

Security Model

[Return to Glossary](#)

The **Security Model** for DDS defines the security principals (users of the system), the objects that are being secured, and the operations on the objects that are to be restricted. DDS applications share information on DDS Global Data Spaces (called DDS Domains) where the information is organized into Topics and accessed by means of read and write operations on data-instances of those Topics.

Ultimately what is being secured is a specific DDS Global Data Space (domain) and, within the domain, the ability to access (read or write) information (specific Topic or even data-object instances within the Topic) in the DDS Global Data Space.

Securing DDS means providing:

- Confidentiality of the data samples
- Integrity of the data samples and the messages that contain them
- Authentication of DDS writers and readers• Authorization of DDS writers and readers
- Message-origin authentication
- Data-origin authentication
- (Optional) Non-repudiation of data

Source: https://www.omg.org/spec/DDS-SECURITY/1.1/PDF#Security_mode Section 7.1

From:

<https://www.omgwiki.org/dds/> - **DDS Foundation Wiki**

Permanent link:

https://www.omgwiki.org/dds/doku.php?id=dds:public:guidebook:06_append:glossary:s:securitymodel&rev=1597954498

Last update: **2020/08/20 16:14**

