Your systems.
Working as one.

Leveraging DDS Security in ROS2

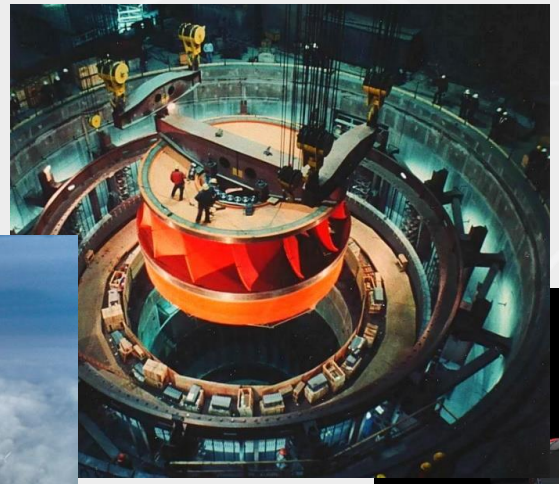
Gerardo Pardo, Ph.D., RTI, gerardo __at__ rti.com

Ruffin White, UC San Diego, rwhitema __at__ eng.ucsd.edu

About RTI

Your systems. Working as one.

Real-Time Innovations (RTI) is the Industrial Internet of Things (IIoT) connectivity company



RTI Offers Free Connext DDS Pro Licenses with Tools to ROS2 University & Research users

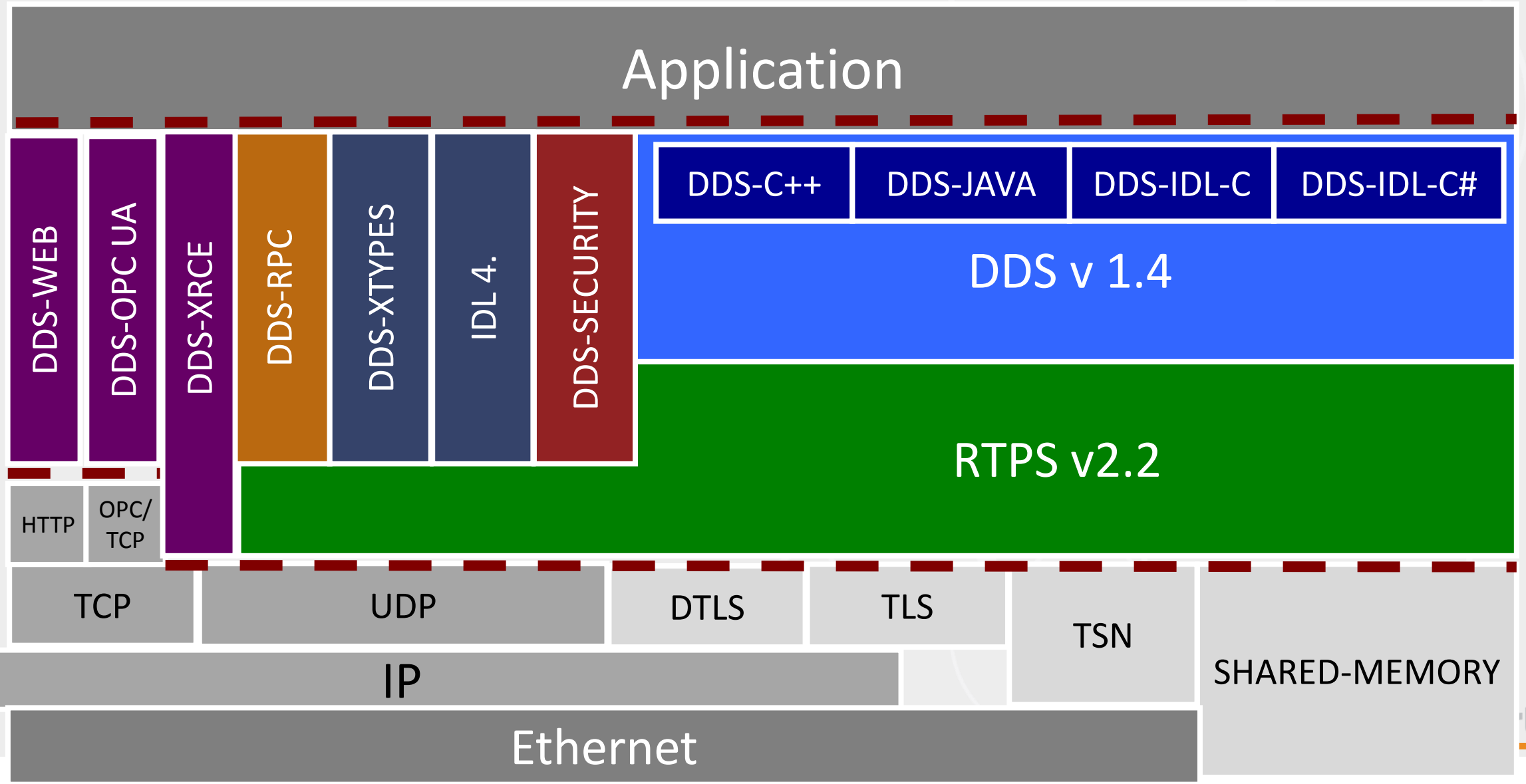
To enable and realize the potential of smart machines to serve mankind

Outline

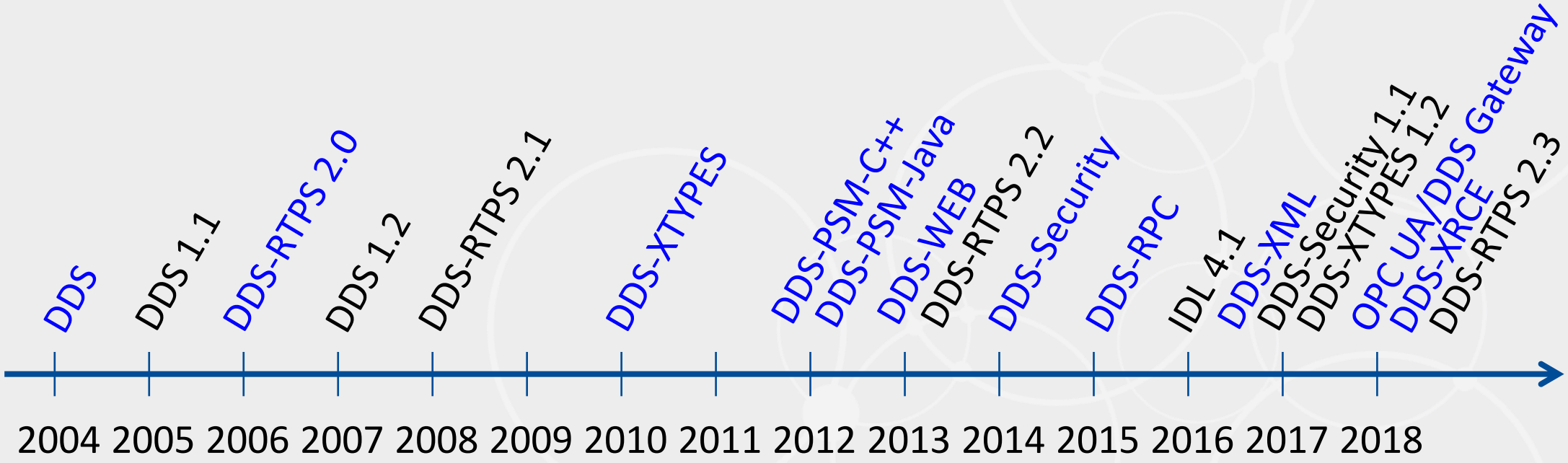
- Intro to DDS Security
- Performance Impact
- How ROS2 maps DDS
- Using DDS Security with ROS

Data Distribution Service (DDS)

DDS Specification family



Timeline



Shared Global Dataspace

Shared Global Dataspace (Domain)

Source (Key)	Speed	Power	Position
CAR1	37.4	122.0	(37.41, -122.01)
CAR2	10.7	74.0	(36.95, -122.05)
CAR3	50.2	150.07	(37.42, -122.17)

QoS
Topic D

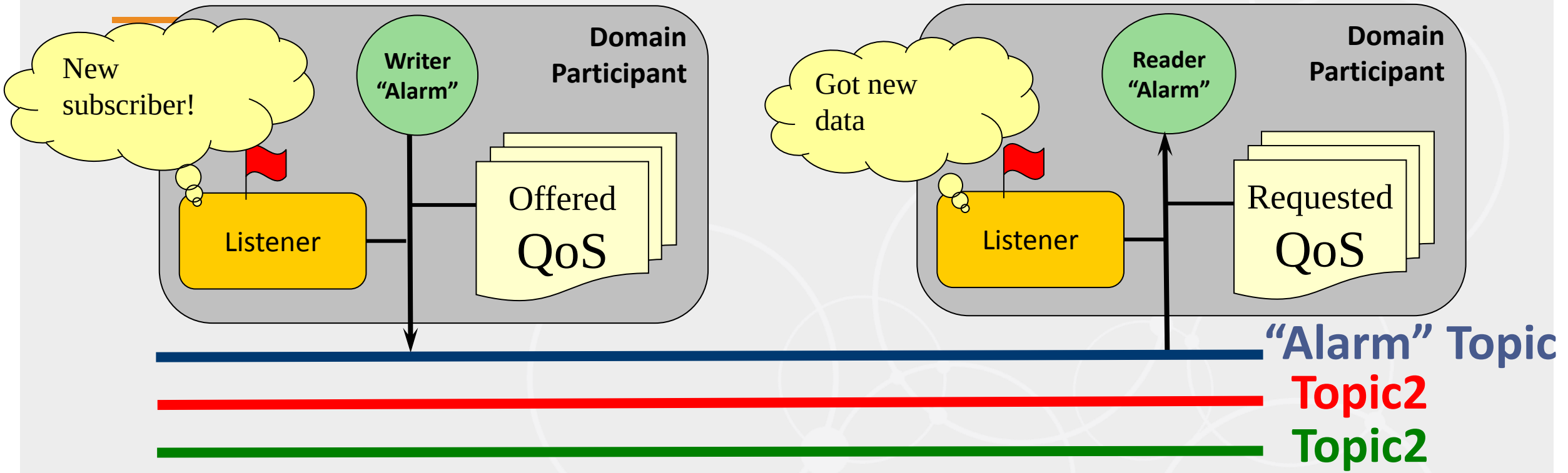
DATABUS

QoS
Topic D

Persistence Service

Recording Service

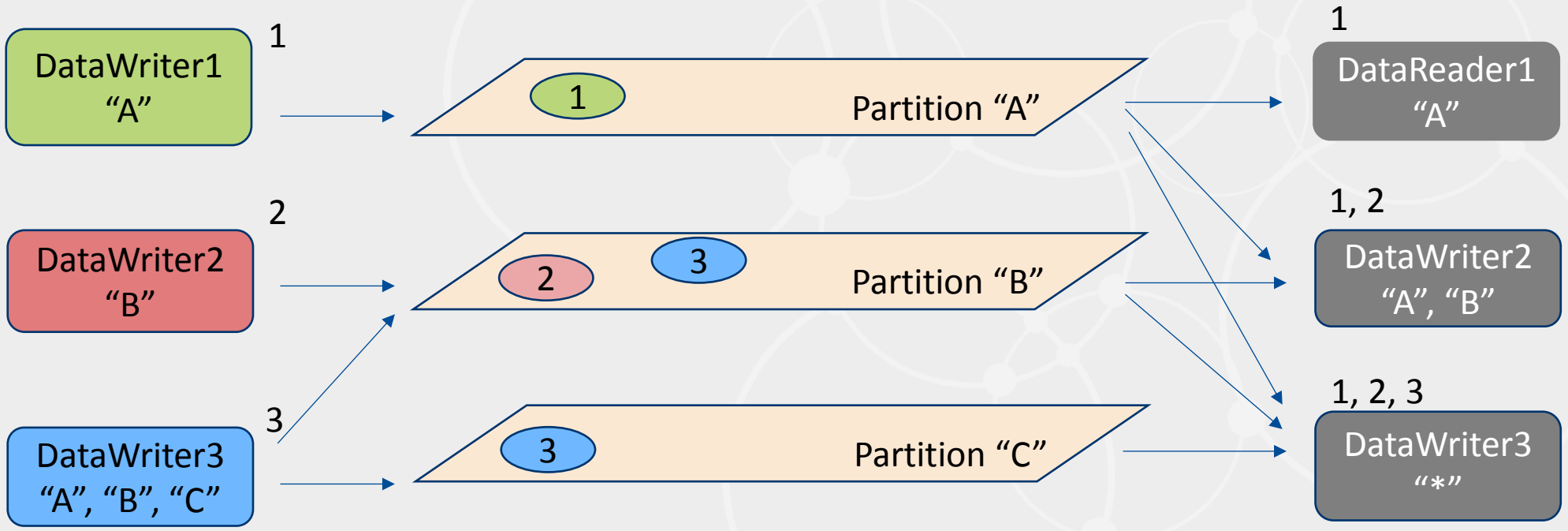
Data-Centric Communications Model



- **DomainParticipant** connects to the global data space (domain)
- **Topics** define the data-objects (collections of subjects)
- **DataWriters** publish data on Topics. **Publishers** are used to group DataWriters.
- **DataReaders** subscribe to data on Topics. **Subscribers** are used to group DataReaders
- **QoS Policies** are used configure the system
- **Listeners** are used to notify the application of events

DDS Partitions

- Provide a “scope” or “namespace” to data published/subscribed
- DataWriters & DataReaders belong to one or More Partitions
- DataWriters/Readers on the same Topic match only if they have a common Partition



Quality of Service (QoS) Policies

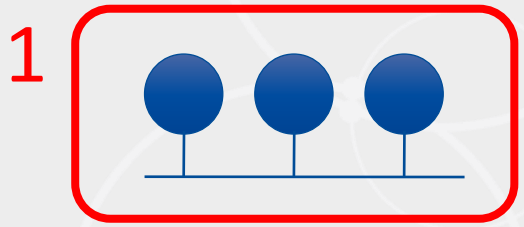
	QoS Policy
Cache	**DURABILITY**
	HISTORY
	LIFESPAN
Resources	WRITER DATA LIFECYCLE
	READER DATA LIFECYCLE
	ENTITY FACTORY
	RESOURCE LIMITS
Delivery	**RELIABILITY**
	TIME BASED FILTER
	DEADLINE
	CONTENT FILTERS

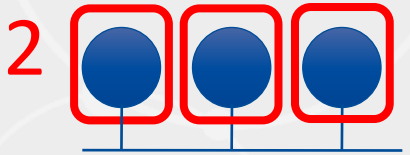
QoS Policy	
USER DATA	User QoS
TOPIC DATA	
GROUP DATA	
PARTITION	
PRESENTATION	Presentation
DESTINATION ORDER	
OWNERSHIP	Availability
OWNERSHIP STRENGTH	
LIVELINESS	
LATENCY BUDGET	Transport
TRANSPORT PRIORITY	

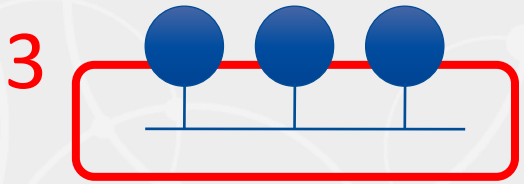
DDS Security

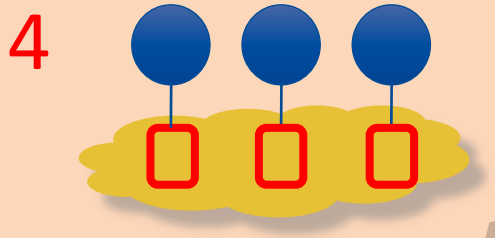
Security Must Protect Dataflow, Too

1. System Boundary
2. Host
3. Network Transport
   - Media access (layer 2)
   - Network (layer 3) security
   - Session/Endpoint (layer 4/5) security
4. Data & Information flows









Secure the Data, Not the Connection

Shared Global Dataspace

Topic

Line	Flight	Dest	Arv
UA	5		7:32
AA	4		9:15
AA		X	9:15
AA		LAX	9:15

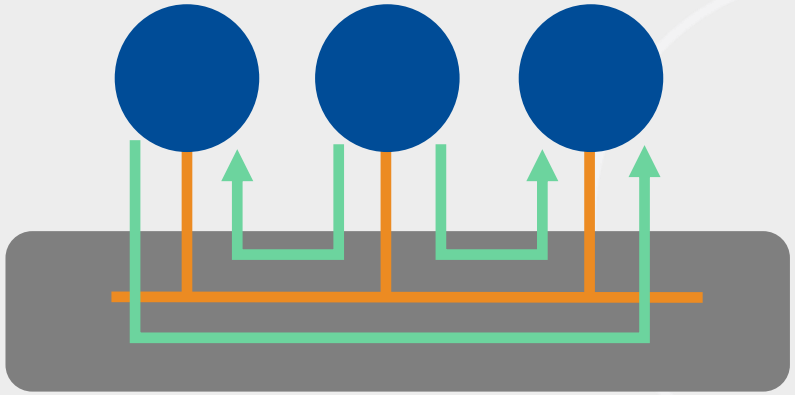
Squawk	Line	Flight
1234	A	567
7654	A	432
765		432

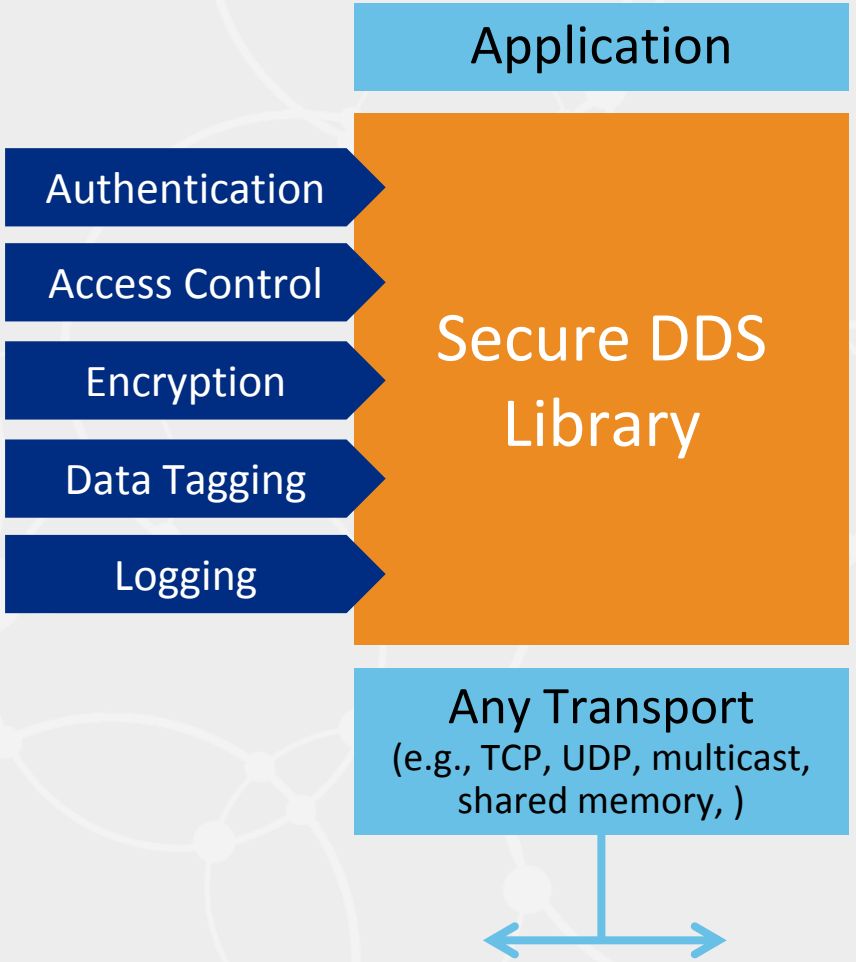
Squawk	Lo g	Lat	Alt
1234		.0	500.0
7654		.0	250.0
7654		74.0	250.0
7654		-74.0	250.0

DDS Domain

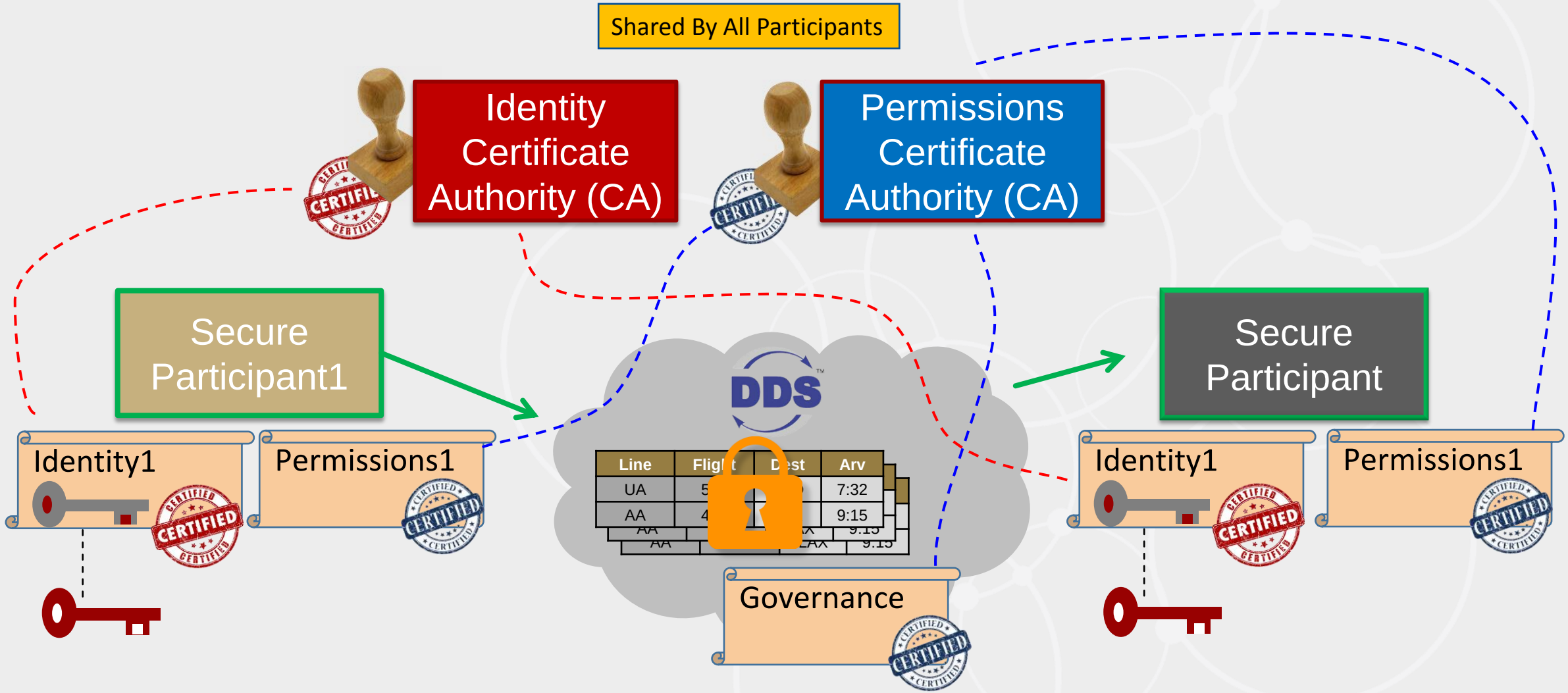
Fine-Grained, DDS Security

Data Flow Security, by Topic

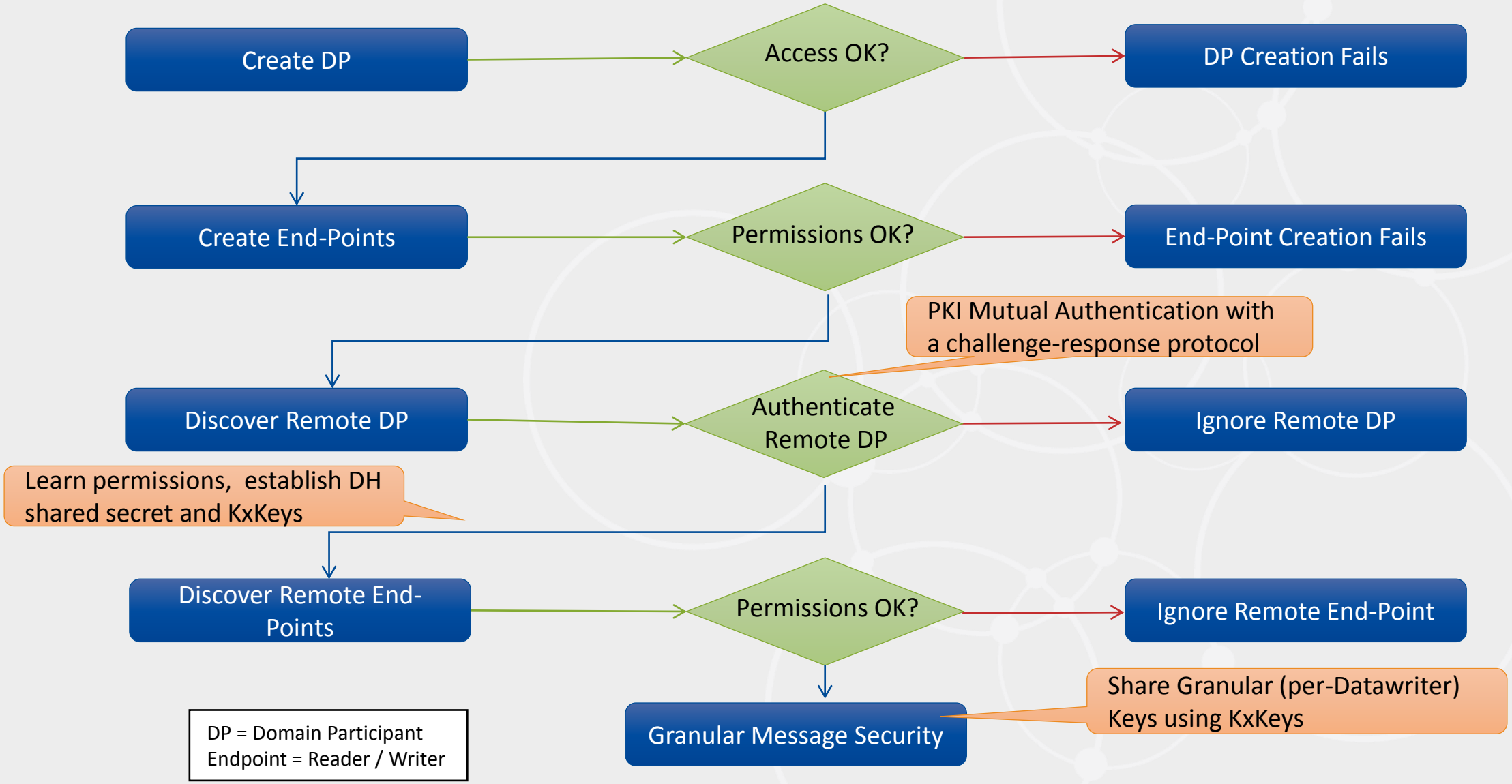




DDS Security Configuration



Authentication and Authorization Steps



Governance

- What Topics are Secure?
- Which Topics use Secure Discovery?
- What Kind of protection is used?
  - Data Encrypt or MAC
  - Protocol Encrypt or MAC

```
<?xml version="1.0" encoding="UTF-8"?>
<dds xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:noNamespaceSchemaLocation="../schema/dds_security_governance.xsd">
    <domain_access_rules>
        <domain_rule>
            <domains>
                <id_range>
                    <min>0</min>
                </id_range>
            </domains>
            <allow_unauthenticated_participants>false</allow_unauthenticated_participants>
            <enable_join_access_control>true</enable_join_access_control>
            <discovery_protection_kind>ENCRYPT</discovery_protection_kind>
            <liveliness_protection_kind>ENCRYPT</liveliness_protection_kind>
            <rtps_protection_kind>SIGN</rtps_protection_kind>
            <topic_access_rules>
                <topic_rule>
                    <topic_expression>*</topic_expression>
                    <enable_discovery_protection>true</enable_discovery_protection>
                    <enable_read_access_control>true</enable_read_access_control>
                    <enable_write_access_control>true</enable_write_access_control>
                    <metadata_protection_kind>ENCRYPT</metadata_protection_kind>
                    <data_protection_kind>ENCRYPT</data_protection_kind>
                </topic_rule>
            </topic_access_rules>
        </domain_rule>
    </domain_access_rules>
</dds>
```

Permissions

For each Participant

- Allowed Domains (domain ID)
- Topics it can read and/or write
- Partitions it can Join
- DataTags it can use

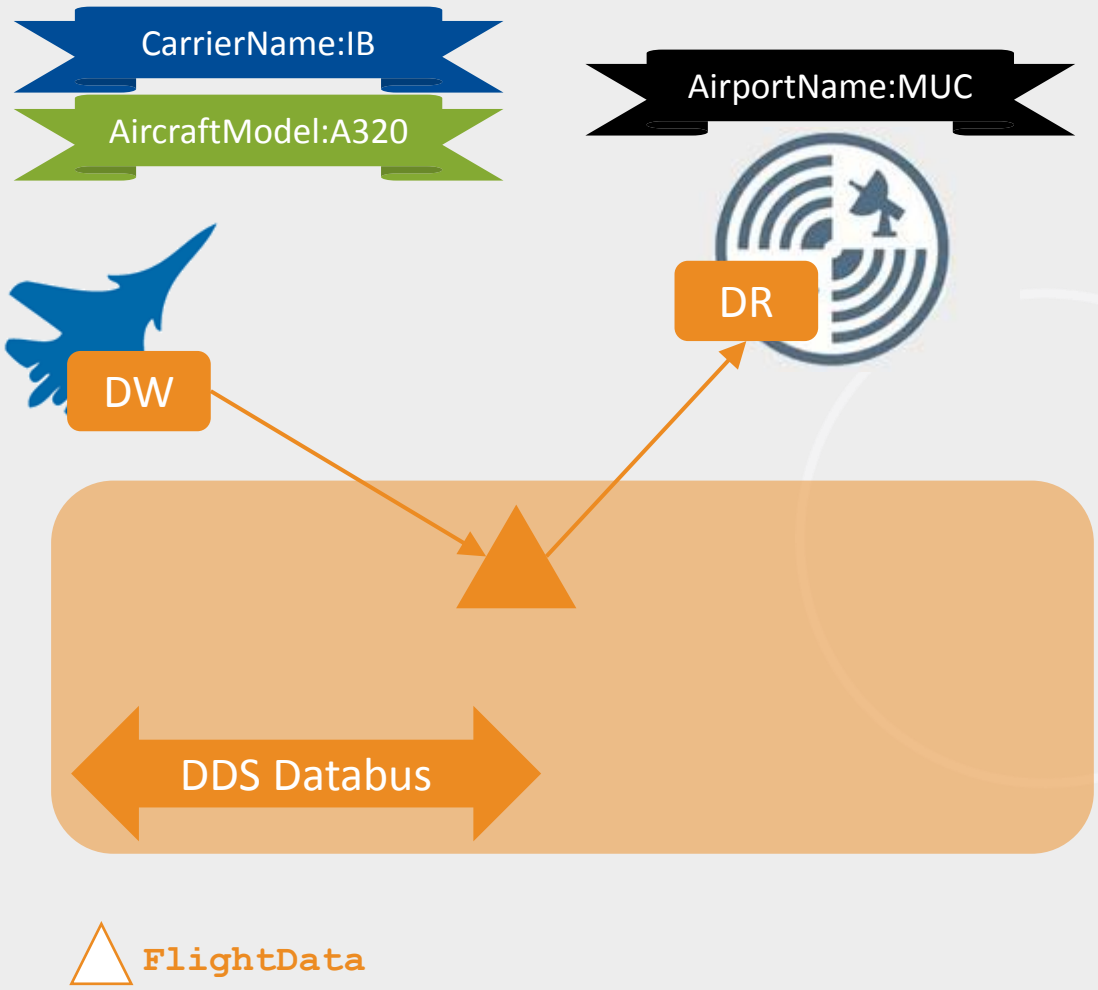
```
<dds xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:noNamespaceSchemaLocation="../schema/dds_security_permissions.xsd">
    <permissions>
        <grant name="ParticipantA">
            <subject_name>C=US, ST=CA, O=Real Time Innovations, CN=dtlsexample/emailAddress=r
            <validity>
                <!-- Format is CCYY-MM-DDThh:mm:ss[Z|(+|-)hh:mm] in GMT -->
                <not_before>2013-06-01T13:00:00</not_before>
                <not_after>2023-06-01T13:00:00</not_after>
            </validity>
            <allow_rule>
                <domains>
                    <id>0</id>
                </domains>
                <publish>
                    <topics>
                        <topic>Cir*</topic>
                    </topics>
                    <partitions>
                        <partition>P1*</partition>
                    </partitions>
                </publish>
                <subscribe>
                    <topics>
                        <topic>Sq*</topic>
                    </topics>
                    <partitions>
                        <partition>P2*</partition>
                    </partitions>
                </subscribe>
                <subscribe>
                    <topics>
                        <topic>Triangle</topic>
                    </topics>
                    <partitions>
                        <partition>P*</partition>
                    </partitions>
                </subscribe>
            </allow_rule>
            <default>ALLOW</default>
        </grant>
    </permissions>
</dds>
```

Understanding DataTags

- Immutable name-value pairs that can be associated with a DDS DataWriter or DataReader
- Matadata propagated by DDS Discovery
- Enforced by Access-Control
- Per-sample remote tags accessible using DDS API

```
Identity: IB-A320-123456
<allow_rule>
  …
  <publish>
    …
    <topics>
      <topic>FlightData</topic>
    </topics>
    <data_tags>
      <tag>
        <name>CarrierName</name>
        <value>IB</value>
      </tag>
      <tag>
        <name>AircraftModel</name>
        <value>A320</value>
      </tag>
    </data_tags>
  </publish>
</allow_rule>

(anything else, denied)
```

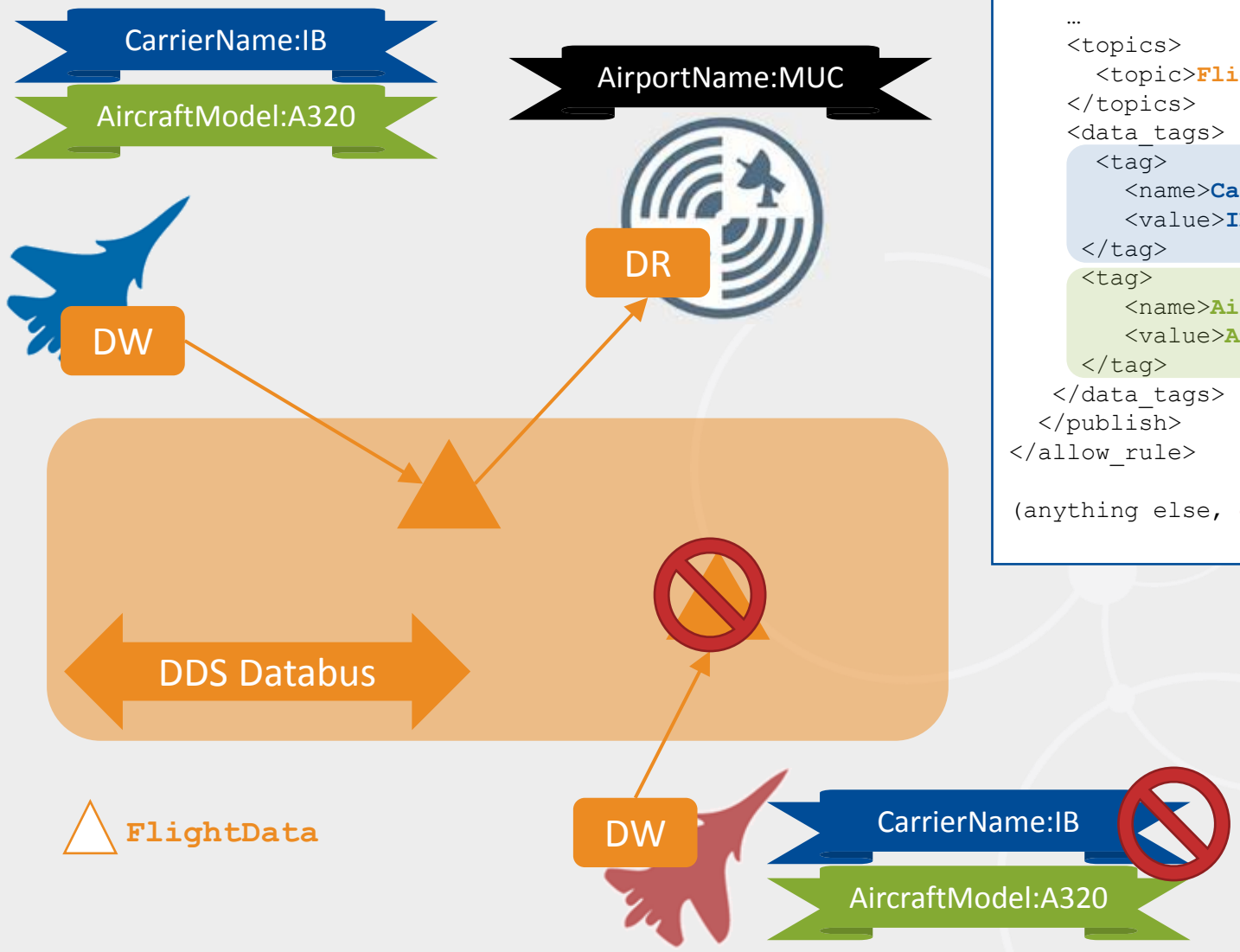
Security: Data Tagging




```
Identity: IB-A320-123456
<allow_rule>
  …
  <publish>
    …
    <topics>
      <topic>FlightData</topic>
    </topics>
    <data_tags>
      <tag>
        <name>CarrierName</name>
        <value>IB</value>
      </tag>
      <tag>
        <name>AircraftModel</name>
        <value>A320</value>
      </tag>
    </data_tags>
  </publish>
</allow_rule>

(anything else, denied)
```

```
Identity: ATC-MUC-2442
<allow_rule>
  …
  <subscribe>
    …
    <topics>
      <topic>FlightData</topic>
    </topics>
    <data_tags>
      <tag>
        <name>AirportName</name>
        <value>MUC</value>
      </tag>
    </data_tags>
  </subscribe>
</allow_rule>

(anything else, denied)
```

Security: Data Tagging



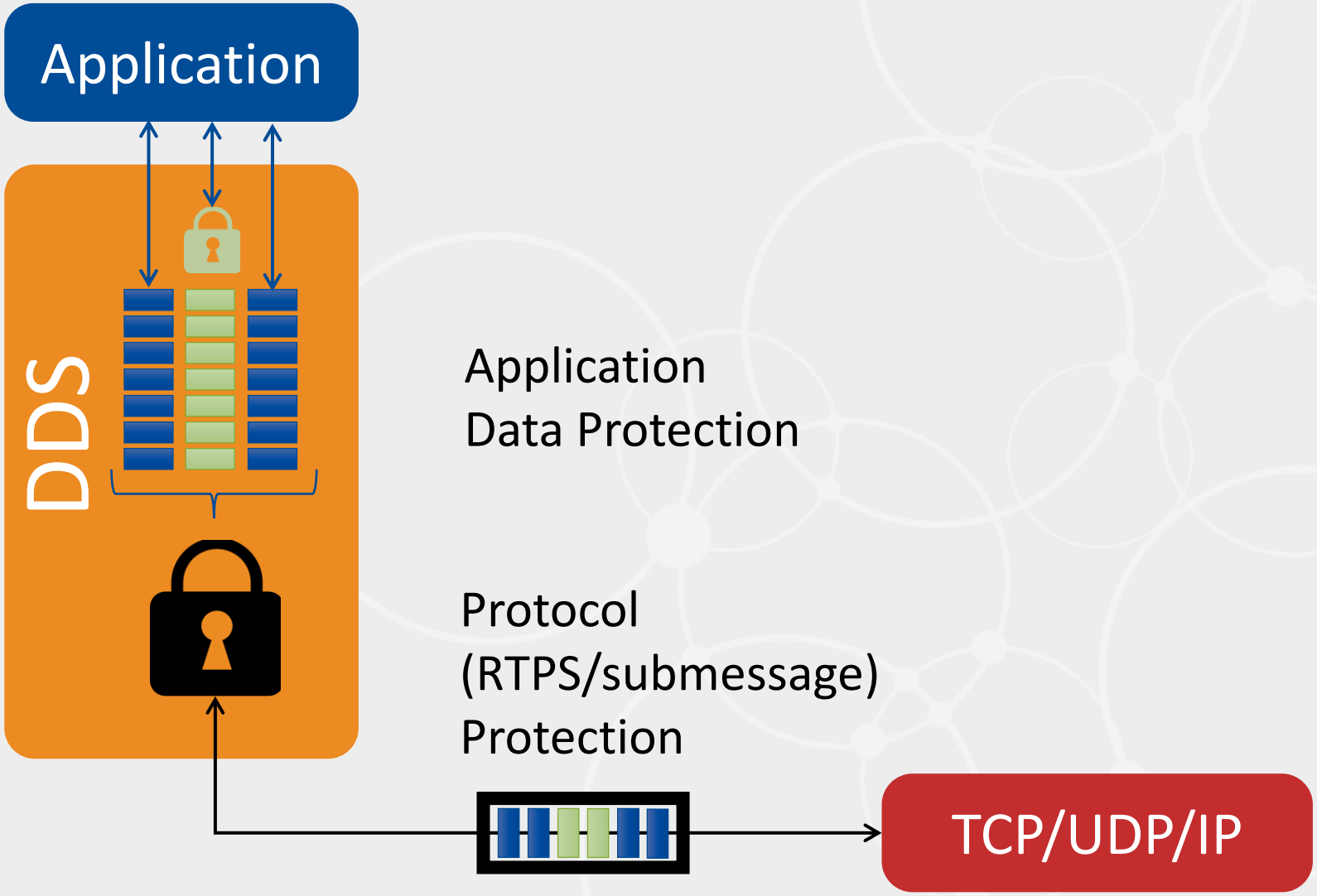

```
Identity: IB-A320-123456
<allow_rule>
  …
  <publish>
    …
    <topics>
      <topic>FlightData</topic>
    </topics>
    <data_tags>
      <tag>
        <name>CarrierName</name>
        <value>IB</value>
      </tag>
      <tag>
        <name>Aircra
        <value>A320<
      </tag>
    </data_tags>
  </publish>
</allow_rule>

(anything else, deni
```

```
Identity: ATC-MUC-2442
<allow_rule>
  …
  <subscribe>
    …
    <topics>
      <topic>FlightData</topic>
    </topics>
    <data_tags>
      <tag>
        <name>AirportName</name>
        <value>MUC</value>

nied)
```

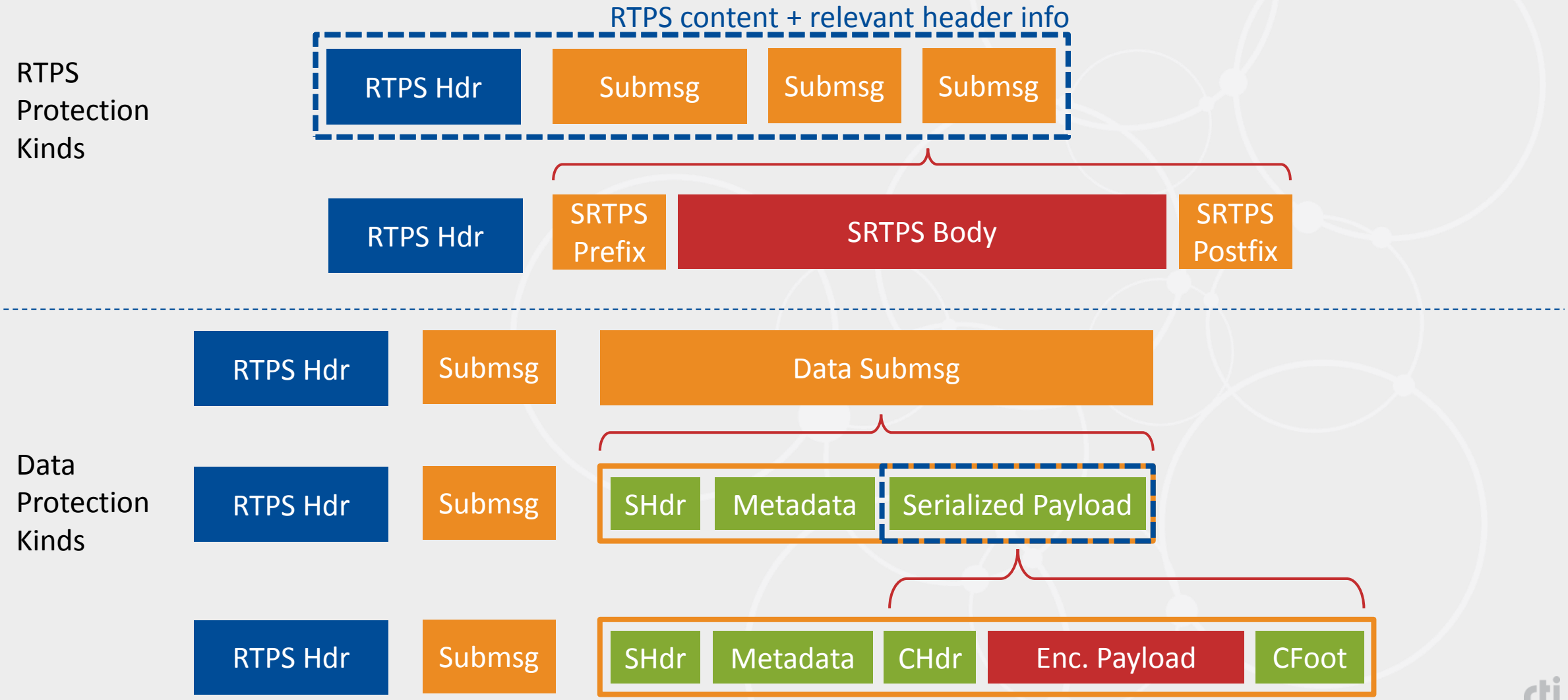
```
Identity: AF-A320-9696
<allow_rule>
  …
  <publish>
    …
    <topics>
      <topic>FlightData</topic>
    </topics>
    <data_tags>
      <tag>
        <name>CarrierName</name>
        <value>AF</value>
      </tag>
      <tag>
        <name>AircraftModel</name>
        <value>A320</value>
      </tag>
    </data_tags>
  </publish>
</allow_rule>

(anything else, denied)
```

DDS Security Performance

DDS : How the data is cryptographically protected

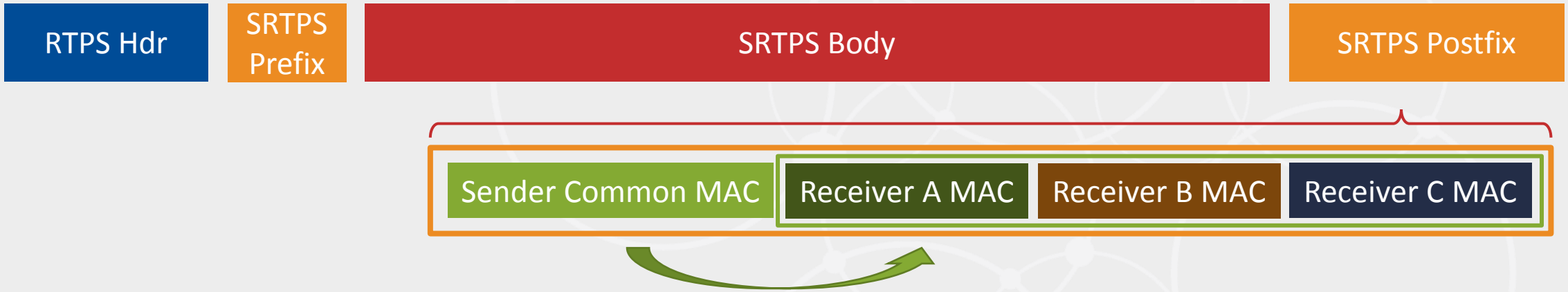


RTPS & Payload Protection Kinds

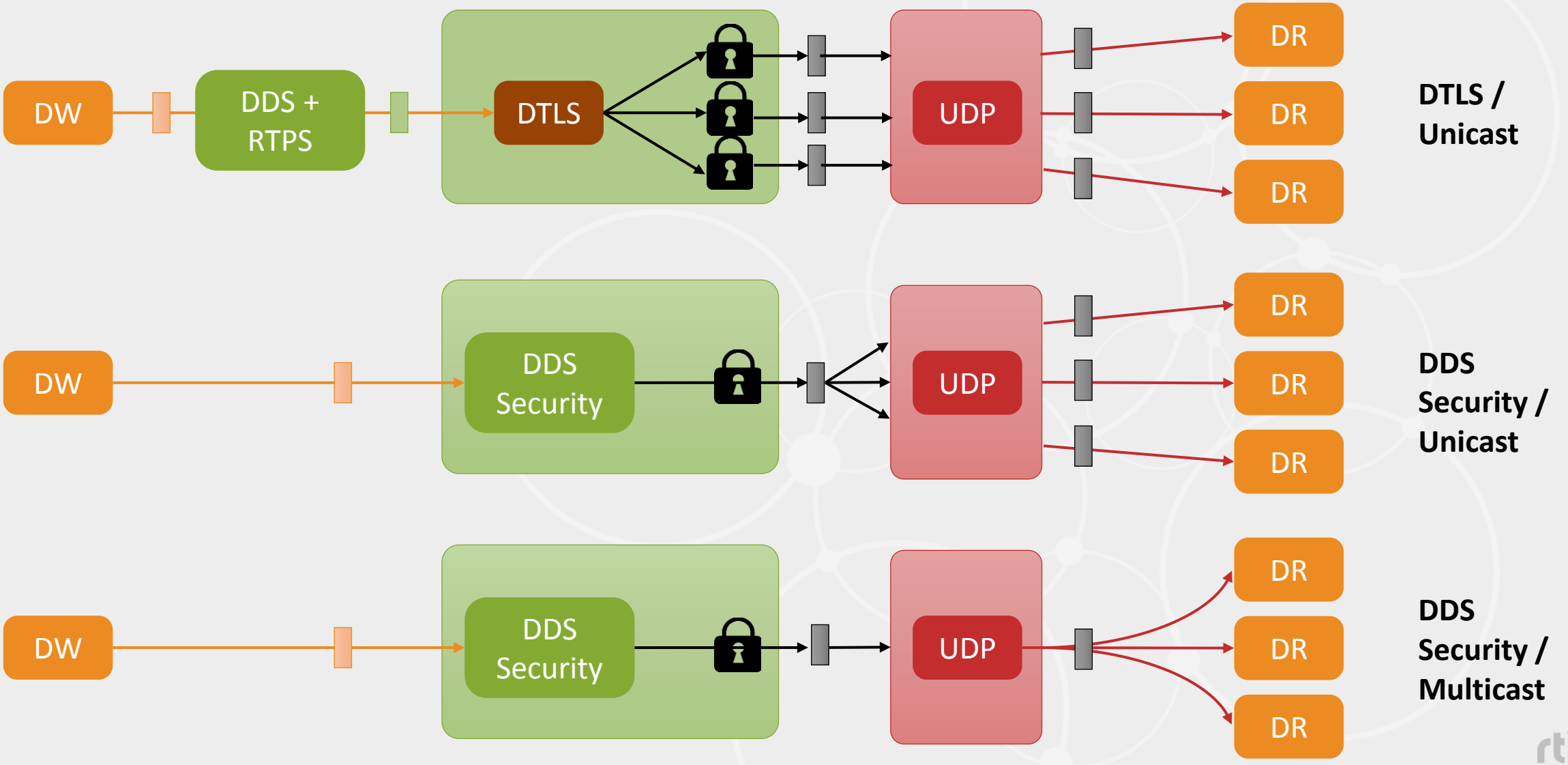


Origin Authentication Protection Kinds

- Enforce Permission to Read vs Write
- Prevent Insider Attacks



Transport Security (e.g. TLS) vs DDS Security



Performance Impact of enabling Security in DDS

DDS Relative Performance only (without RCL/RWM layers)

Using rtiperftest: https://github.com/rticommunity/rtiperftest

Testing platform:

- CPU: Intel i7 6-core CPU 3.33GHz, 12 GB RAM
- NIC: Intel I350, 1 Gb/s
- CentOS Linux 7.1
- C++ API

1 to 1 latency (50 percentile) in milli seconds

Data Size	No Security	Sign Message	Sign Message + Encrypt Data	Sign Message + Encrypt Data + Origin Auth
32 B	0.037	0.046	0.050	0.052
256 B	0.041	0.051	0.055	0.057
2 KB	0.068	0.079	0.086	0.088
16 KB	0.195	0.221	0.250	0.253
128 KB	1.12	1.27	1.51	1.52
1 MB	8.76	8.82	10.92	10.94
Overhead		**1% - 24%**	**25% - 35%**	**25% - 41%**

Performance Impact of enabling Security in DDS

DDS Performance only (without RCL/RWM layers)

Using rtiperftest: https://github.com/rticommunity/rtiperftest

Testing platform:

- CPU: Intel i7 6-core CPU 3.33GHz, 12 GB RAM
- NIC: Intel I350, 1 Gb/s
- CentOS Linux 7.1
- C++ API

1 to 1 throughput (Mbps)

Data Size	No Security	Sign Message	Sign Message + Encrypt Data	Sign Message + Encrypt Data + Origin Auth
32 B	22	18	16	15.5
256 B	177	132	122	120
2 KB	939	895	803	779
16 KB	988	984	981	980
128 KB	991	990	953	957
1 MB	980	985	887	888
Overhead		**0% - 25%**	**1% - 31%**	**1% - 32 %**

Impact of Security on Scalability

1:N Latency (micro seconds)
For 32 Bytes, Multicast

Num Subscribers	No Security	Sign Message	Sign Message + Encrypt Data	Sign Message + Encrypt Data + Origin Auth
1	38	47	51	54
2	35	44	48	50
4	37	48	51	55

1:N Latency (micro seconds)
For 2 KB, Multicast

Num Subscribers	No Security	Sign Message	Sign Message + Encrypt Data	Sign Message + Encrypt Data + Origin Auth
1	69	80	87	89
2	67	79	86	88
4	69	80	87	90

1:N Latency (micro seconds)
For 128 KB, Multicast

Num Subscribers	No Security	Sign Message	Sign Message + Encrypt Data	Sign Message + Encrypt Data + Origin Auth
1	1209	1279	1522	1525
2	1205	1286	1526	1525
4	1203	1282	1530	1534

Impact of Security on Scalability

1:N Throughput (Mbps)
For 32 Bytes, Multicast

Num Subscribers	No Security	Sign Message	Sign Message + Encrypt Data	Sign Message + Encrypt Data + Origin Auth
1	22.5	17.2	15.5	14.8
2	20.1	15.8	14.5	13.3
4	18.4	11.9	11.9	9.6

1:N Throughput (Mbps)
For 2 KB, Multicast

Num Subscribers	No Security	Sign Message	Sign Message + Encrypt Data	Sign Message + Encrypt Data + Origin Auth
1	939.0	893.4	796.3	761.7
2	938.9	877.7	747.3	660.0
4	938.9	742.6	655.1	531.1

1:N Throughput (Mbps)
For 128 KB, Multicast

Num Subscribers	No Security	Sign Message	Sign Message + Encrypt Data	Sign Message + Encrypt Data + Origin Auth
1	991.5	990.4	954.7	955.8
2	991.5	990.4	970.7	964.6
4	991.5	990.3	984.3	982.0

ROS2 on DDS

ROS2 on DDS

ROS Concept	DDS Concept
Node	Participant
Node Namespace	<none>
Topic	Topic
Publisher	Publisher + DataWriter
Subscriber	Subscriber + DataReader
Service	Service(*) or Request/Reply Topic pair
Qos Profile	Qos Profile
Action	Not implemented yet
Parameter	ROS-defined DDS Services to read/write/list parameters

ROS2 on DDS mapping

ROS Concept	DDS Concept
TopicName: rosTopicName	**TopicName:** ddsTopicName = “rt/” + rosNamespace + rosTopicName
Qos Policies/Profiles (3): rmw_qos_history_policy_t rmw_qos_reliability_policy_t rmw_qos_durability_policy_t;	**DDS Qos Policies/Profiles (22):** HISTORY RELIABILITY DURABILITY (kinds VOLATILE, TRANSIENT_LOCAL) Remaining 19 DDS Policies (e.g. PARTITION, OWNERSHIP) are not mapped
ServiceName: rosServiceName	**With DDS-RPC -> DDS Service (RequesTopic, ReplyTopic):** ddsServiceName = “rs/” + rosServiceName **With no DDS-RPC support -> user RequesTopic, ReplyTopic) pair:** ddsRequestTopic = “rq/” + rosServiceName ddsReplyTopic = “rr/” + rosServiceName
Parameter	ROS-defined DDS Services to read/write/list parameters

Using DDS Secure in ROS2

Tools

- SROS offers command-line tools that simply configuration and deployment of DDS Security with ROS2.
- These tools also manage the Topic/Service name mappings to DDS

```
$ ros2 security <command>
        create_key          Create key
        create_keystore     Create keystore
        create_permission   Create permission
        distribute_key      Distribute key
        list_keys           List key

$ keymint <command>
        keystore
```

Come to the SROS tutorial @IROS. Monday 14:30-18:00. Room 4.R4

https://ruffsl.github.io/IROS2018_SROS2_Tutorial/

How to use it?

Secure Talker/Listener

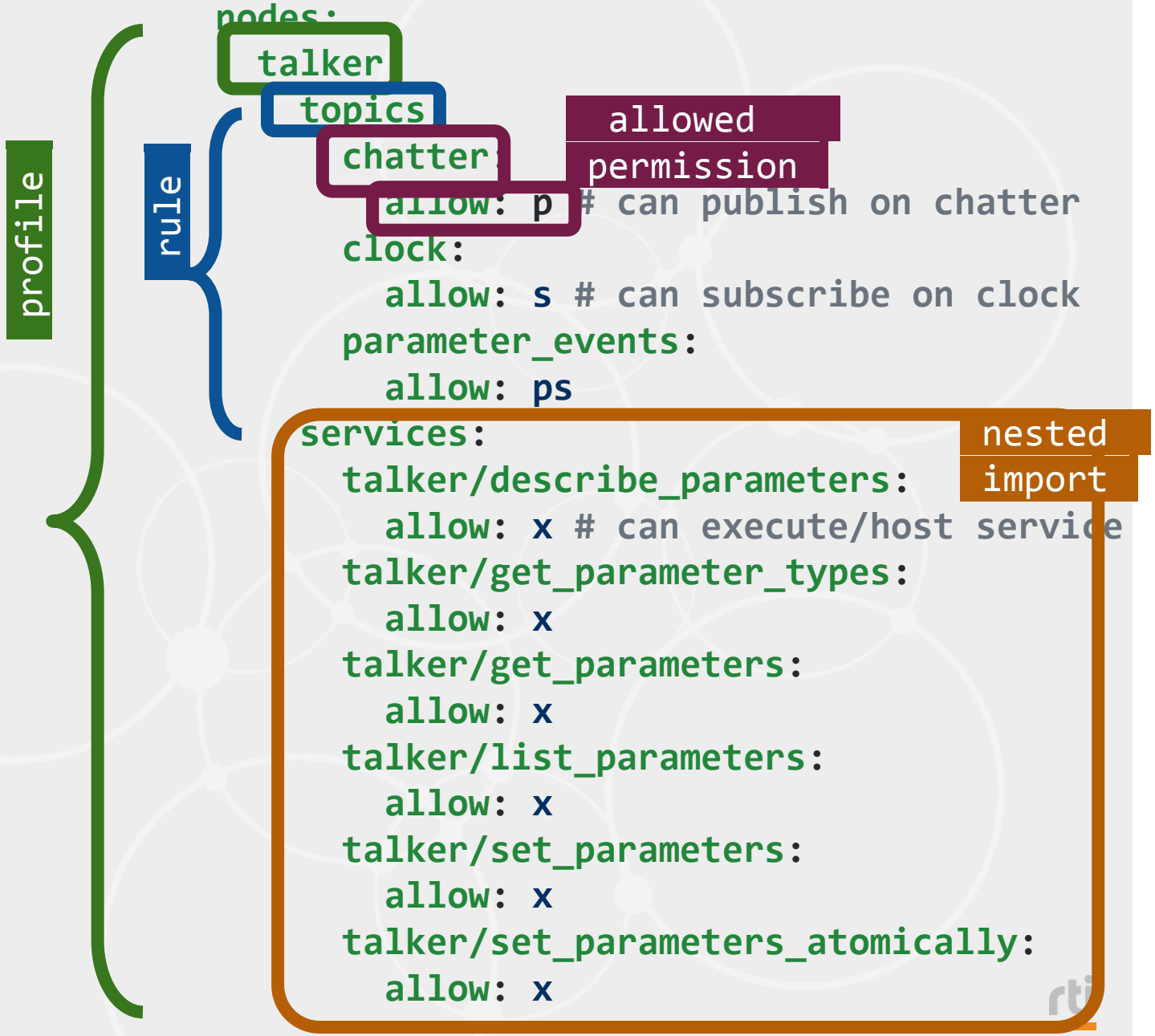
Minimal talker profile

```
nodes:
  talker:
    topics:
      chatter:
        allow: p # can publish on chatter
      clock:
        allow: s # can subscribe on clock
      parameter_events:
        allow: ps
    services:
      talker/describe_parameters:
        allow: x # can execute/host service
      talker/get_parameter_types:
        allow: x
      talker/get_parameters:
        allow: x
      talker/list_parameters:
        allow: x
      talker/set_parameters:
        allow: x
      talker/set_parameters_atomically:
        allow: x
```

How to use it?

Secure Talker/Listener

Minimal talker profile



How to use it?

Secure Talker/Listener

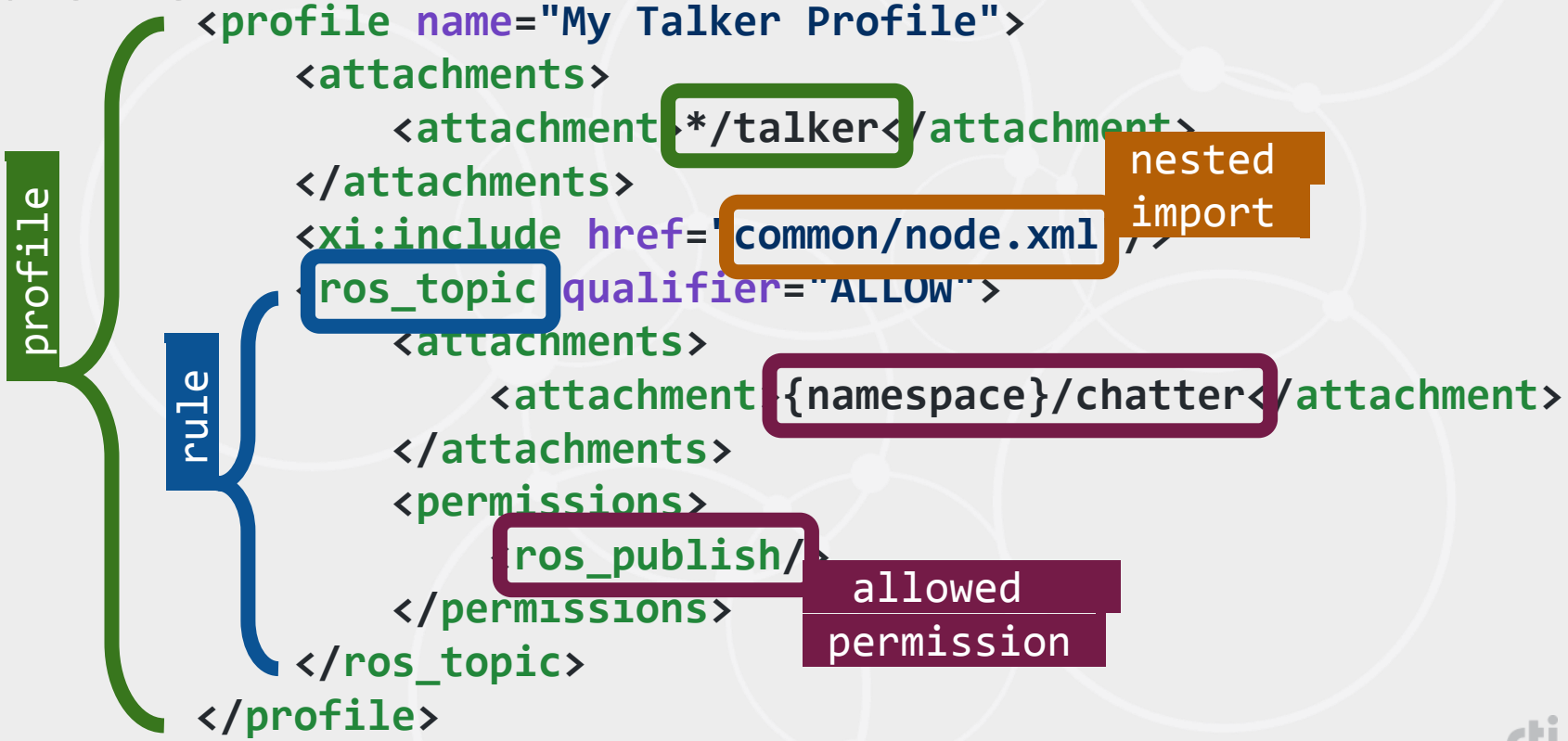
Minimal talker profile

```
<profile name="My Talker Profile">
    <attachments>
        <attachment>*/talker</attachment>
    </attachments>
    <xi:include href="common/node.xml"/>
    <ros_topic qualifier="ALLOW">
        <attachments>
            <attachment>{namespace}/chatter</attachment>
        </attachments>
        <permissions>
            <ros_publish/>
        </permissions>
    </ros_topic>
</profile>
```

How to use it?

Secure Talker/Listener

Minimal talker profile



DDS Secure features available in SROS

- Node (Participant) Authentication
- Access control to Domains
- Access Control to Topics (Node & Topic)
- Access Control to Services (Node & Service granularity)
- Access Control to Parameter (Node granularity)
- Encryption of RTPS Messages and application Data

DDS Secure features currently “not exposed” in SROS

- Access Control to Partitions
- Securing Data Tags
- Fine-grained control of secure discovery
- Fine grain control of Encryption vs Authentication (MAC)
- Use of Origin Authentication
  - Protection against privilege escalation (Read -> Write)

DDS Security provides excellent support to secure ROS

- Standard & Interoperable
- Performant and Scalable
  - Best-of-class cryptography (Elliptic Curve, Diffie Hellman, AES)
  - Single payload encryption multiple destinations, multicast support
- Fine-grained:
  - Access Control at the Node/Topic/Service level
- Flexible:
  - Choice of Encryption vs Authentication vs Origin Authentication
  - Build your own plugins
- Infrastructure-independent:
  - Works over any Transport with any Qos
  - Does not depend on IPSEC, Trusted Routers, Pre-Shared Keys,…
- **Transparent: No changes to Application Code!**
- **Tools being developed to facilitate config and deployment**

References

- http://portals.omg.org/dds
- https://www.omg.org/spec/category/data-distribution-service
- https://www.omg.org/spec/DDS-SECURITY
- http://community.rti.com
- http://www.rti.com
- https://github.com/rticommunity
- https://www.slideshare.net/GerardoPardo/presentations
- https://ruffsl.github.io/IROS2018_SROS2_Tutorial

Thank you!

Questions?