DATA SHEET

TRAFFICAUTH

National Mobility Interchange

HIGHLIGHTS

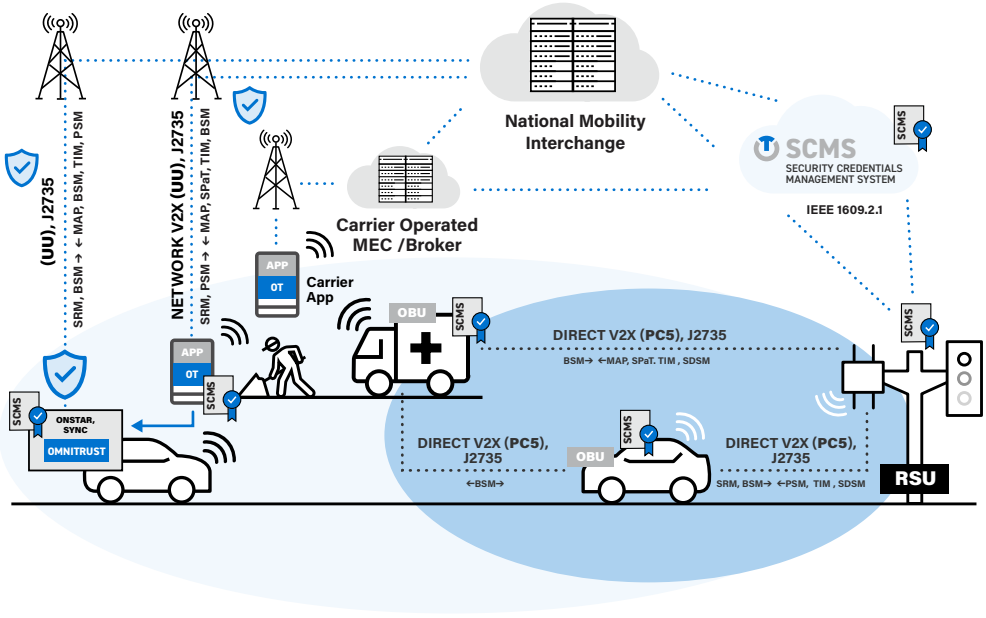
- **Interoperable**
  Seamless end-to-end interoperability using industry-standard protocols.
- **Secure**
  End-to-end security based on the established National Security Credential Management System (SCMS).
- **Standards Compliant**
  Standard SAE J2735 message set with the IEEE 1609.2 security architecture.
- **Flexible SaaS Model**
  Scalable subscription model based on client-defined safety zones.

Activating Intelligent V2X Safety Zones

The National Mobility Interchange (NMI) is a cloud-hosted Software as a Service (SaaS) platform engineered to route critical Network V2X messages with precision and reliability. By enabling subscribers to define and activate specific "safety zones," NMI creates a targeted ecosystem for authentic, interoperable V2X communication.

Rather than simply providing generic coverage, the service uniquely delivers high-performance data exchange where it matters most—at busy intersections, dynamic work zones, and other areas where vehicle and pedestrian interactions are most concentrated.

Hosted on Amazon Web Services (AWS) and compatible with any carrier network, National Mobility Interchange provides the foundational layer for next-generation transportation safety applications.



Features and Capabilities of National Mobility Interchange

STANDARDS-BASED FOR FULL INTEROPERABILITY

NMI ensures seamless end-to-end interoperability by using industry-standard protocols and formats. The default communication protocol is MQTT, and the data payload consists of SAE J2735 compliant packets.

GUARANTEED DATA AUTHENTICITY AND SECURITY

Security is paramount. Every data packet is authenticated with an attached IEEE 1609.2 digital signature. To ensure security, every client system must possess an active SCMS certificate and sign every message it sends in order to post data to a safety zone. Any messages generated from outside the defined zone are automatically rejected by the server, ensuring data relevance and integrity.

HYBRID NETWORK-TO-RADIO CONNECTIVITY

The service creates a powerful, two-way communication flow between the cloud and the physical environment, uniquely bridging cellular networks with the 5.9 GHz safety spectrum. Authorized RoadSide Units (RSUs) can act as relay stations which can receive signed data from the server and broadcast it locally over the safety spectrum, and the same equipment can also capture local broadcast messages and securely deliver them to NMI.

SIMPLIFIED, TOKEN-FREE ACCESS FOR DATA CONSUMERS

To encourage wide adoption and ease of integration, client systems do not need any special tokens or authorization to access the server or subscribe to data streams from a safety zone.

FLEXIBLE AND SCALABLE SAAS MODEL

National Mobility Interchange (NMI) operates on a subscription model where clients pay to activate the safety zones they define. Pricing is based directly on the number of authorized zones, offering a predictable and scalable cost structure.

APPLICATIONS & USE CASES

Smart Traffic Intersections

Activate a safety zone at a busy intersection to provide vehicles with real-time Signal Phase and Timing (SPaT) data, detailed MAP messages of all lanes, and location correction data via RTCM messages. Signal preemption and priority is also available for vehicles that are equipped with authorized certificates.

Traveler Information Messages (TIMs)

Produce and distribute informative TIM messages that can be distributed to all compatible vehicles in the safety zone, over both the network and direct channels.

Location-Specific Safety Alerts

Standard J2735 messages can be used for targeted safety applications such as wrong-way driver detection and alert, flood zones, high winds, icy pavement, etc.

Dynamic Work Zone Safety

Define a temporary safety zone around a work site to deliver critical alerts to passing vehicles about lane closures or rerouting details. Enhance worker safety by triggering alerts if a vehicle gets too close to the work zone perimeter or if a worker accidentally enters an active traffic lane.

Vulnerable Road User (VRU) Protection

Subscribers can receive signed data from any authenticated system within an active zone, enabling applications that protect pedestrians and cyclists in high-traffic areas.

Smart Freight

Enable logistics and delivery fleets to move more efficiently through congested urban areas by securely interfacing with city traffic systems. By allowing authorized freight vehicles to preempt traffic signals along key routes, companies like Amazon, UPS, and FedEx can reduce delays, lower fuel costs, and improve on-time delivery performance.

ABOUT TRAFFICAUTH

TrafficAuth, powered by OmniTrust, secures connected mobility and traffic management networks by establishing trusted identity, authentication, and authorization across vehicles, devices, and traffic systems. Built on the OmniTrust Trust Lifecycle Management platform, TrafficAuth enables verifiable, enforceable trust for the full lifecycle of safety critical traffic infrastructure equipment. Global customers rely on TrafficAuth to secure large-scale networks, including connected vehicles, roadside infrastructure, and sensor networks, ensuring trusted communication, authenticated access, and lifecycle governance across millions of devices. TrafficAuth combines hardware-rooted identity, scalable PKI infrastructure, and policy-driven lifecycle enforcement to support safety-critical transportation, smart infrastructure, and regulated mobility environments.

www.trafficauth.com

OmniTrust