. A hyperscaler can keep regulated or high-value corpora off every terrestrial region while still feeding orbital accelerators at optical rates. Disaster-recovery of a terrestrial training run can be a write-through to orbit rather than a second region.

7.3 Continuous Earth observation

Always-on downlink and long-term archive without building a planetary ground-station network. Products delivered only to approved jurisdictions. Commercial imagery operators gain latency; governments gain control of where the take is allowed to land; both gain an archive that is not a building.

7.4 Financial-grade cold storage

Transaction ledgers, settlement data, and core records in a physical air-gap. Space-based tokenization and HSM-like services under keys that were never in a bank cage. Cross-border movement that sidesteps data-localization conflicts because the object is not in a country. Recovery from a terrestrial outage is a keyed retrieval from orbit, not a failover to another vendor's region.

7.5 Critical-infrastructure air-gap

A disaster-recovery vault that survives EMP, grid failure, and nation-state attack on terrestrial data centers. Grid operators, water, aviation, and public-health records can be stored under the same isolation doctrine. The recovery terminal can be stood up after the event; the corpus does not wait in the blast radius.

7.6 Lunar and deep-space relays

The same isolation, routing, and key doctrines extend to cislunar and interplanetary data. A fabric whose default path is already space does not have to be redesigned when the destination is no longer Earth. Early cislunar use is a relay and store-and-forward node on the GEO ring and on high-MEO; later use is the same protocol on vehicles beyond GEO.

8. Deployment architecture

The stack is modular. It is not a requirement to fly all five layers on day one. The protocol and the claim language are written so that capacity and coverage grow by adding vehicles of known types.

- Phase 0 — Backbone and keys. Hosted or dedicated GEO / high-MEO nodes prove space-primary routing, time-windowed access, and onboard key generation with ISL distribution. This is the smallest closed security argument.
- Phase 1 — First storage and cross-strap pair. A small LEO ring writes fragments under space-minted keys and demonstrates indirect-only retrieval through the gateway. An isolated tenant (sovereign or regulated) is the first production workload.
- Phase 2 — EO highway overlay. Polar collectors dump into the mesh. Direct feed into storage is turned on. The optical ring expands in plane count and in node count.
- Phase 3 — Hybrid and beyond-GEO. Radiation-tolerant edge inference co-located with storage. Cislunar relay path using the same routing and key doctrine.

Two deployment rules are load-bearing. First, leverage what already flies: the overlay is designed to interoperate with and enhance existing GEO fleets rather than requiring a green-field rebuild of global RF capacity. Second, offer isolation as a product: individual storage satellites or private sub-constellations for sovereignty and multi-tenant separation, using the shared backbone and key plane.

Launch vehicle, bus manufacturer, and optical-terminal vendor are integration choices, not architectural ones. The paper does not freeze them. The isolation rules, the mesh, and the key doctrine are the architecture.

9. Position in the orbital-compute market

The orbital data-center sector is concentrating on accelerators in orbit: large-scale GPU payloads, solar power, and thermal rejection in vacuum. That work is necessary and it is not this work. Those constellations still require high-integrity storage of the datasets and model outputs they consume and emit, plus a networking fabric that can move that data without exposing it to the public internet or to a terrestrial region.

OrbitX's position is the complementary layer. The cost thesis is a relatively low-cost LEO storage and relay constellation plus leverage of existing GEO capacity, not a million-satellite compute build. The granted claims give both a defensive and an offensive IP position against pure-play compute systems that will eventually need storage, routing, continuous collection, and a root of trust that does not live in a ground cage.

The operating modes are two, and they are compatible: OrbitX flies the fabric as a service, or OrbitX licenses the stack to a partner that flies metal. In both modes the technical object is the same.

10. Closing

Compute will leave Earth because physics demands it. Trust, storage, and routing must leave with it — or the orbital age inherits every vulnerability of the terrestrial one. The Secure Orbital Fabric is the design for those three functions: a store that does not face the ground, a path that does not take the long-haul, and a key that is not minted in a city.

The five layers are specified, claimed, and intended to be flown as one system. This paper is the technical description of that system.

Appendix A — Patent references

Cited as technical references for the layers described above. All listed instruments are granted U.S. patents. OrbitX licenses and packages the fabric; record title is listed below.

Patent	Title	Record owner	Year
US 9,602,580 B2	Space-Based Electronic Data Storage and Transfer Network System	Cloud Constellation Corp.	2017
US 10,218,431 B2	Space-Based Electronic Data Storage and Transfer Network System (continuation)	Cloud Constellation Corp.	2019
US 10,958,335 B2	Intermediary Satellite Network for Cross-Strapping and Local Network Decongestion	Cloud Constellation Corp.	2021

US 11,040,786 B2	Earth Observation Satellite Information Routing System	Cloud Constellation Corp.	2021
US 12,355,547 B2	Secure Global Satellite Network	H. Kaen & J. Kaen	2025
US 12,407,505 B1	Encryption Key Generating Satellite	Hooshang Kaen	2025

— End of white paper —