Your systems.
Working as one.

DDS Security concepts for SROS

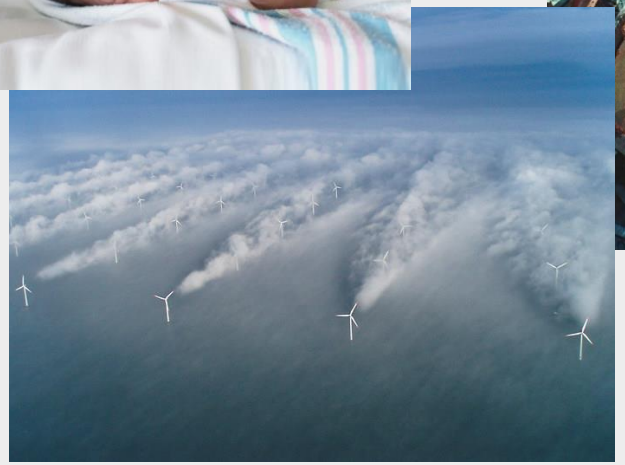
Gerardo Pardo, Ph.D., CTO, RTI, gerardo __at__ rti.com

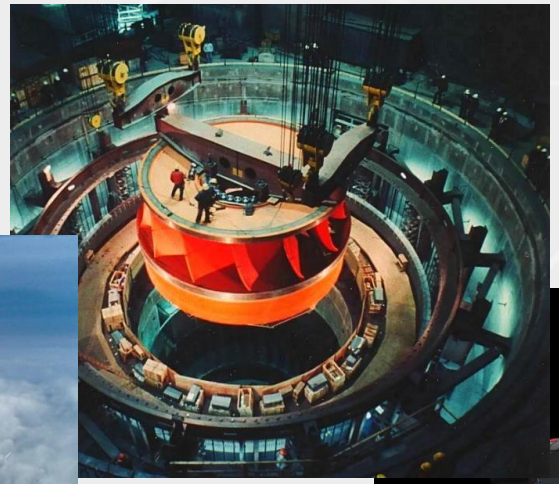
Ruffin White, UC San Diego, rwhitema __at__ eng.ucsd.edu

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

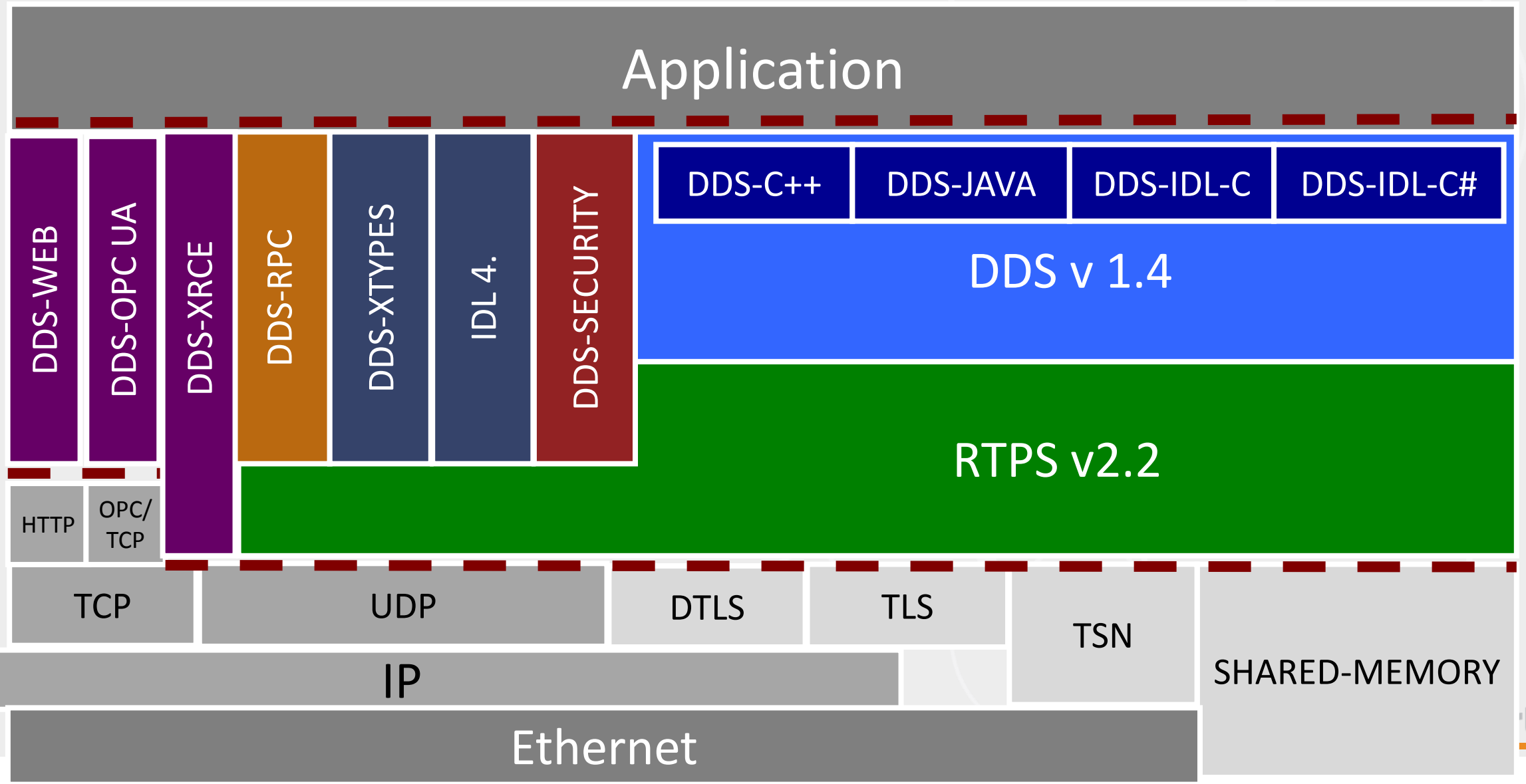
To enable and realize the potential of smart machines to serve mankind

Outline

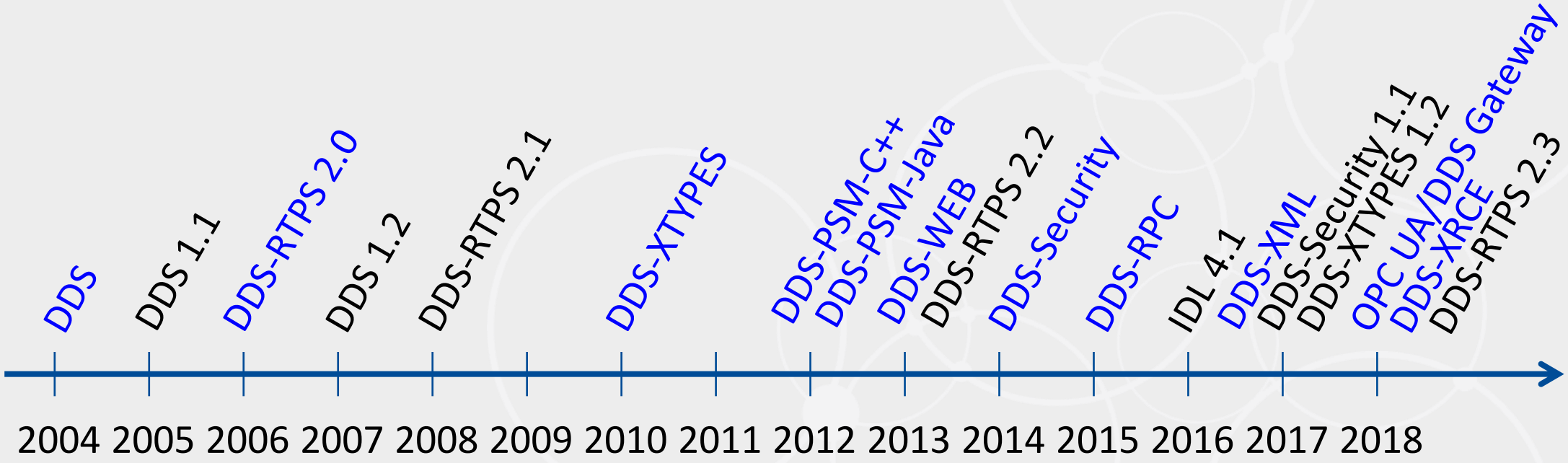
- Intro to DDS
- Intro to DDS Security
- Security at the Wire Protocol level
- Performance Impact
- Takeaways

Data Distribution Service (DDS)

DDS Specification family



Timeline



DDS and the Industrial Internet of Things

rti Your systems. Working as one.

Deployed in 1000s of Systems












Industries: Energy, Industrial Control, Transportation, Healthcare, Defense

Industrial IoT Systems

- Reliability: Severe consequences if offline for 5ms (or 5 min)
- Real-time: measure in ms or µs
- Interface scale: 10+ applications/teams
- Dataflow complexity: data has many destinations
- Architecture: Next generation IIoT

3+ Yes? → DDS

AUTOSAR

OSA · FACE Future Airborne Capability Environment · MD PnP Getting connected for patient safety · OPEN CONNECTIVITY FOUNDATION · The Open Group OPEN PROCESS AUTOMATION™ FORUM · SGIP SMART GRID INTEROPERABILITY PANEL · ICE Alliance Integrating Clinical Environments · ROS · NGVA · AVnu · OpenFog · rti

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

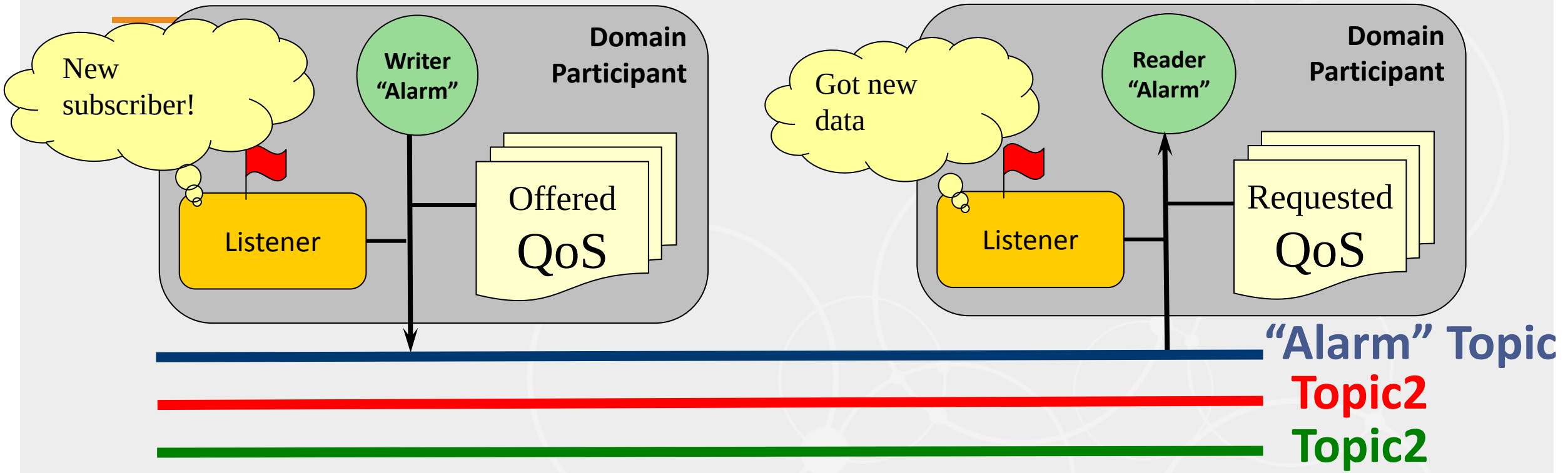
DATABUS

QoS
Topic D

Persistence Service

Recording Service

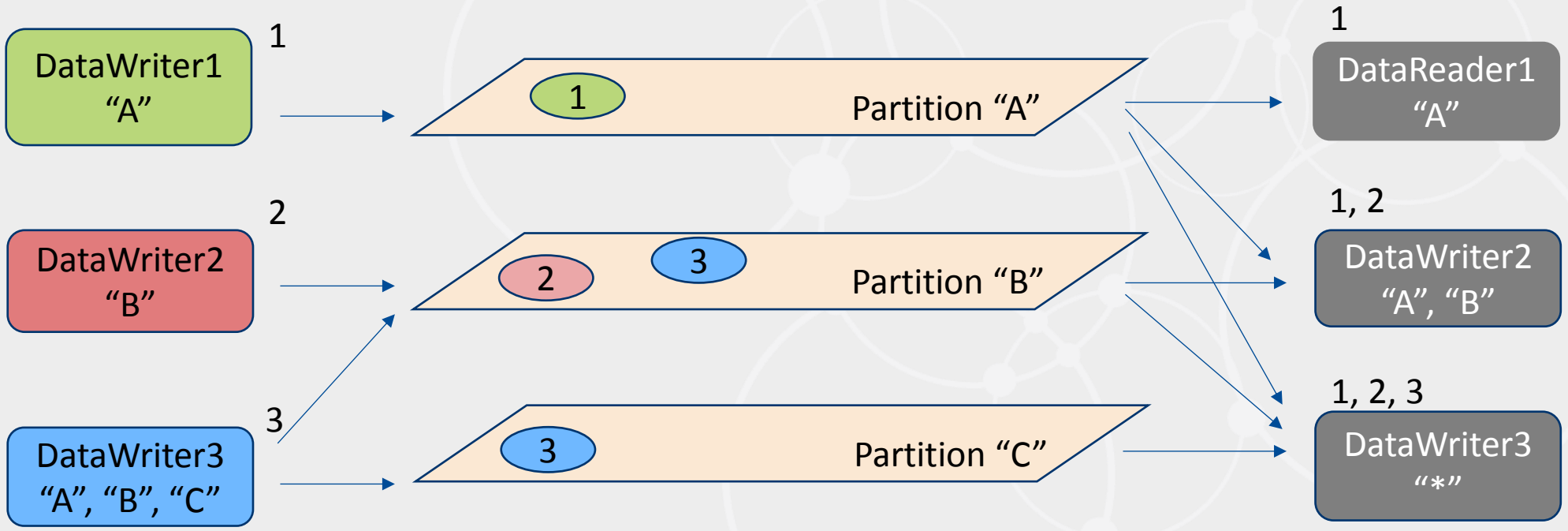
Data-Centric Communications Model



- **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	Availability
PRESENTATION		
DESTINATION ORDER		
OWNERSHIP		
OWNERSHIP STRENGTH		
LIVELINESS		
LATENCY BUDGET	Transport	
TRANSPORT PRIORITY		

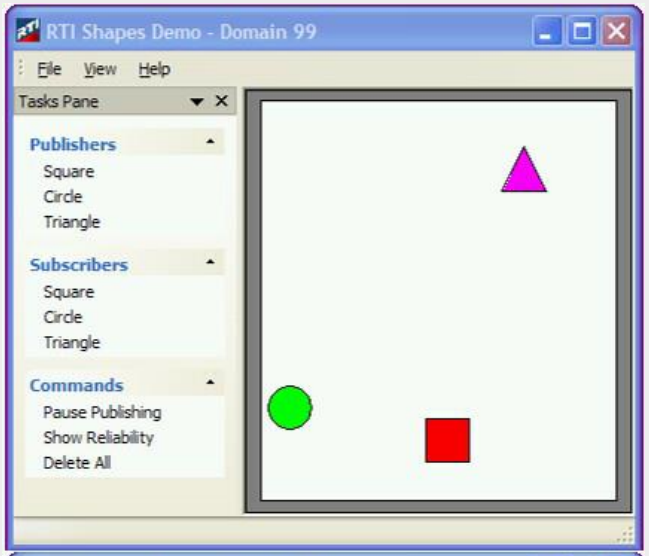
ROS2 on DDS

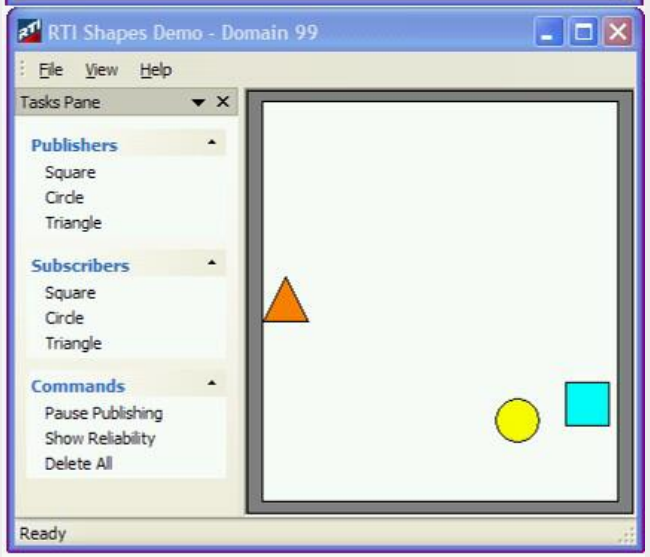
ROS Concept	DDS Concept
Node	Participant
Node Namespace	<none>
Topic	Topic
Publisher	Publisher + DataWriter
Subscriber	Subscriber + DataReader
Service	Service(*) or Request/Reply Topic pair
Qos Profile	Qos Profile (Subset of DDS Qos available in ROS2)
Action	Not implemented yet
Parameter	ROS-defined DDS Services to read/write/list parameters

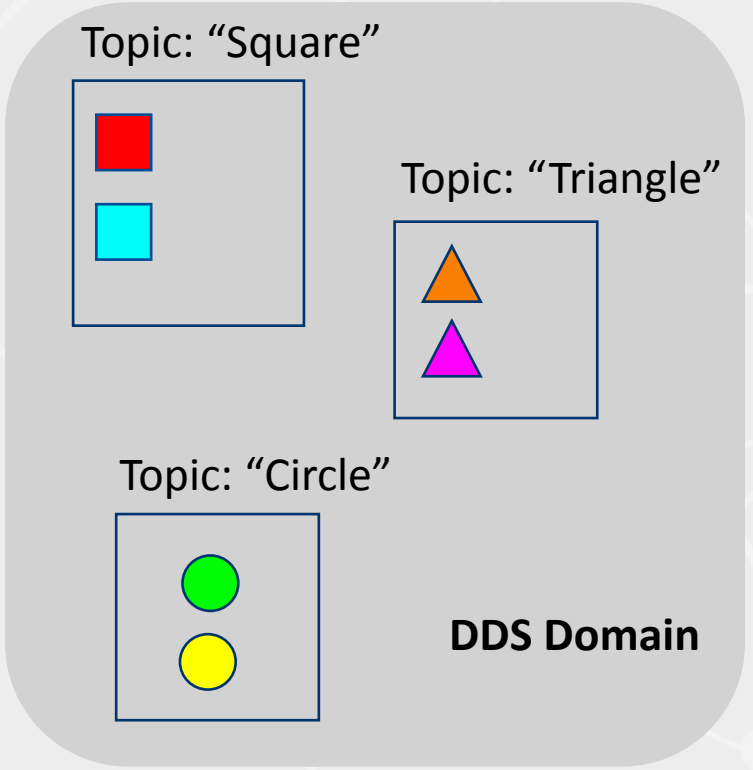
Shapes Demo

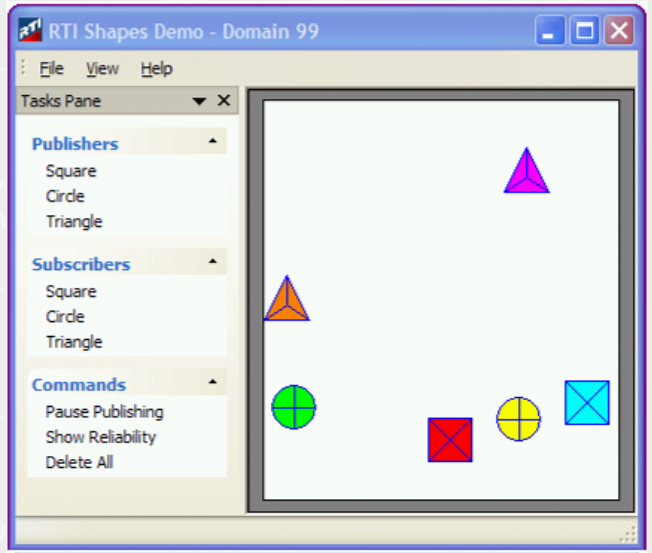
Shapes Demo uses 3 Topics

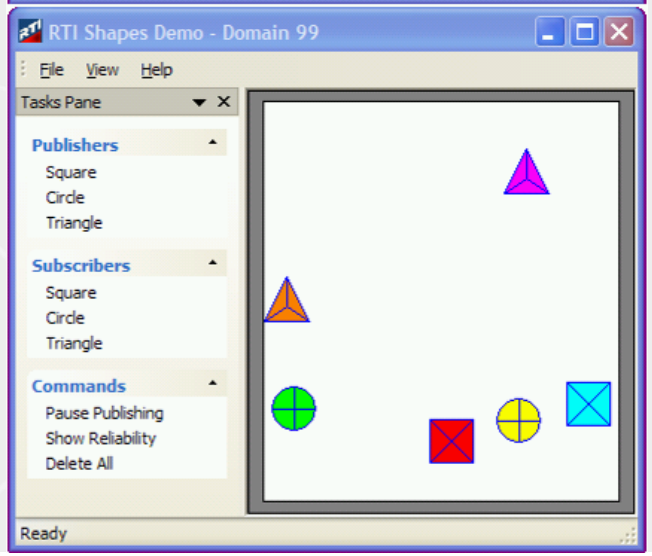
```
struct Shape {
    @key string color;
    int32 x;
    int32 y
    int16 size;
};
```







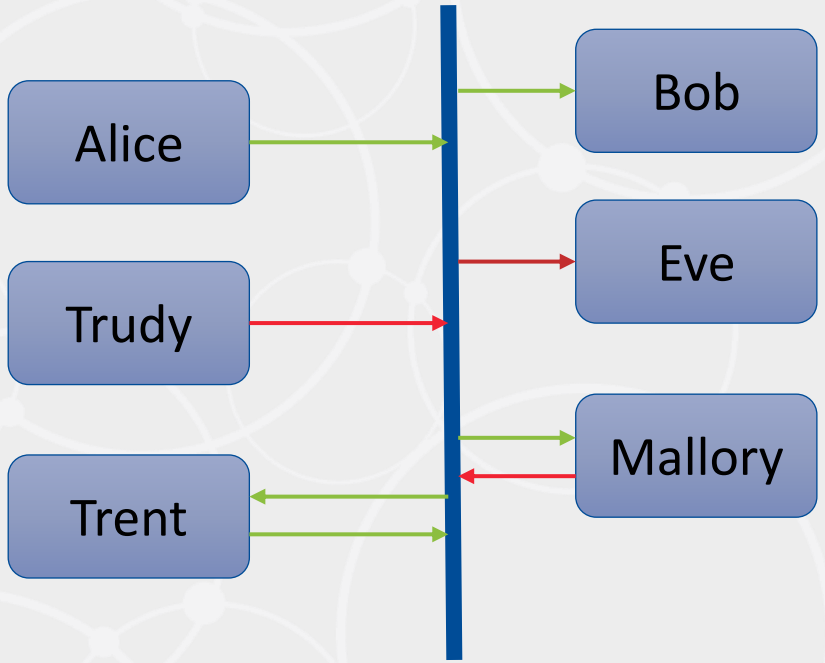




DDS Security

Threats

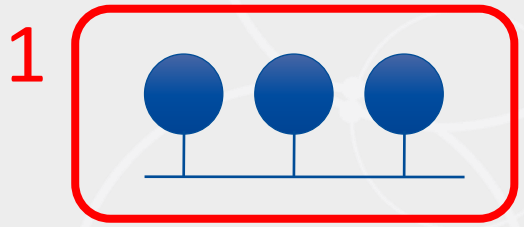
- Unauthorized Subscription
- Unauthorized Publication
- Tampering & Replay
- Insider Attack

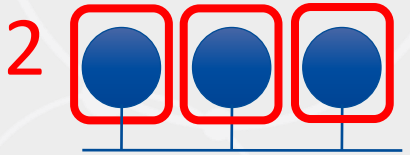


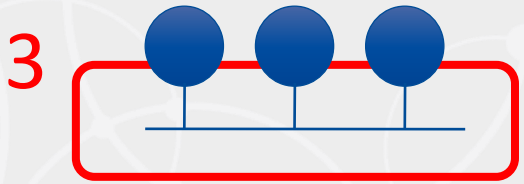
Local machine is assumed to be trusted

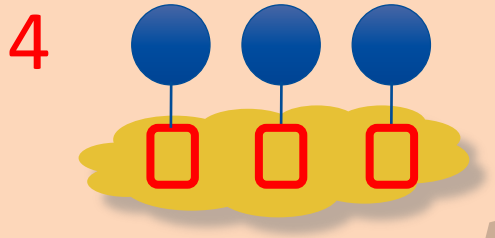
Security Must Protect Dataflow, Too

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

DDS Domain

Topic

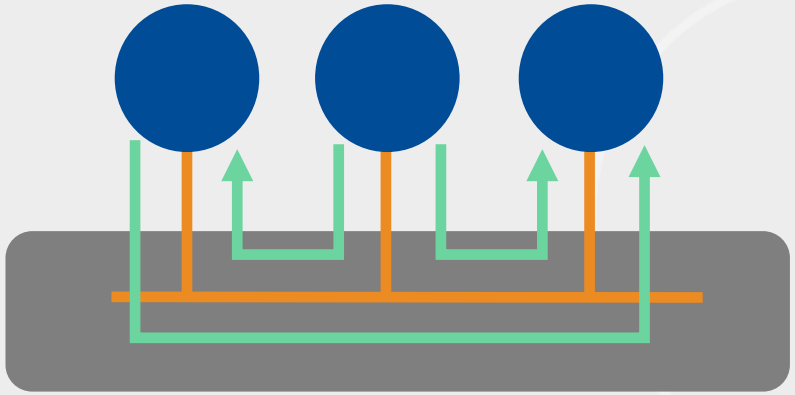
Line	Flight	Dest	Arv
UA	5		7:32
AA	4		9:15
AA			9:15
AA		LAX	9:15

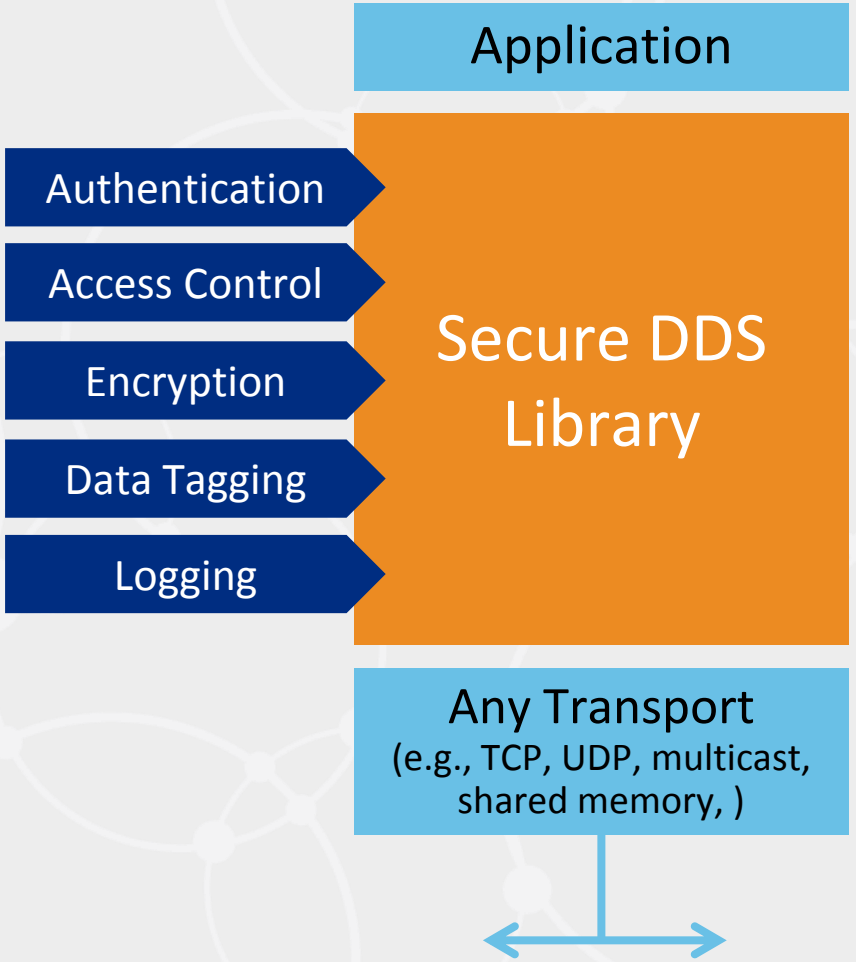
Squawk	Line	Flight
1234	A	567
7654	A	432
765		432

Squawk	Long	Lat	Alt
1234		2.0	500.0
7654		0	250.0
7654		74.0	250.0
7654		-74.0	250.0

Fine-Grained, DDS Security

Data Flow Security, by Topic

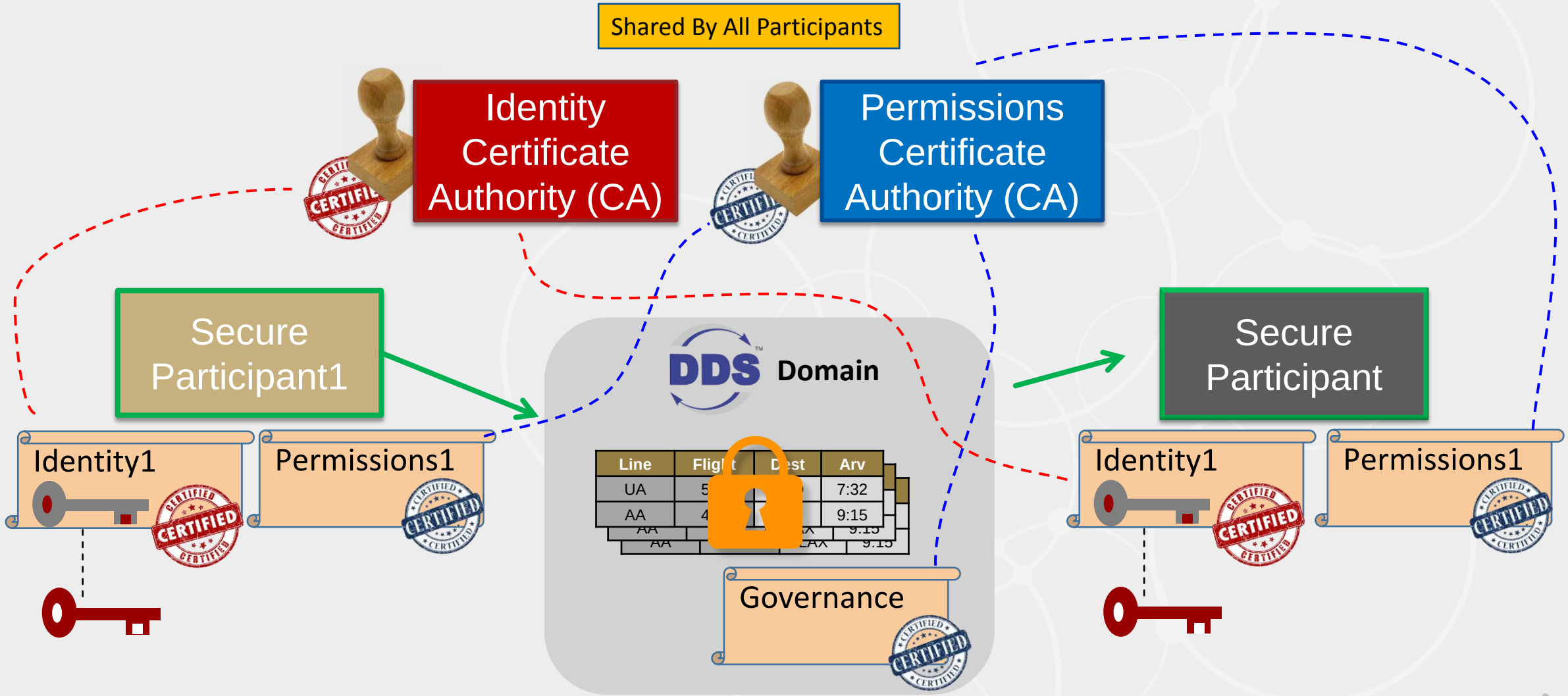




Service Plugin	Purpose	Interactions
Authentication	Authenticate the principal that is joining a DDS Domain. **Handshake and establish shared secret between participants**	Principal may be an application/process or the user associated with that application or process. Can do mutual authentication and establish shared secret
Access Control	Decide whether a principal is allowed to perform a protected operation.	Protected operations include joining a specific DDS domain, creating a Topic, reading a Topic, writing a Topic, etc.
Cryptography	Perform the encryption and decryption operations. Create & Exchange Keys. Compute digests, compute and verify Message Authentication Codes. Sign and verify signatures of messages.	Invoked by DDS middleware to encrypt data compute and verify MAC, compute & verify Digital Signatures
Logging	Log all security relevant events	Invoked by middleware to log
Data Tagging	Enforce meta-data associated with each DataWriter and DataReader	Distributed via Discovery Enforced by Permissions plugin

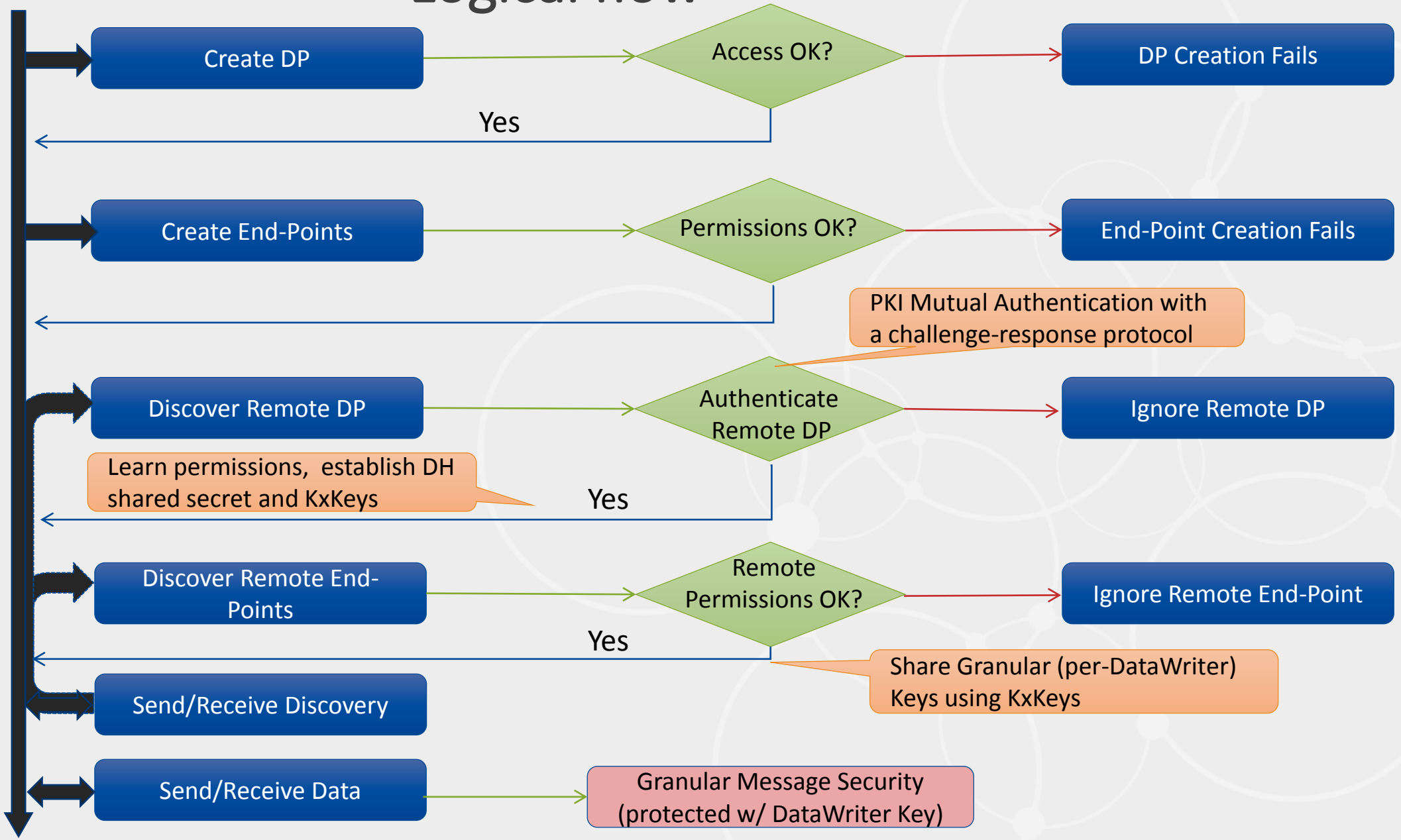
SPI	Builtin Plungin	Notes
Authentication	DDS:Auth:PKI-DH	PKI with a pre-configured Identity CA RSA or ECDSA for authentication DH or ECDH to establish a shared secret
AccessControl	DDS:Access:Permissions	Governance Document and Permissions Document Each signed by pre-configured Permissions CA
Cryptography	DDS:Crypto:AES-GCM-GMAC	Key Generation, Distribution, Encryption and Message Authentication AES-GCM for authenticated encryption AES-GMAC for only message authentication Can use 128 or 256 bit keys
DataTagging	Discovered_EndpointTags	Force association of meta-data with Tags with DataWriters and DataReaders
Logging	DedicatedDDS_LogTopic	Log security-relevant events

DDS Security Configuration



DP = Domain Participant
Endpoint = Reader / Writer

Logical flow



Builtin DDS:PKI-DSA-DH

- Uses shared Certificate Authority (CA)
  - All Participants pre-configured with Shared-CA
  - Each participant has Signed CERT from Shared-CA
  - Can use RSA or EC keys
- Mutual authentication between discovered participants using a challenge-response
- Establishes a shared secret using Diffie-Hellman (DH) or Elliptic Curve DH (ECDH) (Ephemeral Mode)

PKI-Based Mutual Authentication Protocol

C1 := Cert1 , Perm1, pdata_1, ds_algo1, ss_algo1

C2 := Cert2 , Perm2, pdata_2, ds_algo2, ss_algo2

1. P1 <- P2: ParticipantDiscovery (pdata)
2. P1 -> P2: C1, Challenge1, DH1
3. P1 <- P2: C2, Challenge1, Challenge2, DH2, DH1,
   SignP2(Hash(C2)|Challenge2|DH2|Challenge1|DH1|Hash(C1))
4. P1 -> P2: DH1, DH2, Challenge1, Challenge2,
   SignP1(Hash(C1)|Challenge1|DH1|Challenge2|DH2|Hash(C2))

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>
```

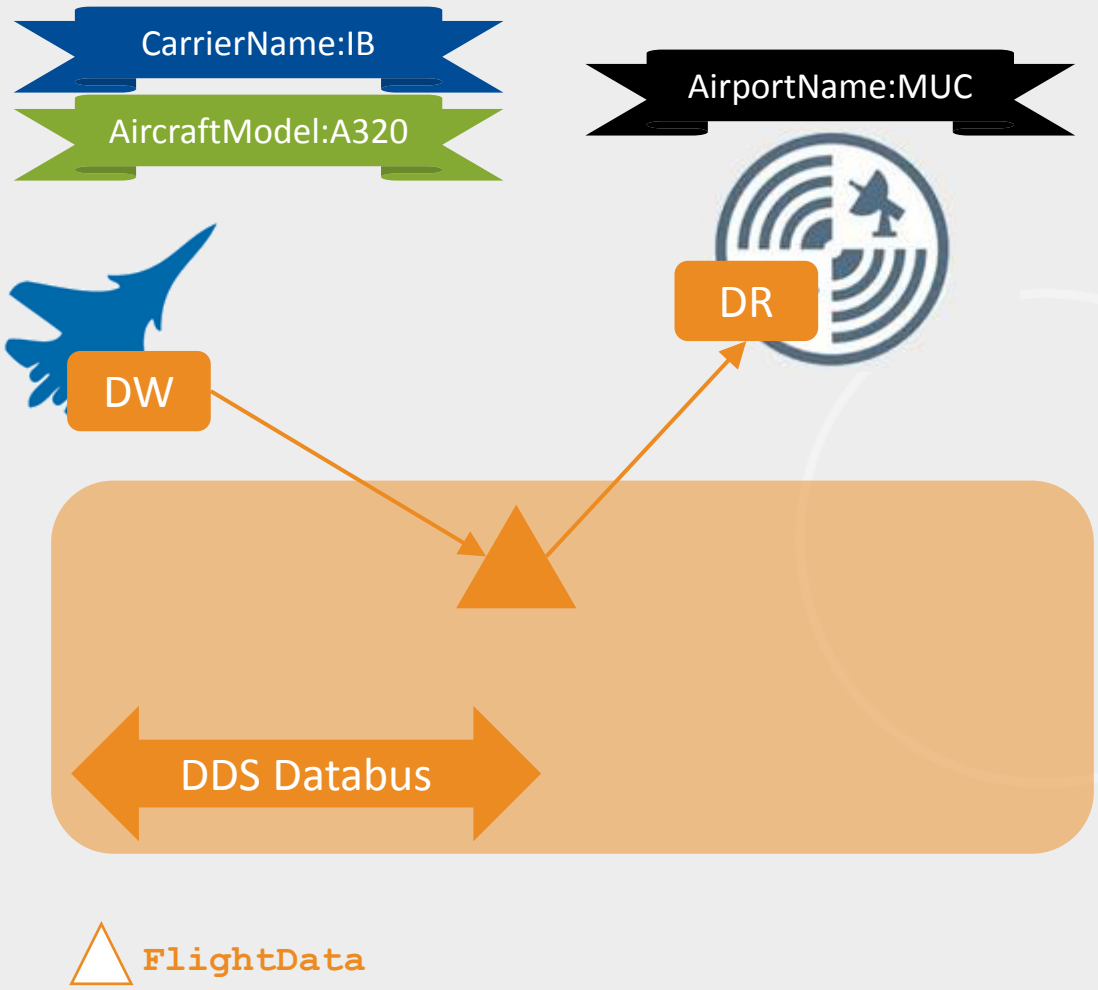
Understanding DataTags

- 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



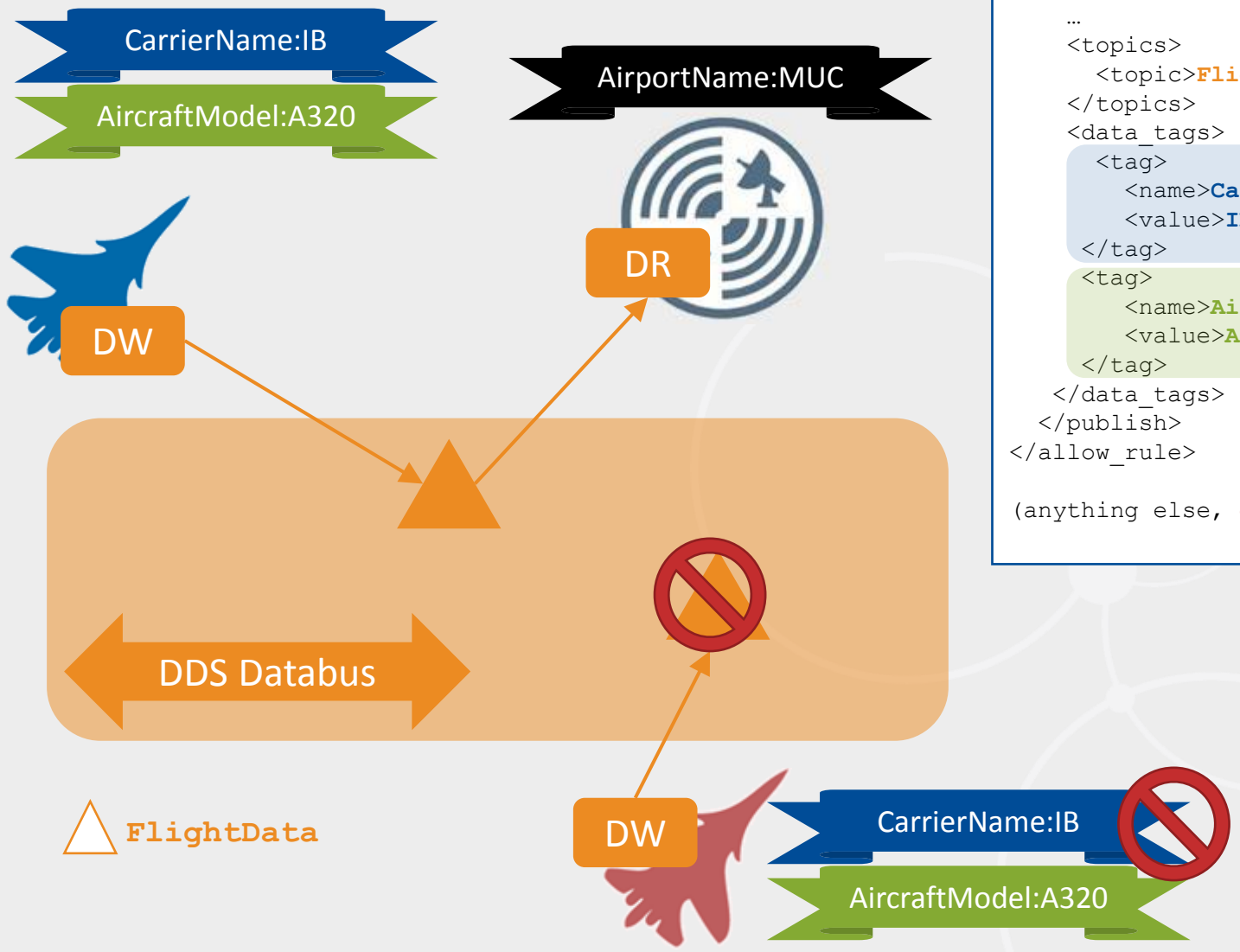

```
Identity: IB-A320-123456
<allow_rule>
  …
  <publish>
    …
    <topics>
      <topic>FlightData</topic>
    </topics>
    <data_tags>
      <tag>
        <name>CarrierName</name>
        <value>IB</value>
      </tag>
      <tag>
        <name>AircraftModel</name>
        <value>A320</value>
  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

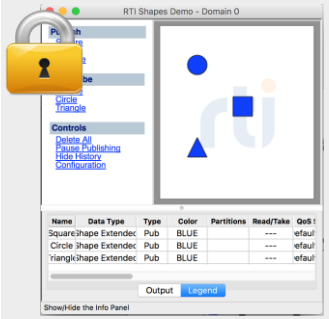
Configuration possibilities

- Are “legacy” or un-identified applications allowed in the Domain? Yes or No.
  - If yes an Unauthenticated applications will:
    - See the “unsecured” discovery Topics
    - Be allowed to read/write the “unsecured” Topics
- Is a particular Topic discovered over protected discovery?
  - If so it can only be seen by “authenticated applications”
- Is a access particular Topic protected?
  - If so only authenticated applications with the correct permissions can read/write
- Is data on a particular Topic protected? How?
  - If so data will be sent signed or encrypted+signed
- Are all protocol messages signed? Encrypted?
  - If so only authenticated applications with right permissions will see anything

DDS Secure Shapes Demo

Setup: Governance & Permissions

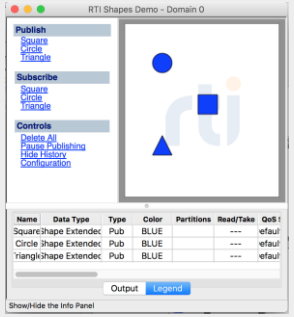
Participant1



AllowAll

Permissions:
Publish: *
Subscribe: *

NoSecurity



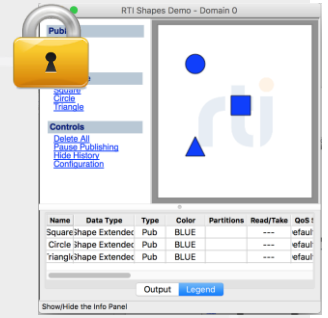
Topic: “Square”

Topic: “Triangle”

Topic: “Circle”

Governance:
Circle -> Open
Square -> Encrypt
Triangle -> Encrypt

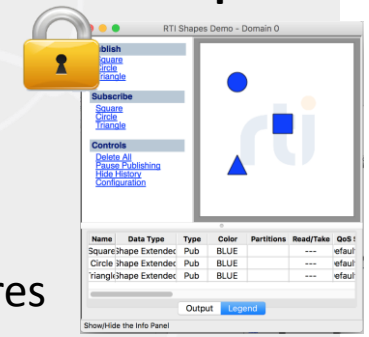
Participant2



DenyPubCircle

Permissions:
Publish: Square, Triangle
Subscribe: *

Participant3

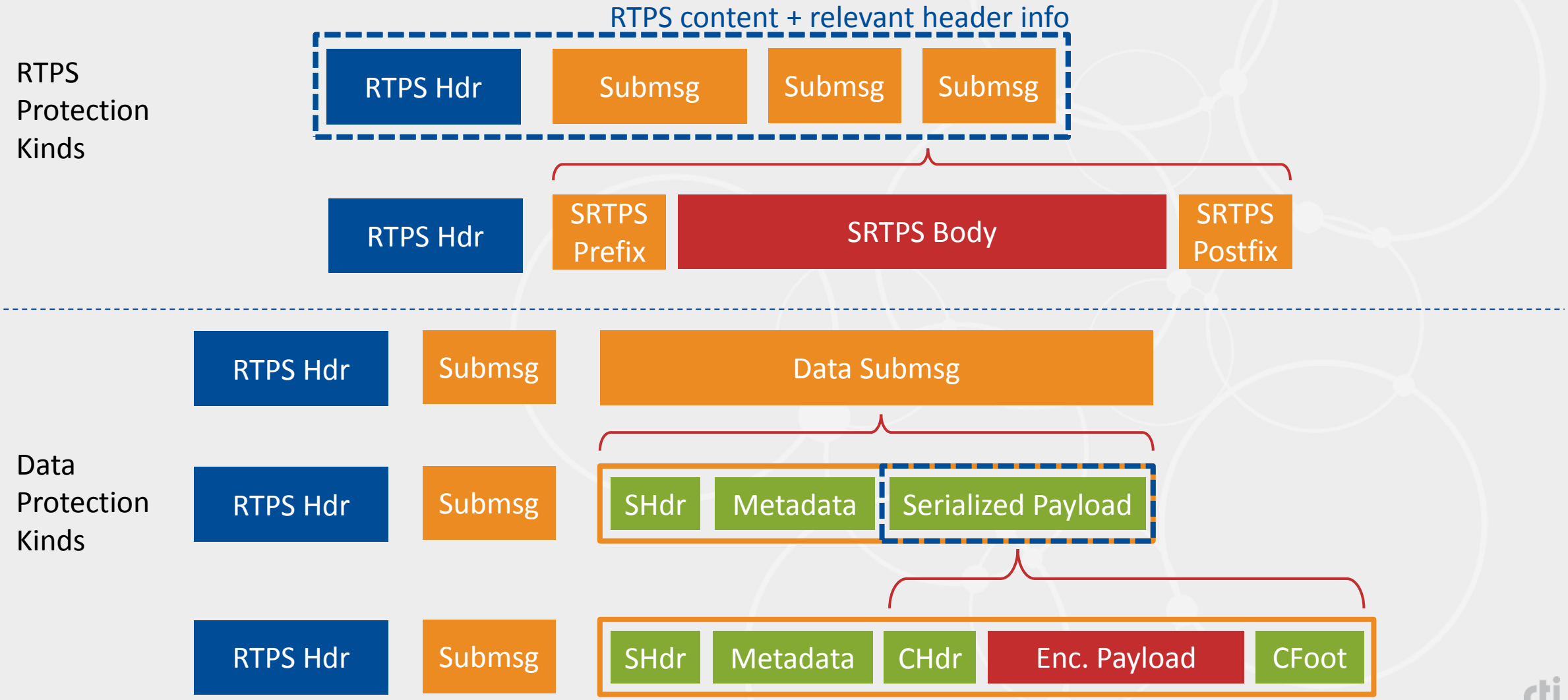


DenySubSquares

Permissions:
Publish: *
Subscribe: Square, Circle

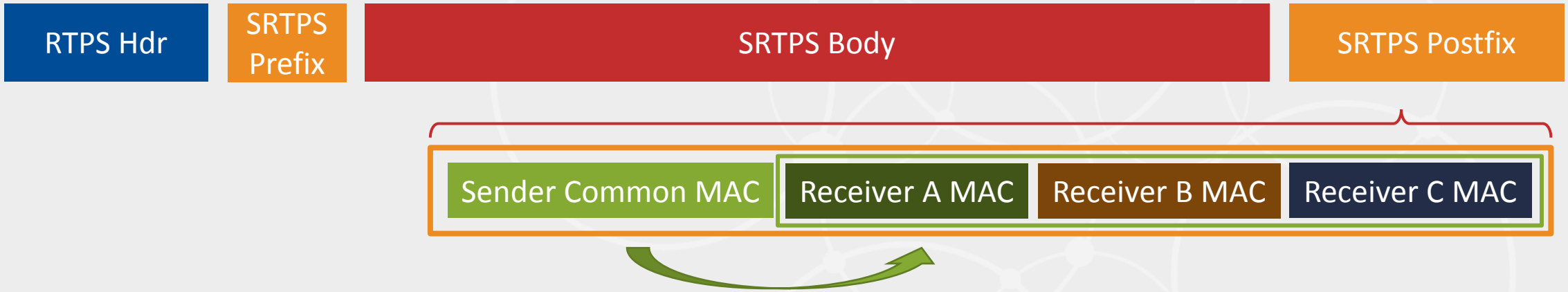
DDS Wire Protocol: Real-Time Publish Subscribe (RTPS)

RTPS & Payload Protection Kinds

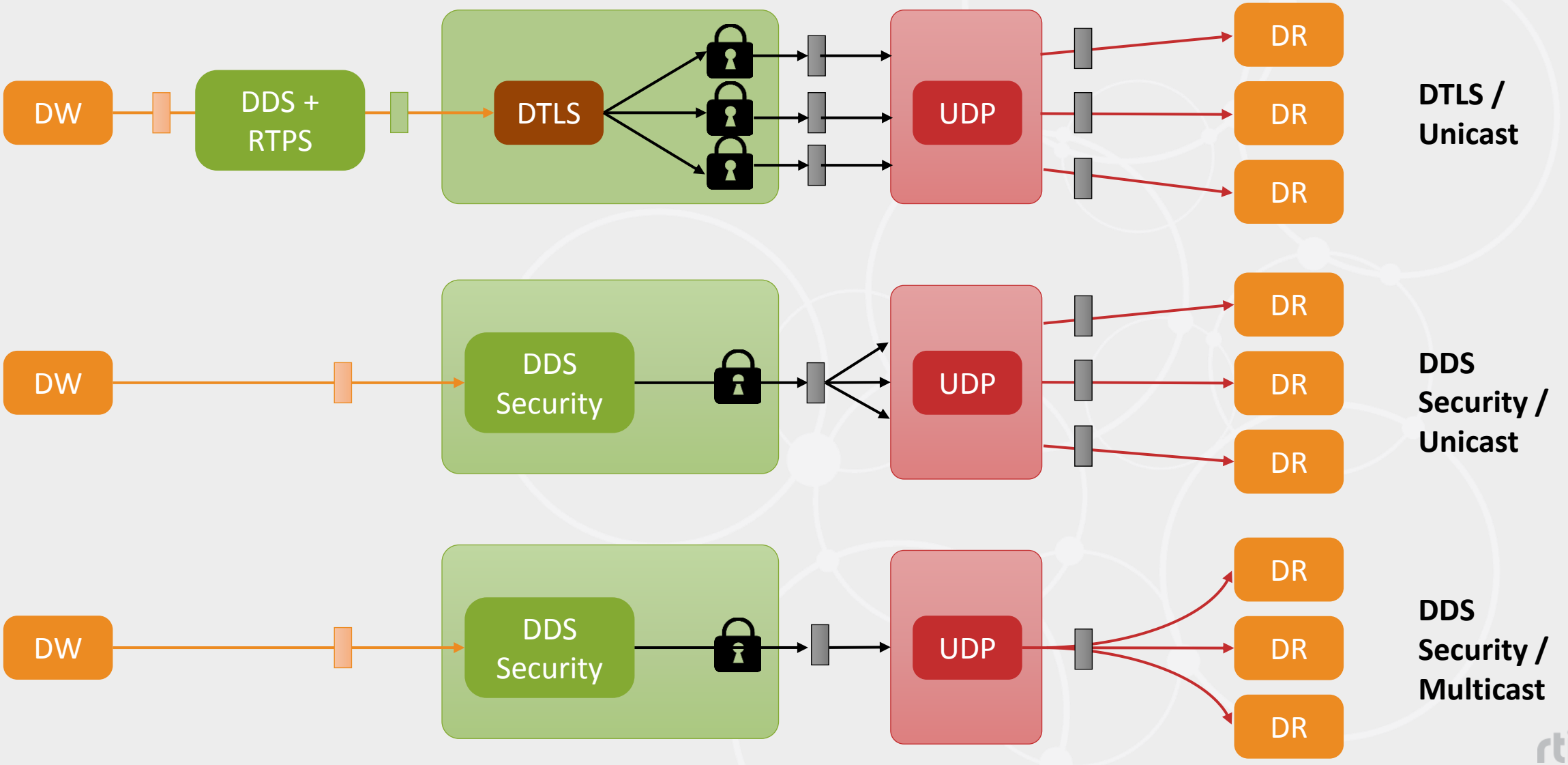


Origin Authentication Protection Kinds

- Enforce Permission to Read vs Write
- Prevent Insider Attacks

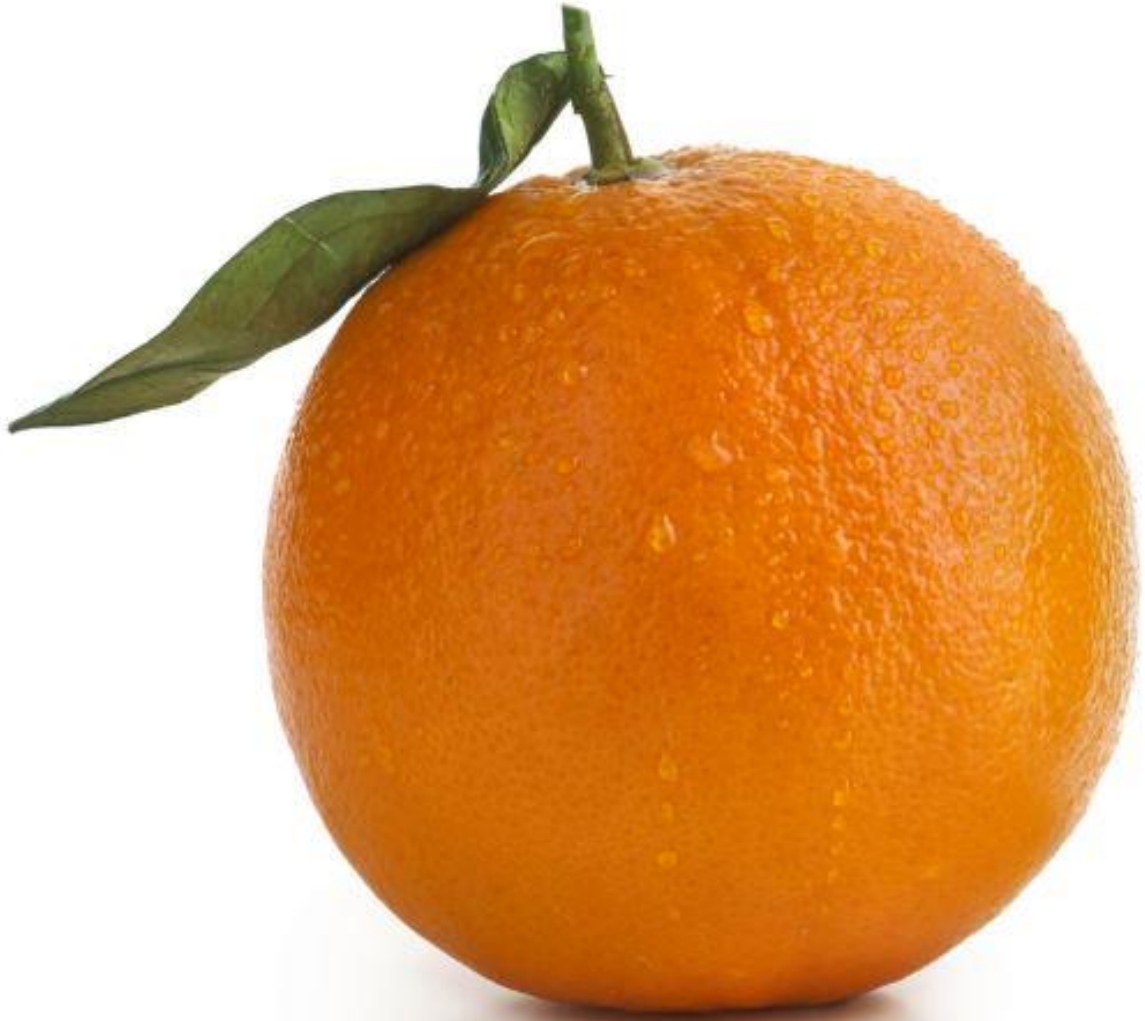


Transport Security (e.g. TLS) vs DDS Security

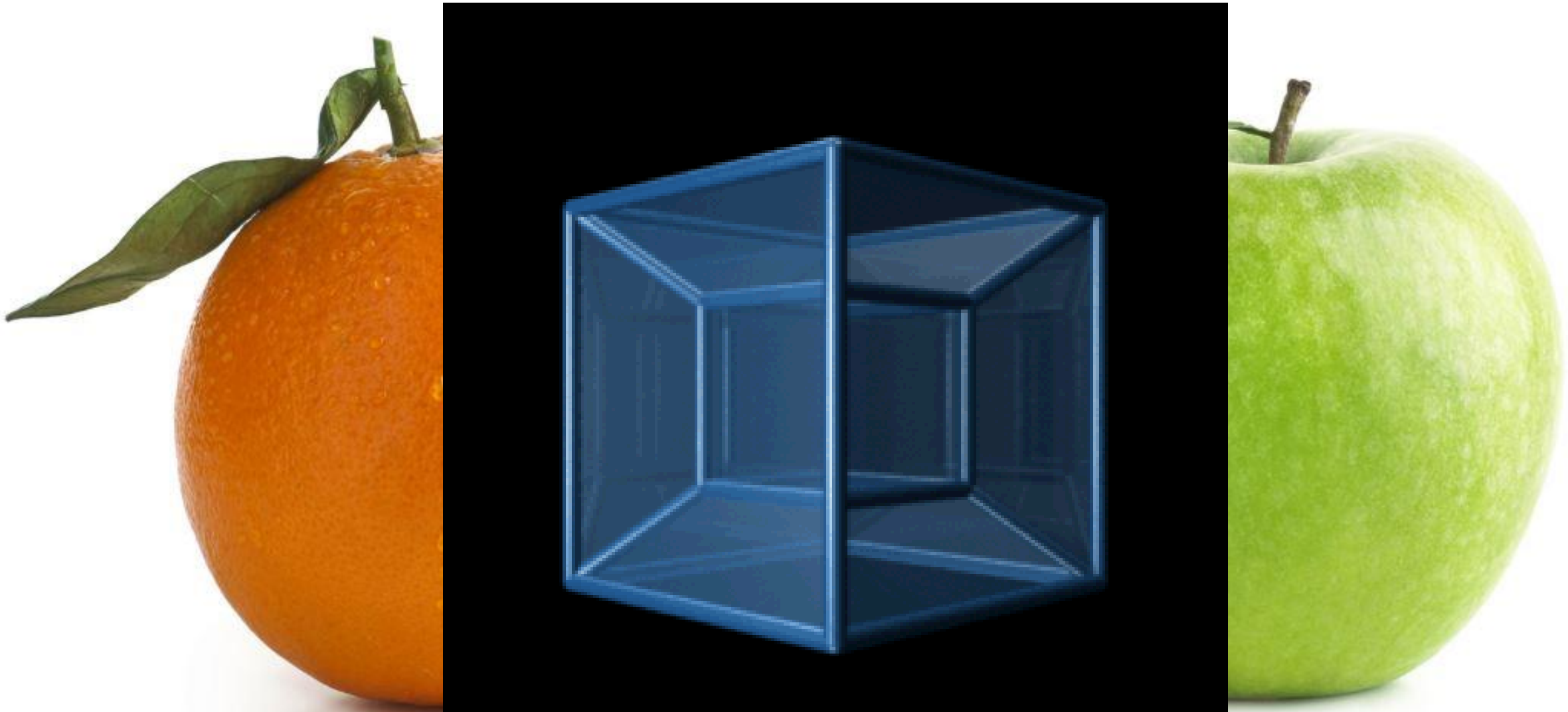


DDS Security Performance

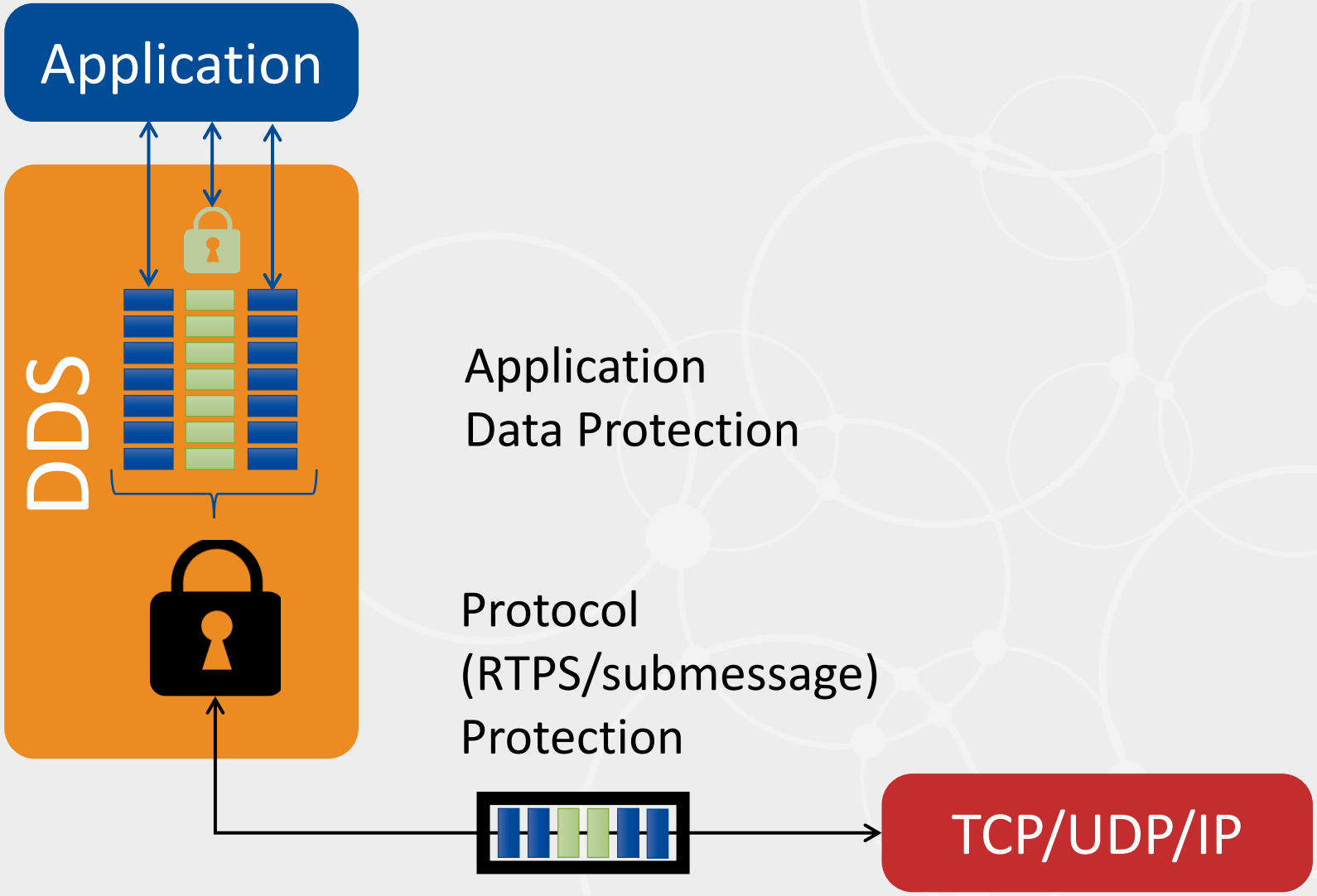
Benchmarking Performance is really hard…



Benchmarking Performance is really hard…
…and multi-dimensional



DDS : How the data is cryptographically protected



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

Takeaways

DDS Security provides excellent support to secure ROS

- DDS is Standard & Interoperable and widely deployed in IIoT
- 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?