

SOLUTION SHEET

Enabling Bicycle Safety with TrafficAuth

The CAR 2 CAR Communication Consortium (C2C-CC) white paper on bicycle safety use cases identifies a focused set of cooperative intelligent transport systems (C-ITS) scenarios intended to reduce collisions between cyclists and motor vehicles. These include intersection movement assist, turning warnings, slow-moving bicycle warnings, backward collision warning, and bicycle accident warning.

The C2C-CC report emphasizes that bicycles are vulnerable road users, that many dangerous conflicts occur at intersections and turning points, and that C-ITS can help because it does not require direct line of sight between road users.

The TrafficAuth suite from OmniTrust supports these bicycle safety concepts by providing a standards-based trust, messaging, and distribution architecture for both Direct Vehicle-to-everything (V2X) and Network V2X deployments. The TrafficAuth SCMS platform establishes trusted device identity and message authenticity, while the TrafficAuth Mobile app and the National Mobility Interchange (NMI) enable mobile and cloud-hosted deployment models that can accelerate bicycle safety services even before widespread embedded bicycle OBU penetration is achieved.

C2C-CC BICYCLE SAFETY USE CASES

The C2C-CC report defines multiple bicycle safety use cases centered on vehicle-to-bicycle and infrastructure-assisted awareness. The major scenarios include:

C2C-CC use case	Safety objective
Intersection movement assist involving bikes (IMA-B)	Warn cyclists and/or drivers of perpendicular crossing conflicts at intersections.
Intersection movement assist with standstill vehicle (IMA-S)	Warn a driver who begins moving from a stopped position when a bicycle is approaching.
Right-turn warning for bike (RTW-B)	Warn about conflicts where a vehicle turns right across the path of a cyclist traveling straight.
Left-turn warning for bike (LTW-B)	Warn about left-turn conflicts involving a cyclist traveling through or parallel to the vehicle path.
Slow moving vehicle ahead (SMVA)	Alert a vehicle driver that a slow-moving bicycle or bicycle group is ahead in the same lane or path.
Bike accident warning (BAW)	Alert approaching vehicles that a cyclist has fallen or is otherwise creating a roadway hazard.

The C2C-CC document also highlights that some scenarios can be implemented vehicle-to-vehicle, while others can benefit from smart road side units (RSUs) using sensors such as cameras to detect unequipped road users and publish collective perception information.

TrafficAuth architecture for bicycle safety

TrafficAuth provides the trust and delivery framework needed to make these warnings actionable and interoperable.



TrafficAuth SCMS:

Trust for Direct and Network V2X

TrafficAuth SCMS issues and manages digital certificates used to sign safety messages. This is essential for bicycle safety because receiving vehicles, mobile apps, infrastructure systems, and network services must be able to determine whether a message is authentic and whether it came from an authorized source. The TrafficAuth family includes TrafficAuth Security for security credentials and public key infrastructure services, including security credential management system (SCMS).

In practice, this means a bicycle app, vehicle on-board unit, RSU, or traffic infrastructure component can sign its transmitted safety messages. Recipients can verify that the message has not been altered and that it originated from a trusted participant.



NMI:

Network V2X Distribution

The National Mobility Interchange is a cloud-hosted V2X data exchange that distributes authenticated transportation messages using a publish/subscribe model. NMI supports real-time data such as signal phase and timing (SPaT), map data message (MAP), bicycle safety modules (BSM), and sensor data sharing message (SDSM) messages, uses Society of Automotive Engineers (SAE) J2735 payloads, COER encoding, and an Institute of Electrical and Electronics Engineers (IEEE) 1609.2 security wrapper.

For bicycle safety, NMI provides the network distribution layer. Cyclists, vehicles, RSUs, fleet systems, and traffic management centers can publish or subscribe to relevant safety-zone topics. The NMI data sheet also describes hybrid network-to-radio connectivity, where RSUs can relay signed data between cloud services and the 5.9 GHz safety spectrum.



TrafficAuth Mobile:

Bicycle and vulnerable road user participation

The TrafficAuth Mobile app is well suited to bicycle safety because it can turn a smartphone into a Network V2X participant. The existing TrafficAuth work zone concept already describes a mobile app that generates digitally signed Personal Safety Messages for vulnerable road users, routes those messages through a TrafficAuth server, and supports alerts based on location and hazard context.

For bicycle safety, the same model can be applied to cyclists. A cyclist's phone can publish position, heading, speed, and status information. It can also receive warnings about nearby vehicles, turning conflicts, road hazards, work zones, or other cyclist-relevant safety events.

Mapping TrafficAuth to the C2C bicycle use cases



Intersection movement assist involving bikes

For IMA-B and IMA-S, TrafficAuthMobile can publish the cyclist's signed location, heading, and speed over Network V2X. Vehicles approaching the same intersection can receive the data through NMI or through a local RSU. If the vehicle has Direct V2X, the same trusted data can be bridged or rebroadcast locally. MAP and SPaT data from the infrastructure can improve conflict prediction by adding lane geometry and signal phase context.

This directly supports the C2C-CC objective of warning a cyclist or driver when crossing paths create a potential collision risk. The C2C-CC report notes that smart RSUs can reduce the required penetration rate because not every road user needs to carry a full V2X OBU if infrastructure can detect and publish their presence.



Slow moving vehicle ahead and backward collision warning

TrafficAuth supports SMVA by allowing a cyclist, bicycle group, or infrastructure detector to publish an authenticated bicycle presence message. Approaching vehicles can receive the alert through NMI, a local RSU, or Direct V2X. For the reverse direction, a cyclist using TrafficAuth Mobile can receive a backward collision warning when a fast-approaching vehicle is detected behind them.

This is particularly useful for rural roads, low-visibility corridors, curves, and routes where cyclists share the lane with higher-speed traffic.



Right-turn and left-turn warnings

For RTW-B and LTW-B, TrafficAuth can combine cyclist trajectory information from TrafficAuth Mobile with vehicle data from BSMs, fleet telematics, or infrastructure sensors. A backend service, edge RSU, or in-vehicle application can evaluate likely paths and issue warnings when a turning vehicle may cross the cyclist's path.

This is especially valuable in urban settings where cyclists may be in a bike lane, on a cycle track, or approaching from a direction that is not in the driver's primary visual focus. The C2C-CC accident analysis specifically identifies intersection and turning scenarios as high-priority bicycle-to-car crash types.



Bike accident warning

For BAW, TrafficAuth Mobile can use phone sensors, connected wearables, or bicycle-mounted devices to detect a potential fall. Once triggered, the system can publish a signed hazard alert with the cyclist's location and event type. NMI can distribute this message to approaching vehicles, traffic operations centers, emergency responders, and RSUs. A local RSU can also rebroadcast the warning over Direct V2X.

The C2C-CC use case describes this as a way to prevent secondary collisions after a cyclist falls, including on curves or at night where the cyclist may not be visible in time.

Deployment Benefits

TrafficAuth provides several practical advantages for deploying bicycle safety use cases:

- ▶ **Lower adoption barrier.** Cyclists can participate through a mobile app rather than waiting for widespread bicycle OBU installation.
- ▶ **Trusted safety messages.** SCMS-issued certificates and IEEE 1609.2 signing help vehicles and infrastructure trust the data they receive.
- ▶ **Network and Direct V2X support.** NMI supports Network V2X distribution, while RSUs can bridge messages into local radio channels for Direct V2X users.
- ▶ **Infrastructure-assisted coverage.** Smart intersections and sensor-equipped RSUs can detect cyclists who are not carrying V2X equipment and publish authenticated perception messages.
- ▶ **Scalable safety zones.** NMI's safety-zone model allows agencies to activate services at high-risk intersections, bike corridors, work zones, school zones, and freight conflict areas.

Implementation Considerations

The C2C-CC document references European C-ITS messages such as cooperative awareness message (CAM), CAMv2, collective perception message (CPM), and decentralized environmental notification message (DENM). TrafficAuth deployments in North America commonly use SAE J2735 messages with IEEE 1609.2 security. Therefore, an implementation may require a message-profile adaptation layer where strict C2C/ETSI interoperability is required. The safety logic remains the same: authenticated road-user state, infrastructure context, collision-risk assessment, and timely alert delivery.

A practical TrafficAuth bicycle safety pilot could begin with Network V2X using TrafficAuth Mobile and NMI, then expand to hybrid Network/Direct V2X using RSUs at selected intersections. Over time, bicycle OEMs, micromobility fleets, delivery fleets, and automotive OEMs can add embedded support while preserving the same trust framework.

Conclusion

The C2C-CC bicycle safety use cases provide a strong blueprint for reducing collisions between cyclists and motor vehicles. TrafficAuth can operationalize these use cases by combining trusted credentials, signed safety messages, mobile participation, cloud-based V2X distribution, and RSU-based Direct V2X bridging.

By supporting both smartphone-based Network V2X and standards-based Direct V2X, TrafficAuth gives agencies, OEMs, fleets, and infrastructure operators a practical path to deploy bicycle safety services now, while maintaining a migration path toward broader interoperable C-ITS adoption.

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.