

2.2.2.1.1 Secure Messaging

[return to Network View](#)

The lowest functional layer of a node component is secure messaging. It is essential that a [distributed system](#) be able to have trusted, reliable, tamper resistant, and anti-snoop data flow between [nodes](#) in the network. Secure messaging must also include a standardized, consistent, and predictable way to marshal data between nodes. For example, the [Endianness](#) of each node may be different. This requires a solid transport mechanism, an excellent security infrastructure, and a standardized way to distribute data quickly and efficiently.

Standards

Technical Standards

- [RFC7235 - Hypertext Transfer Protocol \(HTTP/1.1\): Authentication](#)
- [RFC2818 - HTTP Over TLS \(HTTPS\)](#)
- [RFC6749 - The OAuth 2.0 Authorization Framework](#)
- [RFC6750 - The OAuth 2.0 Authorization Framework: Bearer Token Usage](#)
- [RFC2315 - Cryptographic Message Syntax](#)
- [RFC3447 - PKCS #1: RSA Cryptography Specifications](#)
- [RFC7061 - eXtensible Access Control Markup Language \(XACML\) XML Media Type](#)
- [RFC2818 - HTTP Over TLS \(HTTPS\)](#)
- [RFC6101 - The Secure Sockets Layer \(SSL\) Protocol Version 3.0](#)
- [RFC2104 - Keyed-Hashing for Message Authentication \(HMAC\)](#)
- [OMG: Data Distribution Service \(DDS\)](#)
- [OMG: DDS Security \(DDS-SECURITY\)](#)

de facto Standards

- [ZeroMQ Distributed Messaging](#)
- [Google: gRPC](#)
- [Google: Protocol Buffers](#)
- [Linux Foundation: Open Middleware Agnostic Messaging API \(OpenMAMA\)](#)
- [Linux Foundation: Open Messaging](#)
- [BIP 0070 - Payment Protocol](#)

Last
update:
2021/11/09 15:51 dido:public:ra:1.2_views:2_tech_views:2-nodenet:2_net:1_msg https://www.omgwiki.org/dido/doku.php?id=dido:public:ra:1.2_views:2_tech_views:2-nodenet:2_net:1_msg

From:
<https://www.omgwiki.org/dido/> - **DIDO Wiki**

Permanent link:
https://www.omgwiki.org/dido/doku.php?id=dido:public:ra:1.2_views:2_tech_views:2-nodenet:2_net:1_msg

Last update: **2021/11/09 15:51**

