CAPABILITY BRIEF

Connext Drive: The Foundation for SDV Security

FORTIFIED DDS-BASED SECURITY WITH PSK-BASED PROTECTION FOR AUTOMOTIVE SYSTEMS

With RTI Connext Drive®, OEMs can manage risk while meeting the highest levels of automotive cybersecurity standards. Connext Drive provides a proactive design-time strategy that hardens the entire system from the inside out. PSK protection ensures robust defense against external threats at the domain boundary, ensuring data availability, integrity and confidentiality for communication throughout the vehicle and over wide-area networks (WAN).

HIGHLIGHTS

- Defends vehicles from external threats through Pre-Shared Key (PSK) protection
- Delivers flexible, lightweight security for optimal performance and efficiency
- Connects securely across WAN and LAN environments, working jointly with Real-Time WAN Transport
- Integrates with security plugins for encryption, authentication and granular, fine-grained, topic-level security
- Secures multi-tenant systems via a layered cryptography stack

The shift toward connected software-defined vehicles has exponentially increased their attack surface, making them prime targets for cyber threats and exploitation. OEMs face an urgent challenge to protect the integrity and safety of modern interconnected systems. System architects must move beyond traditional security measures and embed a dynamic, multi-layered defense system into every vehicle's design.

Based on the Data Distribution Service (DDS™) standard, RTI Connext Drive provides comprehensive built-in security throughout all stages of vehicle development, providing protection against cyberattacks. This approach provides a proactive strategy that hardens the entire system from the inside out and provides robust perimeter defense via PSK protection to ensure the availability, integrity, and confidentiality of data against external threats.

Comprehensive Security for Software-defined Vehicles

DDS Security Threat Model

RTI's comprehensive DDS-Security™ threat model provides a structured approach to securing automotive systems by defining clear Domain Trust Boundaries. This is crucial in complex, multi-vendor environments where different vehicle functions and ECUs need to communicate securely without external threat exposure. Each domain can be thought of as a secure, isolated network, as depicted in Figure 1.

The Connext Drive security framework includes topic-level protection to ensure granular control over data access. Each DomainParticipant is assigned its own unique Identity Certificate and private key. This one-to-one mapping establishes and verifies trust by defining the specific security risks associated with each domain. By preventing the use of shared credentials, the system can precisely track and authenticate every participant's actions. This approach secures communications while providing insider protection, as it eliminates the ambiguity of shared keys and allows for the easy identification and isolation of any compromised or unauthorized participant.

Integration with Security Plugins

Connext Drive works with all levels of security plugins to provide the necessary security throughout the vehicle. In use cases that deploy lightweight plugins, Connext Drive uses PSKs exclusively for symmetric encryption and message authentication.

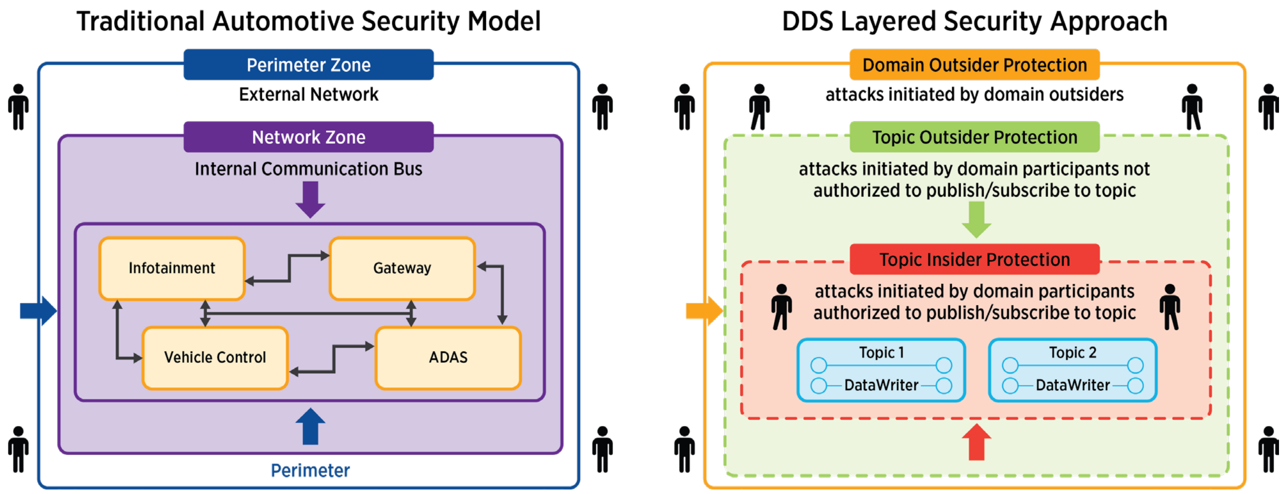

Figure 1. Side-by-side comparison of the two security threat model approaches, highlighting the key differences in protection boundaries and security principles.

Connext Drive also includes security options with support for Hardware Security Modules (HSMs) through the RTI Micro Lightweight Security PSL SDK. By leveraging HSM integration, developers can now enable secure key storage, cryptographic acceleration and tamper resistance. For full-featured built-in plugins, it protects by using PSKs for initial authentication and discovery bootstrapping, and leverages advanced security features to enable granular top-level security through the vehicle.

PSK Protection

With PSK protection at the domain boundary, developers can create a secure perimeter that defends against external threats from the start. Inside the vehicle, Connext Drive ensures data availability, integrity and confidentiality across every communication, whether it's between internal systems or over a WAN.

The PSK Secret Passphrase (a.k.a. PSK seed) produces information to derive symmetric session keys unique to each participant and is configured uniquely for each domain. If any domain is compromised, the impact of the security breach is limited to that specific domain. With Connext Drive, the PSK seed does not need to be hardcoded and can be provided via QoS updates or files, enabling dynamic updates without restarting Connext applications.

Layered Cryptography Stack

Connext Drive uses the Layered Cryptography Stack to provide a multi-faceted security approach. It begins with a PSK for the first layer, establishing a baseline of trust for a new connection. Once this initial trust is established, the system transitions to a higher level of security using Public Key Infrastructure (PKI) for peer-to-peer authentication.

The PKI allows vehicles and infrastructure components to verify each other's identities without sharing a common secret key, providing a more scalable and secure method than PSKs for ongoing communication. Developers can update a DomainParticipant's identity certificate and private key on the fly, without system downtime.

Application eXchange Keys (AXK) protect the actual encrypted traffic. These symmetric keys are dynamically generated for each session, ensuring that even if one session's key is compromised, the security of other sessions is not impacted.

Connext Drive provides a comprehensive, layered approach to security that helps developers to focus on innovation instead of vulnerabilities:

- Reduced risk of cyberattacks
- Continuous operation without downtime
- Flexible, multi-layered security architecture
- Seamless integration with HSMs

To learn more about safeguarding next-generation vehicles from evolving cybersecurity threats, please contact your RTI representative or visit www.rti.com/drive.

ABOUT RTI

RTI delivers the real-time data communication that powers the next generation of Software Defined Vehicles (SDVs). RTI is the safety-certified communication framework leader for SDVs, trusted by OEMs to bridge from legacy to modern architectures, thereby accelerating development from simulation to production. RTI Connext Drive® powers over 1 million vehicles on the road today and is used by more than 25 automotive companies to accelerate their SDV programs and enable zonal, ADAS, and telematics architectures.

Experience the industry's leading solution and try Connext Drive for free at rti.com/drive.

Your systems. Working as one.
CORPORATE HEADQUARTERS: 232 E. Java Drive, Sunnyvale, CA 94089 • +1 (408) 990-7400 • info@rti.com
rti.com rti.com/blog rti.com/podcast company/rti rti_software rtisoftware