Nick Clark · Published April 25, 2026 · PDF

How to Build Credentialed Infrastructure Markers for Indoor Positioning

If you run vehicles or robots through a warehouse, port, or indoor facility where GPS does not reach, you have probably reached for a central positioning service that every unit must trust and stay connected to. This guide describes a different architecture: fixed infrastructure markers that carry authority-signed positional data a vehicle reads directly and verifies for itself, with no central positioning server in the loop. It describes an architecture disclosed in U.S. Provisional Application No. 64/049,409, not a shipping library, and its home inventive step is the Marker Track Transport inventive step.

What You Are Building

You are building a positioning layer for vehicles or robots that operate where satellite navigation is unavailable or unreliable: warehouse aisles, port terminals, airfield aprons, indoor floors, tunnels. The unit needs to know where it is and what the local geometry allows, accurately enough to plan and act, and it needs that answer to be trustworthy even if someone tries to lie to it.

The architecture in this guide answers that need with fixed physical markers installed into the infrastructure itself. Each marker stores a small, self-contained record: an identifier, its own position in a coordinate frame, the local geometry around it, and,

critically, an authority credential and cryptographic attestation binding that data to whoever installed it. A unit passing by reads the marker, checks the credential against its own trust model, and consumes the position. There is no central positioning service the unit must query and no server whose uptime becomes your single point of failure. The marker is both the data and the proof of the data.

This is the substance of what the underlying patent disclosure calls the Marker Track Transport inventive step: units navigating along governance-credentialed marker sequences as their primary spatial reference.

Why the Obvious Approaches Fall Short

The usual approaches each solve part of the problem and leave a structural gap.

Plain RFID or barcode tags. Embedding identifier tags in the floor is a well-established idea. The gap is that a bare tag encodes only an identifier or a relay-point code. The unit must then look that identifier up against a remote database to learn what it means, which reintroduces the central dependency you were trying to escape, and the tag itself carries no proof that the identifier is legitimate. Anyone can print another tag with the same number.

Central positioning services. A server that fuses beacons, cameras, or fingerprints and hands each unit a coordinate is accurate and centrally manageable. But every unit now depends on continuous connectivity and on the server's integrity. If the link drops or the service is compromised, positioning degrades for the whole fleet at once.

Computer vision over human-oriented features. Reading painted lines, signs, and reflectors works until those features are worn, dirty, occluded, or simply absent, and it offers no cryptographic notion of whether what the camera sees is authorized ground truth or an adversarial paint job.

Authenticated messaging without authority semantics. Public-key infrastructure and credential-management systems can authenticate that a message came from a valid key. Described accurately, that is what they do well. What they do not do on their own is tell the unit *what kind of authority* signed the data, so a message from a regulator and a message from an unregistered contributor are treated identically. Positioning needs that distinction: geometry from the facility operator should outrank an advisory hint from an unverified source.

The gap common to all of these is that the positional data and its proof of authority are separated. Either the data travels without proof, or the proof exists but carries no notion of graded authority, or both live behind a central service.

The Architecture

The disclosed approach closes that gap by putting signed, authority-scoped data into the marker itself and letting each unit verify it locally. The pieces below all trace to the filed specification.

The marker as a self-contained record. A passive environmental marker is a device installed on or embedded in the infrastructure that stores data and emits it in response to interrogation by a reader on a passing unit. In its passive form it carries no internal battery and no active radio; it derives the energy to respond from the reader's interrogation. The stored data is organized as two rows. A payload row carries the domain fields: a marker identifier, a spatial-reference field giving the marker's position in a coordinate frame, a segment or zone identifier, a delineation-role classification (lane-edge, dock-edge, platform-edge, junction, and so on), a geometry field for local parameters such as curvature, grade, or width, an advisory field, a distance-to-neighboring-markers field, and hazard flags. A separate governance-chain row carries an authority-credential field, a temporal-scope field for how long the data is valid, and a cryptographic attestation binding the stored data to the installing authority.

Because the marker encodes the local geometry directly rather than an identifier to look up, a unit learns what the location *means* from the read itself. No remote database round-trip is required to interpret it.

Authority-credentialed observations. Every observation emitted in the mesh carries an authority credential identifying who is responsible for it. Per the spec, that credential encodes at minimum an issuing-authority identifier, a scope specification, a temporal-validity period, a device-binding attestation tying the credential to the emitting device, and a cryptographic attestation. The attestation mechanism is deliberately not fixed to one primitive; the disclosure contemplates digital signatures, threshold signatures, zero-knowledge attestations, or post-quantum attestations as substitutable so long as they carry the governance-chain properties.

The authority taxonomy. This is what separates the approach from flat message authentication. A consuming unit evaluates each read against a governance-configurable authority taxonomy: a hierarchical trust structure a deploying authority defines for its domain. Each level maps to a behavioral response (from treating the observation as a hard substrate condition down to treating it as an untrusted proposal), a rule for whether the observation may be injected into the unit's planning, an evidential weight, and a supersession rule for when a higher level overrides a conflicting lower one. The spec gives domain examples, including a warehouse or port taxonomy with facility-operations, zone-supervisor, shift-lead, and individual-operator levels. So the same signed-marker mechanism carries different weight depending on who signed it.

A self-maintaining geometry store. A collection of these markers installed across a region constitutes a geometry store that maintains itself by construction. A unit reading a sequence of markers along its path accumulates their data into a geometry track of that path. If an expected marker is missing at an expected position, the unit's failure to

read it is itself a governed observation of marker absence, propagated through the mesh for corrective action. No separate survey process is needed to keep the store current; installing and updating markers *is* the maintenance.

Marker-sequence-primary navigation and read admissibility. During operation, the governance-credentialed sequence of marker reads is the primary spatial reference. At each read the unit validates the marker's authority credential, updates its progress against a pre-departure route manifest, and checks that the next expected marker is consistent with the current marker's distance-to-next data. The unit's own sensors run in parallel for obstacles and conditions the markers do not describe, and conflicts are resolved through the coherence and graduated-response machinery rather than by blindly trusting either source. A marker-read admissibility evaluator rejects spoofed, injected, or otherwise inadmissible reads through several checks named in the spec: integrity attestation, authority credential, sequence consistency with the previous marker's next-expected specification, position consistency against the unit's independently derived position, and temporal consistency. Named adversarial cases include replay, injection, substitution, and denial attacks.

How to Approach the Build

You implement this yourself. The steps below follow the architecture; treat any interface sketch as illustrative, not as code to copy into production.

1. **Define your authority taxonomy first.** Before any hardware, write down the trust hierarchy for your facility and what each level is allowed to assert. This is the design decision everything else hangs on. For a warehouse, that might be facility-operations at the top, then zone-supervisor, shift-lead, and operator.
2. **Design the marker record.** Lay out the two rows. Fix the payload fields you need (identifier, spatial reference, zone, role, geometry, distance, hazards) and the governance-chain fields (authority credential, temporal scope, attestation). An illustrative shape:

```
marker {
  payload:    { id, position, zone, role, geometry, distanceToNext, hazard
  governance: { authorityCredential, temporalScope, attestation }
}
```

3. **Choose a signaling mechanism per environment.** The spec treats the passive signaling channel as selectable: radio-frequency backscatter, modulated optical retroreflection, surface-acoustic-wave chipless tags, near-field magnetic coupling, and others. Pick per your read range, interference, and surface constraints. The inventive part is the credentialed, lineage-attached data, not the physical channel.
4. **Provision credentials at install time.** When an authority installs a marker, it signs the stored data with an attestation bound to that marker and stamps the temporal scope. Keep the marker's data writable under authenticated write so you can revise it in the field without physical replacement, and version each revision.
5. **Build the reader-side verifier.** On the unit, implement the admissibility evaluator as an ordered gate: verify the integrity attestation, check the authority credential against your taxonomy, confirm sequence consistency with the previous marker's next-expected field, cross-check the claimed position against your independent position estimate, and check temporal validity. Reject and log anything that fails; a failed read is itself an observation worth recording.
6. **Make navigation marker-primary, sensor-parallel.** Drive route progress from the verified marker sequence and run sensors alongside for obstacles and off-topology conditions, resolving conflicts through graduated response rather than letting either source win unconditionally.
7. **Plan for mixed coverage.** Design fallback tiers now: full marker density, sparse coverage with reduced speed and higher sensor reliance, and unmarked stretches where the unit runs as a conservative autonomous unit until markers resume. This

lets you deploy markers incrementally rather than needing total coverage on day one.

What This Does Not Give You

This is an architecture, not a drop-in library. There is no package to install and nothing here "just works" out of the box. You implement the marker record, the credentialing, the reader verifier, and the navigation logic yourself, and you choose the cryptographic primitive and signaling channel appropriate to your deployment.

The approach is disclosed in a patent filing. It has not been presented here as a benchmarked or production-proven system, and this guide states no accuracy, latency, or throughput numbers, because the specification states none and you should not infer any. Your achievable positioning accuracy depends entirely on your marker spacing, placement, signaling channel, and reader hardware.

The architecture also does not remove the need for the deploying authority to run a real credentialing process: the trust model is only as good as the key management and installation discipline behind it. And it presumes an environment where you can physically install and maintain markers. In spaces where you cannot place infrastructure, or where the local geometry changes faster than you can revise markers, a fixed-marker approach is the wrong tool.

Disclosure Scope

The architecture described in this guide is disclosed in U.S. Provisional Application No. 64/049,409. This guide is educational: it explains an architectural approach so a developer can understand and build it, and it faithfully traces the disclosed mechanisms to that filing. It is not a warranty, a specification of a product, or an offer of software,

and nothing here should be read as a promise of performance or fitness for any particular deployment. You are responsible for your own implementation and for any intellectual-property clearance relevant to your use.

Marker Track Transport (/marker-track)

All 40 steps → (/inventive-steps)

Rail-analogous guidance on existing roads. Per-segment regulatory authorization.

Provisional application

PRIMARY TECHNICAL DISCLOSURE

- Marker Track Transport: Credentialed Marker Sequences as Primary Routing (/articles/marker-track-transport-credentialed-marker-sequences-as-primary-routing)

SECONDARY TECHNICAL

- Credentialed Markers as Primary Routing Reference (/articles/marker-track/credentialed-marker-primary)
- Per-Segment Authority Attestation (/articles/marker-track/per-segment-attestation)
- Route Manifest Composition (/articles/marker-track/route-manifest-composition)
- Cross-Authority Route Composition (/articles/marker-track/cross-authority-routes)
- Progressive-Density Fallback (/articles/marker-track/progressive-density-fallback)
- Byzantine-Robust Platooning Under Credentialed Sequences (/articles/marker-track/byzantine-platooning)
- Adversarial Marker Rejection (/articles/marker-track/adversarial-marker-rejection)
- Regulatory Segment Approval (/articles/marker-track/regulatory-segment-approval)
- Multi-Class Operator Parameterization (/articles/marker-track/multi-class-parameterization)
- Dual-Use Marker Article: Roadway Infrastructure as Credentialed Device (/articles/marker-track/dual-use-marker-article)

APPLICATIONS · GENERAL

- Automated Guideway Transit Without Rails: A Virtual Fixed Guideway From Credentialed Track Markers (/articles/marker-track/automated-guideway-transit)

- Credentialed Highway Marker Network for GNSS-Denied Autonomous Vehicle Positioning (/articles/marker-track/highway-infrastructure-marker-network)
- Indoor Positioning Without Vendor Lock-In: Credentialed Marker Infrastructure for Hospitals, Airports, and Multi-Tenant Buildings (/articles/marker-track/indoor-positioning-credentialed-infrastructure)
- Audit-Grade Warehouse RFID Positioning: A Credentialed Marker Mesh for DSCSA, FSMA 204, and FTZ Compliance (/articles/marker-track/warehouse-credentialed-rfid-mesh)
- Credentialed Field Markers for Precision Agriculture and GPS-Resilient Autonomy (/articles/marker-track/agricultural-marker-network)
- Credentialed Markers for Construction Site Safety and Autonomous Equipment Authorization (/articles/marker-track/construction-site-credentialed-markers)
- Credentialed Marker Positioning for Underground and Open-Pit Mining (/articles/marker-track/mining-credentialed-positioning)
- Credentialed Trail Markers for National Parks: Multi-Authority Positioning for Hikers, SAR, and Park Shuttles (/articles/marker-track/national-park-trail-markers)
- Smart Stadium Positioning: Credentialed Marker Networks for Event Venues (/articles/marker-track/smart-stadium-event-positioning)

APPLICATIONS · SPECIFIC

- 3M Connected Roads vs Credentialed Marker Architecture (/articles/marker-track/3m-connected-roads)
- Avery Dennison RFID vs Credentialed Marker Observations (/articles/marker-track/avery-dennison-rfid)
- Trimble RTK Alternative for GNSS-Denied Positioning: Credentialed Markers (/articles/marker-track/trimble-rtk-corrections)
- Impinj RFID Alternative: Credentialed Marker Substrate Beyond Item Identity (/articles/marker-track/impinj-rfid)
- NXP RFID IC Alternative: Credentialed Marker Specification Beyond UCODE and NTAG (/articles/marker-track/nxp-rfid-ic)
- Does a RoadVista retroreflectometer read a credentialed road marker? (/articles/marker-track/roadvista-tape)
- Trimble Survey Markers vs Credentialed Machine-Readable Monuments (/articles/marker-track/trimble-survey-marker)
- Zebra RFID Alternative: Credentialed Marker and Track Beyond EPC Identification (/articles/marker-track/zebra-rfid)
- 6 River Systems (Shopify/Ocado) Chuck vs Credentialed Marker and Track (/articles/marker-track/6-river-systems-shopify)

- AutoStore Alternative: Credentialed Marker and Track Positioning for Warehouse Robots (/articles/marker-track/autostore-warehouse)
- Berkshire Grey Alternative: Credentialed Marker and Track for Mixed-Vendor Fulfillment (/articles/marker-track/berkshire-grey)
- Brain Corp Alternative: Credentialed Lane Authority for Mixed-Fleet Floor Care (/articles/marker-track/brain-corp-floor-care)
- Fetch Robotics (Zebra) FetchCore Alternative: Credentialed Marker and Track for Mixed Fleets (/articles/marker-track/fetch-zebra-fulfillment)
- Geek+ Alternative for Multi-Vendor Warehouses: Credentialed Marker and Track (/articles/marker-track/geek-plus-warehouse)
- inVia Robotics Alternative: Credentialed Marker-Track Routing for Multi-Vendor Warehouses (/articles/marker-track/invia-robotics)
- Locus Robotics vs Credentialed Marker and Track Warehouse Positioning (/articles/marker-track/locus-robotics)
- Ocado Smart Platform Alternative: Credentialed Marker-Track Routing Beyond the Grid (/articles/marker-track/ocado-smart-platform)

Marker Track Transport overview → (/marker-track)