

TRAFFICAUTH

Secure Critical Transportation Infrastructure

APPLICATIONS

- **Intersection validation:** collect data from your roadside units (RSUs) and confirms that they are compliant with the secure credential management service (SCMS) Manager validation policy.
- **Continuous monitoring:** collect samples of blind spot monitoring (BSM) data from RSUs and perform required analysis to confirm that vehicles behave as expected.
- **Patch management:** service that loads and validates software patches for your traffic devices and other equipment.
- **RSU monitoring:** report on RSU activity and location using our RSU monitor, or "bring your own" third party application and let OmniTrust provide the secure connectivity.
- **Tolling:** enable V2X tolling with easy connectivity to external tracking and payment, including proprietary secure links with EZ-pass.

Traffic Management Center (TMC) networks operated by state and regional Departments of Transportation (DOTs) have been classified as critical infrastructure by the Federal Department of Homeland Security (DHS). This means that these networks need to be designed to resist attacks by sophisticated adversaries including nation state level actors but at the same time they need to provide connectivity for a variety of modern applications that rely on Internet access.

That's why OmniTrust created TrafficAuth to securely connect traffic devices to Internet-facing systems. It acts as a secure network gateway so selected devices can access authorized Internet-facing applications and receive a response. It also acts as an industry-specific application-proxy firewall that monitors all messages to ensure only properly structured and authorized data is allowed. The TrafficAuth architecture follows NIST Cybersecurity Framework for critical infrastructure and ISA/IEC 62443.

With TrafficAuth, the TMC operator can not only control which devices are allowed access to cloud-facing applications, but also define specific protocols and use cases. And, for special high-security applications, TrafficAuth can host the actual content in the secure OmniTrust datacenter so that your device data never crosses the Internet.

The Benefits for TMCs

PROVEN SECURITY PLATFORM

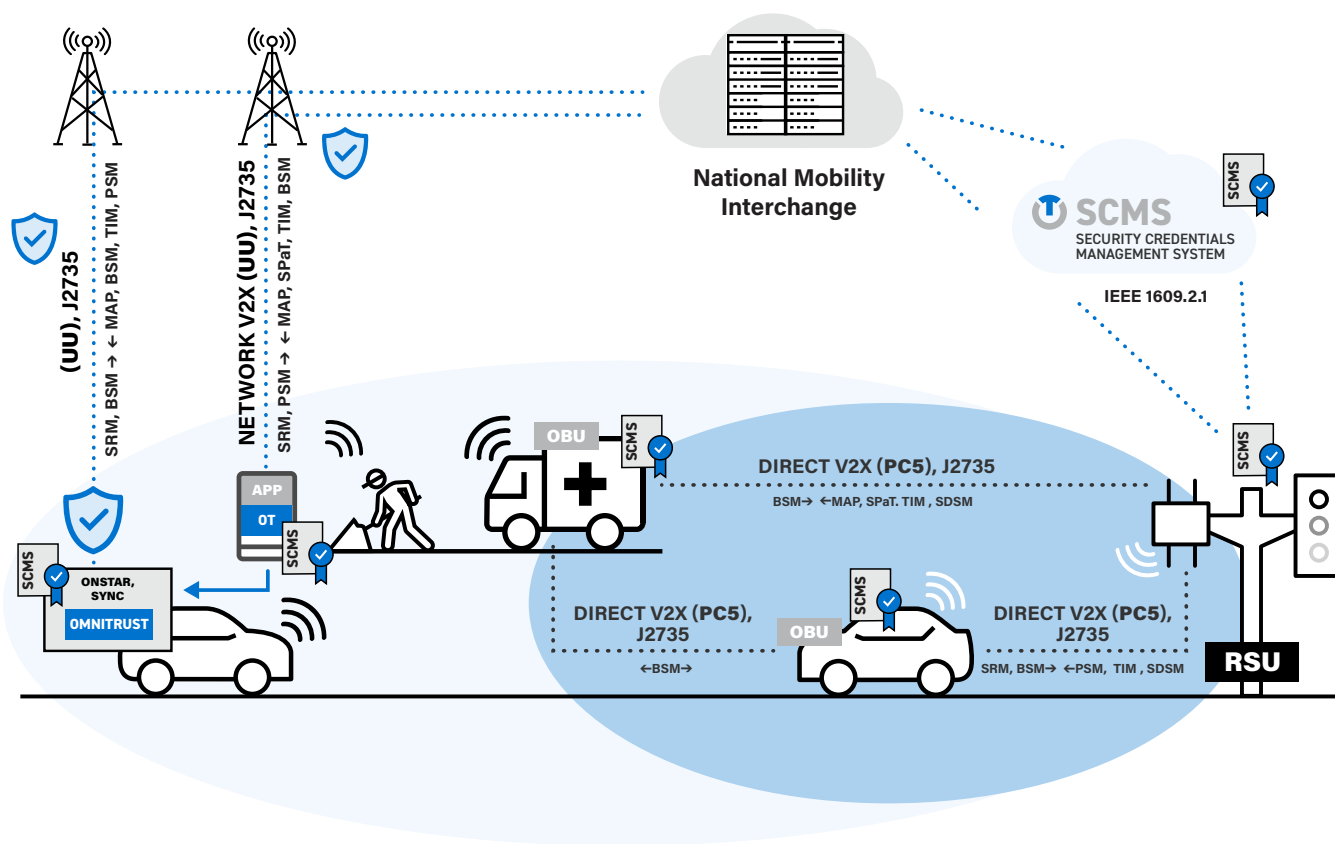
The world's first turnkey managed certificate service in full production today, the OmniTrust Secure Credential Management Service (SCMS) is the de facto standard in V2X and C2X secure communication credentials and is the foundation on which TrafficAuth is built.

QUICKLY ADD NEW APPLICATIONS

Additional third-party tools and applications can be quickly added to your instance of TrafficAuth and run in the OmniTrust datacenter. This provides faster, more secure access for your mission-critical traffic management communications.

LARGE-SCALE EXPERIENCE

OmniTrust is known for delivering a reliable, secure, production-grade certificate services for high-volume manufacturing and has extensive experience in supporting large-scale deployments of roadside infrastructure for state DOTs.



SUPPORTED STANDARDS

ISA/IEC 62443

Industrial communication networks - Network and system security

NIST SP 800-82

Guide to Operational Technology (OT) Security

DHS

Transportation Systems Sector Cybersecurity Framework Implementation Guidance

CTI 4501

Connected Intersections (CI) Implementation Guide

The TrafficAuth Family of Solutions

TrafficAuth is a collection of interoperable, standards-compliant and secure services for infrastructure owner operators (IOOs). It is bundled with mission-critical applications and an extensible API that supports native, 3rd-party and custom applications.

TrafficAuth-Authority (TAA)

Secure service for message signing and validation

TrafficAuth-Compliance (TAC)

Device registration for regulatory (FCC) compliance

TrafficAuth-Gateway (TAG)

Network gateway for secure messaging

TrafficAuth-Manage (TAM)

Secure device management and monitoring

TrafficAuth-Security (TAS)

Security credentials and PKI services (includes SCMS)

TrafficAuth-Update (TAU)

Managed software update analysis, approval, and distribution

TrafficAuth-Validate (TAV)

Connected intersection validation and monitoring services

TrafficAuth-Mobile

V2N2X application available on Android and iOS

Advantages of the Hosted TrafficAuth Platform

	OpenSource CV Manager	TrafficAuth Platform
HOSTING	Configure and maintain your own servers and network	Hosted platform, scalable performance
DATABASE	Build and maintain your own DB	Hosted DB shared across multiple apps
COMMON APPS	Contract with multiple vendors to build individual apps, debug and test	Marketplace of integrated apps optimized for the platform
CUSTOM APPS	Custom development with long-term maintenance commitment	Build custom apps to a common API, leverage hosted infrastructure
DEVICE CONNECTIVITY	Multitude of connectivity challenges	Secure model for external connectivity
UPDATES	Self-managed, need to keep multiple systems up-to-date	Centrally managed, all systems and apps supported and maintained
COST	Difficult to plan, potential for unplanned expenses	Predictable annual cost model

TrafficAuth-Mobile for Transportation Safety

TrafficAuth-Mobile is the first Vehicle-to-Network-to-Everything (V2N2X) application that enables workers to securely send and receive messages across cellular networks from any mobile device to the transportation network, which improves the efficiency of roadway systems and operations—and helps keep American drivers and transport workers safe, connected, and secure.

Part of the TrafficAuth family of products, this application creates a secure and authenticated communications channel between a worker or driver's cellphones and the cellular or transportation V2X networks. The TrafficAuth-SCMSclient API offers the same functionality but can be used by service providers and other transportation vendors to embed the same functionality in their own app for V2N2X communications.

TrafficAuth-Mobile and its related toolkit features:

- **A secure, integrated, and fully interoperable all-in-one V2N2X solution**
- **Complete end-to-end security credential management and authorization**
- **Full PCS V2X broadcast connectivity**
- **Ability to monitor and control highway operations, streamline transport services, and send work-zone safety or traffic messages directly to workers and drivers**
- **Compliance with all IEEE 1609.2.1 and SAE J2735 standards and Department of Transportation requirements for security credential management system (SCMS) funding**

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

