DATASHEET

RTI Security Extensions

PROTECT SYSTEM INTEGRITY WITH REAL-TIME OPTIMIZED AUTHENTICATION, ENCRYPTION AND ACCESS

HIGHLIGHTS

Fine-grained authentication, authorization, confidentiality and integrity to defend against unauthorized access, tampering and replay

Lightweight Security Plugins are also available to enhance connectivity across distributed systems, providing efficient security in resource-constrained environments

Pluggable design to protect applications with minimal-to-no changes

Operates without centralized servers for high performance, scalability and availability

Provides essential help for compliance with modern cybersecurity regulations and Zero Trust policies

RTI Security Extensions provide flexible security options, offering industry-leading protection that is designed to efficiently secure applications and help ensure compliance. With the April 2024 release of RTI Connext® Professional 7.3 LTS, the functionalities formerly comprising Connext Secure are now available as Security Extensions, an optional component to Connext Professional.

SECURING AUTONOMOUS SYSTEMS

Securing autonomous systems — such as those in medical, energy, transportation and defense industries — requires careful architecting of the entire distributed system. These systems often include diverse technology components from different project teams or third-party suppliers. As a result, these systems tend to offer different levels of trust and performance. One option is for OEMs to write and maintain the integration code to connect these complex devices.

However, complex systems are constrained to the most stringent low-latency, highly reliable and scalable data communication requirements. Therefore, finding the right balance between securing the systems and preserving the most reliable performance across these heterogeneous environments is vital.

RTI Security Extensions take a data-centric approach to securing data including:

- Interoperability between DDS-Security™ applications based on the system's data model.
- Optimized security and performance by signing and encrypting only sensitive data.
- Automatic discovery of each participant for trusted peer-to-peer communications.

Based on the Data Distribution Service (DDS™) standard, the Security Extensions are built upon and supported by RTI's unparalleled expertise in architecting, developing and deploying intelligent distributed systems. The options include:

- **Built-In Security Plugins** — enable system architects to protect and defend systems through flexible, fine-grained security for optimal performance and efficiency, from device to cloud.
- **Built-In Lightweight Security Plugins** — provide integrity and confidentiality through Pre-Shared Keys (PSK) for resource constrained devices.
- **TLS Support** — provides integrity and confidentiality of whole communication at the transport level. If optimal performance is not your main concern, this well-known protocol provides a simpler protection with an equivalent level of security. It does not support multicast.
- **Optional** — Security Extensions can be used to connect securely across WAN and LAN environments, working jointly with RTI Real-Time WAN Transport (a separate product).

CAPABILITIES DELIVERED WITH BUILT-IN SECURITY PLUGINS

Fine-grained security

Choose between non-secured, signed and encrypted topics to meet your security requirements and use cases, while optimizing performance. Not only can select topics be protected, but they can be protected at varying levels of granularity. Fine-grained security allows architects to:

- Sign/encrypt the entire RTPS message
- Sign/encrypt select RTPS sub messages
- Sign/encrypt the serialized user data

Pluggable and customizable

The Connext platform enables fast, flexible changes. Minimal-to-no changes are required for existing DDS applications when using built-in plugins. The plugins only need to be configured via XML to enable security. An optional software development kit is available, enabling custom integration with crypto libraries, crypto hardware (such as accelerators or TPMs), and custom logging.

Authentication

- X.509 Public Key Infrastructure (PKI) with Certificate Authorities (CA), and support for certificate chaining and certificate revocation lists
- RSA or Elliptic Curve DSA (ECDSA) for authentication
- Diffie Hellman (DH) or ECDH in ephemeral mode for perfect forward secrecy for shared secret agreements

Access Control

- Configured by domain using a shared Governance file signed by shared CA
- Control over ability to join DDS Domains and Partitions and Reading or Writing Topics
- Control on individual objects and Quality of Service (QoS) via plugins

Cryptography

- AES-GCM in GMAC mode with 128- and 256-bit keys for data integrity
- AES-GCM with 128- and 256-bit keys for data confidentiality and integrity
- AES-GCM in GMAC mode with 256-bit key for data source authentication

Logging

- Designed to support auditing of all DDS security-relevant events, increasing system visibility
- Log security events to a file or propagate securely over DDS
- It can be integrated with the RTI Observability Framework and with the main Observability solutions on the market via OpenTelemetry

Transport agnostic

Since security is implemented above the transport layer, any Connext transport can be used securely, including UDP, TCP, shared memory and Real-Time WAN Transport. Support for UDP multicast (both reliable and best effort) enables efficient data distribution to multiple authenticated subscribers.

CAPABILITIES DELIVERED WITH BUILT-IN LIGHTWEIGHT SECURITY PLUGINS

Resource-constrained devices

Cryptography based on pre-shared keys (PSK) requires fewer resources in terms of CPU and memory and can be used on a wider range of devices.

Fast startup

By not having to go through the authentication or key negotiation phases, the startup of the devices is much faster.

Simple management

This set of plugins does not require digital certificates nor, therefore, the management of a PKI. For some organizations this may be an advantage, especially if they already have a solution in place to distribute shared keys between their applications.

Benefits preserved

Having been designed as part of the DDS standard, this set of plugins has benefits in common with the Built-in Security Plugins, provided you do not require fine-grained security:

- Pluggable and customizable
- Logging
- Transport agnostic

SUPPORTED CRYPTO MODULES

Non-certified modules:

- OpenSSL 3

FIPS 140-2 certified modules:

- OpenSSL 3 FIPS Provider
- WolfSSL 5.5
- Trusted Platform Modules (TPMs)

ABOUT RTI

Real-Time Innovations (RTI) is the infrastructure software company for smart-world systems. Across industries, RTI Connext® is the leading software framework for intelligent distributed systems. RTI runs a smarter world.

RTI is the market leader in products compliant with the Data Distribution Service (DDS™) standard. RTI is privately held and headquartered in Silicon Valley with regional offices in Colorado, Spain, and Singapore.

Your systems. Working as one.

CORPORATE HEADQUARTERS

232 E. Java Drive, Sunnyvale, CA 94089
Telephone: +1 (408) 990-7400
info@rti.com

rti.com
rti_software
rtisoftware
company/rti
rti.com/blog
connextpodcast