Adax SCTP/T & DTLS Protocol Modules

Legacy to 5G and IoT

Run-time Security and Reliable Delivery of Valuable and Real-Time Data in 3G, 4G, 5G, IoT and M2M networks

Overview

There is renewed urgency to address signaling-based threats to communications networks: 4G is delivering on its promise of mobile broadband data services, IoT networks are starting to grow, and 5G is not far behind. As the number of subscribers and connected devices grows so do the demands for secure, reliable, robust and high-performing networks to support them.

Steeped in the tradition of telecom reliability and robustness, with thousands of SIGTRAN installations, the Adax SCTP/T and DTLS modules meet the challenges of network growth and performance, whilst maintaining service and data delivery and thwarting malicious intent.

Adax SCTP for Telecom (SCTP/T)

SCTP/T provides the transport layer necessary to deliver the protection and high level of customer experience today's networks demand. Adax SCTP/T is specifically designed to meet the signaling demands of these networks, ensuring the consistent and timely delivery of the valuable data to the applications, and securing the millions of simultaneous associations required.

Without SCPT/T network connections are vulnerable to fraudulent packet injection and hijacking and the delivery of this valuable, time dependent, data is at risk. Enhanced network security from "man in the middle attacks" is provided by the optional Adax SCTP/T AUTH feature defined in RFC4895.

Adax SCTP/T has provisioning options that can achieve link monitoring and fail-over robustness and redundancy for IP signaling that rival traditional SS7 networks. These Adax specific features make a significant difference for real-time applications with a low tolerance of latency, where data arrival must be fast, timely and reliable.

Adax DTLS over SCTP/T

DTLS is an optional module that delivers transport security by providing communications privacy for client/server applications to prevent eavesdropping and detect tampering or message forgery. Applications using Adax DTLS can use all the transport features provided by Adax SCTP/T and its extensions. This is especially important for Diameter where RFC 6733 states all Diameter base protocol implementations MUST support the use of DTLS/SCTP.

Quality and Reliability of Service

Built to meet the exacting demands of 3G, 4G, 5G, IoT and M2M, Adax SCTP/T provides the signaling reliability to enable service providers to ensure the delivery of valuable and timely data for real-time applications with a low tolerance of latency, by implementing signaling protocols and services that:

- Perform vigilant in-service quality monitoring of the signaling links
- Detect degradation of link quality at very short, programmable intervals and take action to move to alternative links before the primary link goes out of service
- Provide redundancy via an enhanced version of multi-homing

Adax SCTP/T constantly monitors the primary and alternative links to ensure faster lost packet recovery in both single or multi-homing situations and pro-actively starts to repair and correct lost packet after one 'rto_min' period.

Secure Authentication with Performance & Visibility

Security in the network is more important today than ever before. Networks are subject to attacks with greater frequency and potential damage is a constant threat. The number of instances will only increase as more IoT devices are connected to the network. With the RFC 4895 Authentication and RFC 6083 detecting tampering or message forgery Adax SCTP/T and DTLS address these concerns without compromising performance or network monitoring visibility like IPsec/VPNs can do.

SCTP and DTLS for Diameter

The flat architecture of the 4G and 5G network requires a very large number of signaling connections and signaling concentration for efficient routing. Diameter signaling, especially on the S6a interface, can be the bottleneck in network performance. Linux-supplied SCTP is a seemingly convenient and economical solution but is simply not up to this task. Likewise the large number of IoT and M2M connections over the S1 interface cannot be handled effectively.

Adax SCTP/T and DTLS resolves all of these issues and the advanced multi-core implementation allows the Linux host to provide thousands of associations and connections, instantly ready to carry the traffic required by the host application.

Performance is in the Details…

Adax SCTP/T and DTLS achieves levels of signaling performance and delivery of valuable and timely real-time data unsurpassed in the industry, providing:

- Up to 10,000 simultaneous associations for maximum connectivity
- Secure authentication with performance & visibility
- Protocol implementation in the OS kernel for accurate timer control and quick recovery
- In-service monitoring and detection of link degradation, anticipating the need to offload to secondary links
- Enhanced multi-homing provisioning options improve fail-over robustness and redundancy

Supporting up to 10,000 simultaneous SCTP associations on the application's Linux host, while utilizing less than 20% of the CPU, Adax SCTP/T leaves ample resources for any type of application. Today's networks need reliable, high-performance, high-capacity, signaling capabilities similar to traditional SS7 networks. Adax SCTP/T and DTLS are the most robust, scalable, authenticated implementations available and will enable you to secure, optimize and grow your network.

Adax SCPT/T and DTLS meet the signaling demands of today's networks

Faster lost packet recovery in single or multi-homing

- Adax SCTP/T has a 20 mS recovery compared to 200 mS for lksctp
- Adax SCTP pro-actively fixes a lost packet after one 'rto_min' period

Better monitoring of Multi-Homed links for fast fault recovery

- Adax Auto newpri automatically sets a new primary destination address when the current primary address is failing or has failed for excessive errors
- lksctp it doesn't retransmit on the original main link, just on an alternate
- Adax SCTP/T sets parameter per Association for the optimization of individual targets
- lksctp can only set these parameters globally

Better dynamic tracking of link quality with Adax SLQ

- Adax SCTP/T tracks and measures the correct return of HeartBeat Requests
- Adax SCTP/T SLQ (SCTP Link Quality) dynamically monitors link quality

Adax auto newpri and SLQ automates multi-homing

- Automated decisions make the best selection from all the available alternate links
- Unique Adax multi-homing automation feature dramatically improves link changeover
- Option provided for manual decisions to be taken using the same decision data

Timer efficiency for large, highly parallel implementations

- Search and timer management features and load balancing capabilities
- Delivers neutrality for large and small volume applications simultaneously on same host

DTLS tuned with Adax SCTP for fast, real-time, performance

- Adax DTLS is designed to use all the attributes of Adax SCTP to their maximum advantage
- Improved error correction and faster link failure recovery than standard DTLS method
- Preservation of message boundaries, ordered and unordered delivery of SCTP user messages, and support for large numbers of unidirectional and bidirectional streams
- Partial reliability extension as defined in RFC3758 and dynamic address reconfiguration extension as defined in RFC5061
- DTLS over SCTP/T gives 2-to-5 times better real-time response than UDP
- Adax libraries provide a simple framework for applications to interface directly to DTLS and take full advantage of the underlying SCTP features

Why Adax?

No other implementation includes all of these enhancements and options, enabling Adax SCTP/T and DTLS to deliver the highest levels of performance and service that:

- Detects and fixes real-time failures and achieve service restoration through alternate destination addresses
- Provides both redundancy and fault tolerance for signaling applications avoiding single points of network failure
- Transparently switches to the secondary path, without packet loss or upper layer intervention
- Improves destination and peer path failure detection

Sample Applications that require the advantages of Adax SCTP and DTLS

Applications with high-throughput requirements include:

- Augmented and Virtual Reality
- Vehicle control, telematics and updates
- Remote personal healthcare and some wearables
- Video surveillance
- Location tracking

Applications with a low tolerance of latency include:

- Location-based marketing and advertising
- Industrial robotics and environmental control
- Smart home control
- Augmented and Virtual Reality
- Vehicle control, telematics and updates
- Remote personal healthcare and some wearables

Standards

- IETF RFC 6733 SCTP as Transport for Diameter Base Protocol
- IETF RFC 6347 Datagram Transport Layer Security v1.2
- IETF RFC 6083 Datagram Transport Layer Security (DTLS) for SCTP
- IETF RFC 5062 Security Attacks Against SCTP
- IETF RFC 5061 Dynamic Address Reconfiguration
- IETF RFC 4960 Stream Control Transport Protocol
- IEFT RFC 4895 Authenticated Chunks for SCTP
- IETF RFC 4460 Errata and Issues
- IETF RFC 4086 Random Number Generation
- IETF RFC 3873 SNMP MIB
- IETF RFC 3758 Partial Reliability Extension
- IETF RFC 2104 HMAC: Keyed-Hashing for Message Authentication
- IETF RFC 1321 The MD5 Message-Digest Algorithm

SCTP/T 0118/08

adax inc
2900 Lakeshore Ave,
Oakland, CA 94610, USA
Tel: (510) 548 7047
Fax: (510) 548 5526
Email: sales@adax.com

adax europe ltd
40 Caversham Road
Reading, Berkshire,
RG1 7EB, UK
Tel: +44 (0) 118 952 2800
Fax: +44 (0) 118 957 1530
Email: sales@adax.co.uk

adax china
Unit B-4 27 floor,
No. 888 Wan Hang Du Road
Shanghai 200042, China
Tel / Fax: +86 21 6386 8802
Email: sales@adax.com