OBJECT MANAGEMENT GROUP®

DDS Security Interoperability Demo

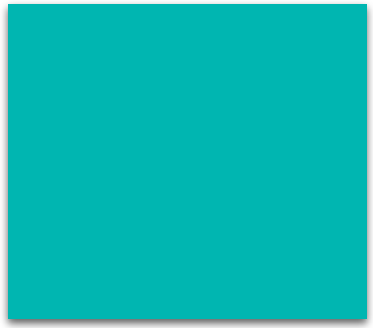
DDS™ – The Proven Data Connectivity Standard for IIoT™

Reston, March 2018

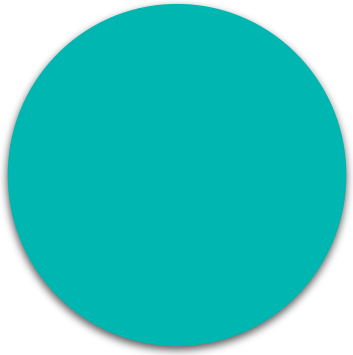
DDS Security Demo — Overview

- 5 Vendor Products:
  - CoreDX DDS from Twin Oaks Computing
  - Connext DDS from Real Time Innovations (RTI)
  - InterComm DDS from Kongsberg
  - Vortex Cafe DDS from ADLink
  - OpenDDS from Object Computing Inc (OCI)
- Using Shapes demo software:
  - Familiar from previous interoperability demos
- Demonstrating granular configurability of DDS Security protocols
  - Each Participant has its own permissions – what exactly it can publish / subscribe
  - Each Topic has its own configuration – encrypted, signed, clear, encrypted discovery

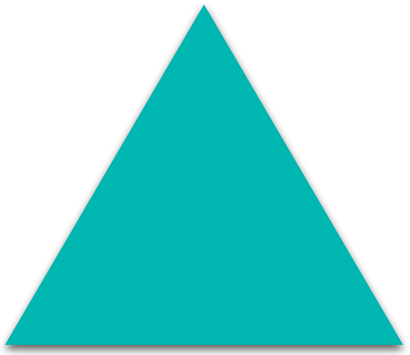
DDS Security Demo — Topics



Square Topic
- Secure Discovery
- Encrypted Data
- Authenticated Metadata
- Protected Access:
  Authenticated Participants must have permissions to publish and/or subscribe

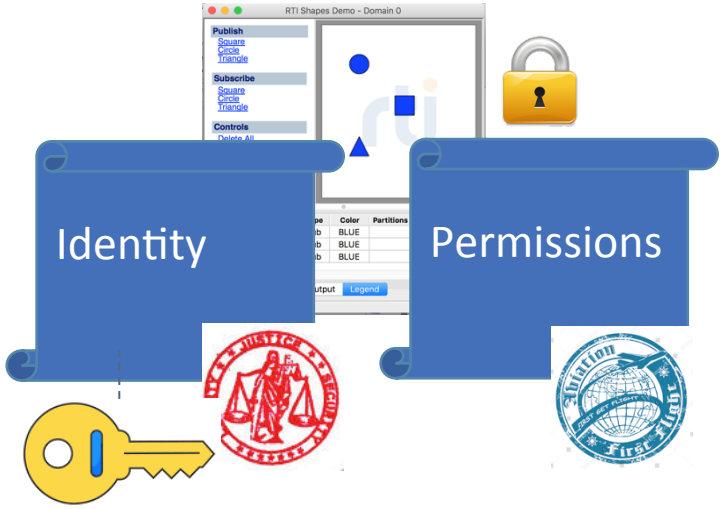


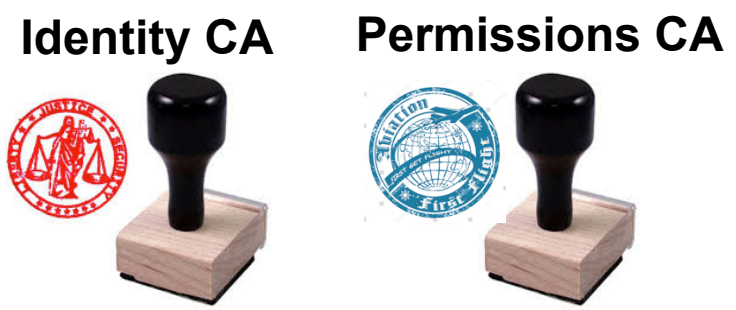
Circle Topic
- Secure Discovery
- Authenticated Data
- Authenticated Metadata
- Protected Access:
  Participants must have permissions to publish and/or subscribe

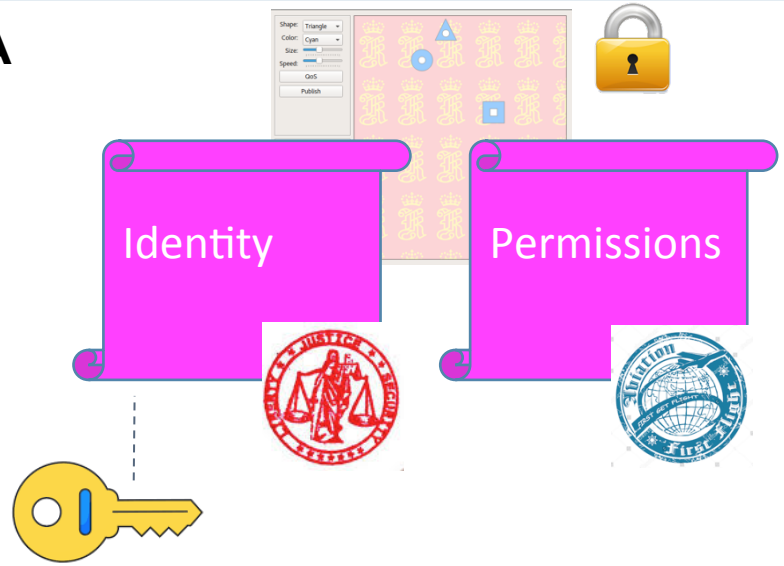


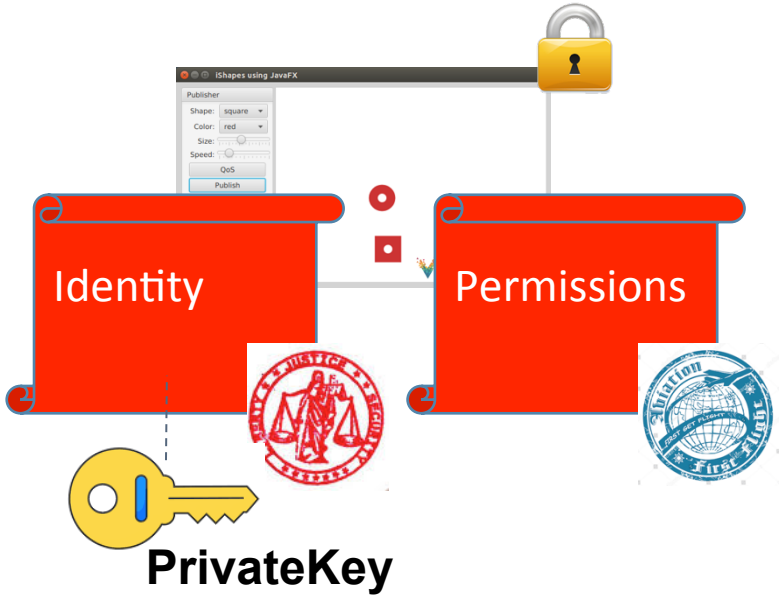
Triangle Topic
- Open Discovery
- Open Data
- Open Access:
  Any participant may publish and/or subscribe

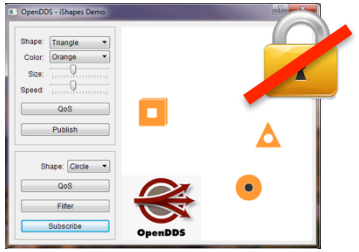
DDS Security Configuration

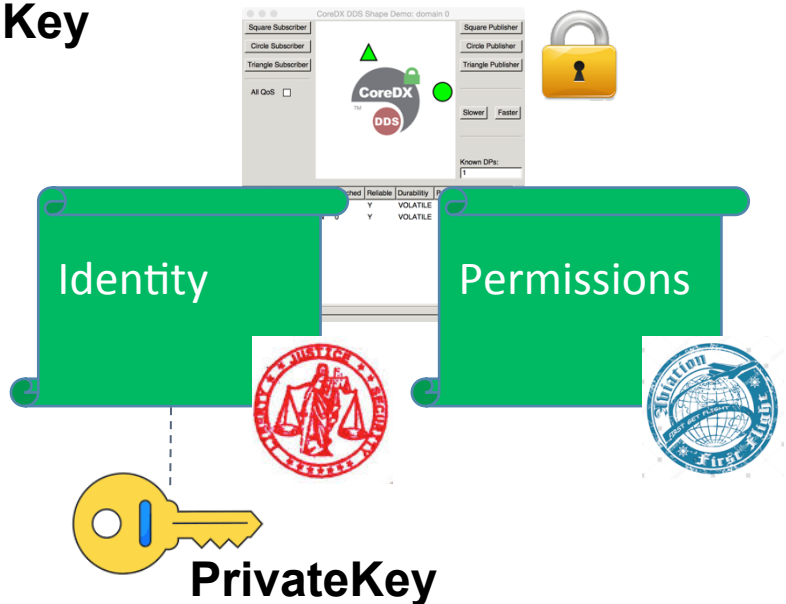




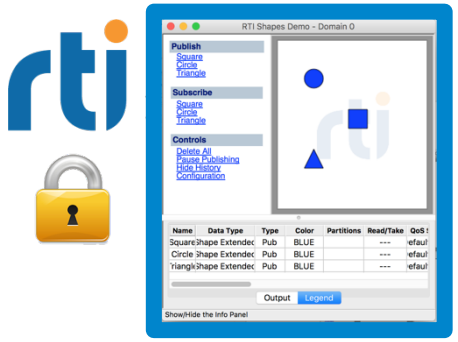






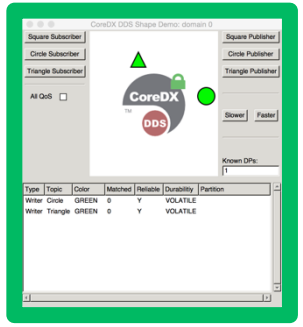


DDS Security Demo — Publishing

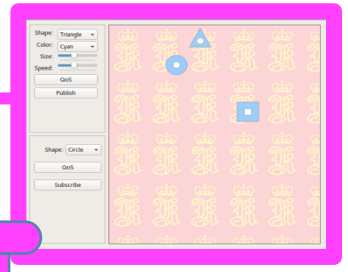


Permissions
- ALLOW Write Square
- DENY Write Circle

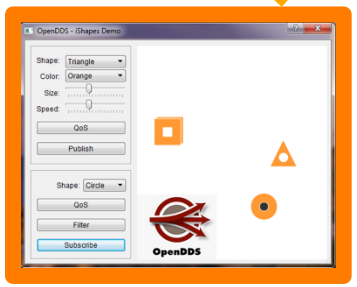
Permissions
- ALLOW Write Circle
- DENY Write Triangle



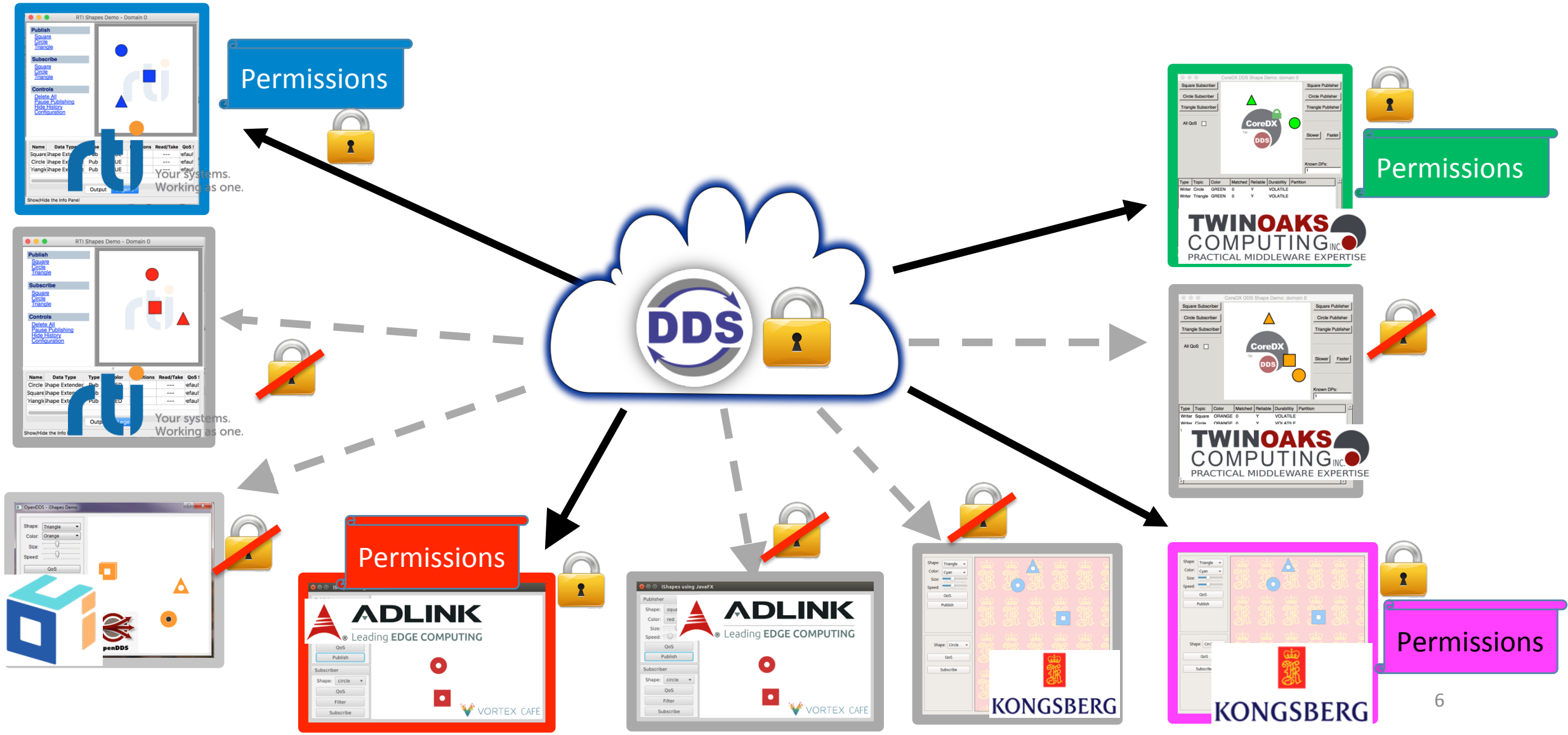
Permissions
- ALLOW Write Triangle
- DENY Write Circle



Permissions
- ALLOW Write Triangle
- DENY Write Square



DDS Security Demo — Subscribing



Demo

- The demo consists of the following scenarios:
  - Interoperability Without Security Enabled (SC#0)
  - **Controlled Access to Domain (SC#1)**
  - Enabling Open Access to Selected Topics (SC#2)
  - **Data Integrity versus Encryption (SC#3)**
  - Metadata protection (SC#4)
  - Secure Discovery (SC#5)
  - **Topic Level Access Control (SC#6)**

SC#0: Interoperability Without Security

- **Objective:** DDS Security is an extension of DDS —still possible to run applications without any protection.
- **Governance File:** Specifies domain 0 as an "open domain". `Governance_SC0_SecurityDisabled.xml`
- **Permission Files:** None are needed for this scenario. `Permissions_JoinDomain_<VENDOR>.xml`
- **Applications:** Regular and Secured and Shapes Demo

Publishing	
RTI SecureShapes **BLUE Square**	OFF
TwinOaks SecureShapes **GREEN Square**	OFF
Kongsberg SecureShapes **MAGENTA Square**	OFF
ADLink RegularShapes **RED Square**	OFF
OCI RegularShapes **ORANGE Square**	

Subscribing to "Square"	*Expected Result*
All (**Secure**) **RTI, TwinOaks, Kongsberg**	Receives All: Square: **BLUE**, **GREEN**, **MAGENTA** , **RED**, **ORANGE** OFF
All (**Not Secure**) **RTI, TwinOaks, Kongsberg**	Receives All: Square: **BLUE**, **GREEN**, **MAGENTA**, **RED**, **ORANGE**

SC#1: Controlled Access to Domain

- **Objective:** DDS Security can be used to protect access to a DDS Domain. Only applications that can authenticate and have the proper permissions can join the Domain.
- **Governance File:** Specifies domain 0 as a "protected domain." `Governance_SC1_ProtectedDomain1.xml`
- **Permission Files:** Each vendor has its own permissions file. `Permissions_JoinDomain_<VENDOR>.xml`.
- **Applications:** Regular and Secured and Shapes Demo

Publishing
RTI **BLUE** **Square**
TwinOaks **GREEN** **Square**
Kongsberg **MAGENTA** **Square**
ADLink **RED** **Square**
OCI **ORANGE** **Square**

DDS

Subscribing to "Square"	*Expected Result*
All (**Secure**) **RTI, TwinOaks, Kongsberg, ADLink**	Receives only from **Secure**: Square: **BLUE**, **GREEN**, **MAGENTA** , **RED**
All (**Not Secure**) **RTI, TwinOaks, Kongsberg, OCI, ADLink**	Receives only from **Non-Secure** Square: **ORANGE**

SC#2: Open Access to Selected Topics

- **Objective:** Illustrates it is possible to allow access to certain Topics by unsecured applications (e.g, for legacy applications not running DDS Security).
- **Governance File:** `Governance_SC2_ProtectedDomain2.xml`
  - Allows unauthenticated participants to join domain 0
  - Square and Circle:
    - Protected for read/write access
    - Encrypt/sign metadata
    - Use secure discovery
  - Triangle
    - Unprotected for read/write access (open to all)
    - No encrypt/sign
    - Use regular (unsecured) discovery
- **Permission Files:** Each vendor has its own permissions file. `Permissions_TopicLevel_<VENDOR>.xml`.
- **Applications:** Regular and Secure and Shapes Demo

Publishing
RTI Write Perm: **Squares** BLUE Square BLUE Circle BLUE Triangle
TwinOaks Write Perm: **Circle** GREEN Square GREEN Circle GREEN Triangle
Kongsberg Write Perm: **Square** MAGENTA Square MAGENTA Circle MAGENTA Triangle
ADLink Write Perm: **Circle** RED Square RED Circle RED Triangle
OCI ORANGE Square ORANGE Circle ORANGE Triangle

DDS

Subscribing **"Square", "Circle", "Triangle"**	*Expected Result Receives:*
RTI (**Secure**) Read Perm: **Circle** + **Triangle**	Square: none Circle: GREEN, RED Triangle: BLUE, GREEN, MAGENTA , RED, ORANGE
Twin Oaks (**Secure**) Read Perm: **Square** + **Triangle**	Square: BLUE, MAGENTA Circle: none Triangle: BLUE, GREEN, MAGENTA, RED, ORANGE
Kongsberg (**Secure**) Read Perm: **Square** + **Circle**	Square: BLUE, MAGENTA Circle: GREEN, RED Triangle: BLUE, GREEN, MAGENTA, RED, ORANGE
ADLink (**Secure**) Read Perm: **Square** + **Circle**	Square: BLUE, MAGENTA , Circle: GREEN, RED Triangle: BLUE, GREEN, MAGENTA , RED, ORANGE
OCI (**Not Secure**)	Square: ORANGE, Circle: ORANGE Triangle: BLUE, GREEN, MAGENTA, RED, ORANGE

SC#3: Data Integrity versus Encryption

- **Objective:** Illustrate different kinds of data protection.
  - **Encrypted (EN+SG)**—(Encrypt and Sign) protected
  - **Signed data (SG)**—vulnerable to snooping but not tampering
  - **Open data (OD)**—vulnerable to tampering
- **Governance File:** Specifies domain 0 as a "protected domain" `Governance_SC3_ProtectedDomain3.xml`
  - Squares shall be encrypted
  - Circles shall be signed
  - Triangles are unprotected
- **Permission Files:** Each vendor has its own permissions file. `Permissions_JoinDomain_<VENDOR>.xml`.
- **Applications:** Secured Shapes Demo + Wireshark

Publishing
RTI **BLUE Square (EN + SG) '#'** **BLUE Circle (SG) '$'** **BLUE Triangle (OD) '%'**
TwinOaks **GREEN Square (EN + SG) '#'** **GREEN Circle (SG) '$'** **GREEN Triangle (OD) '%'**
Kongsberg **MAGENTA Square (EN + SG) '#'** **MAGENTA Circle (SG) '$'** **MAGENTA Triangle (OD) '%'**
ADLink **GREEN Square (EN + SG) '#'** **GREEN Circle (SG) '$'** **RED Triangle (OD) '%'**
OCI (not secure) **ORANGE Triangle '%'**

DDS

Subscribing: Square + Circle + Triangle	***Expected Result***
All (**Secure**) RTI, TwinOaks, Kongsberg, ADLink	Square: **BLUE**, **GREEN**, **MAGENTA**, **RED** Circle: **BLUE**, **GREEN**, **MAGENTA**, **RED** Triangle: **BLUE, GREEN**, **MAGENTA**, **RED**, **ORANGE**
All (**Not Secure**) RTI, TwinOaks, Kongsberg, OCI, ADLink	Square: Circle: Triangle: **BLUE, GREEN**, **MAGENTA**, **RED**, **ORANGE**
Wireshark	Can see Triangle data in the clear Can see Circle data, but it is signed (or OD from OCI) Cannot see Square data—it is encrypted

ShapeSizes:
Square -> 35 '#'
Circle -> 36 '$'
Triangle -> 37 '%'

SC#4: Metadata Protection

- **Objective:** Illustrate concept of protecting metadata.
  - **Encrypted (EN+SG)**—Encrypt and Signed metadata protected
  - **Signed metadata (SG)**—vulnerable to snooping but not tampering
  - **Open metadata (OD)**—vulnerable to tampering
- **Governance File:** Specifies domain 0 as a "protected domain" `Governance_SC4_ProtectedDomain4.xml`
  - Square metadata shall be encrypted
  - Circle metadata shall be signed,
  - **Triangle metadata is unprotected**
  - Payload is left open for all topics for illustration
- **Permission Files:** Each vendor has its own permissions file. `Permissions_JoinDomain_<VENDOR>.xml`.

Publishing
RTI **BLUE Square (EN + SG) '#'** **BLUE Circle (SG) '$'** **BLUE Triangle (OD) '%'**
TwinOaks **GREEN Square (EN + SG) '#'** **GREEN Circle (SG) '$'** **GREEN Triangle (OD) '%'**
Kongsberg **MAGENTA Square (EN+SG) '#'** **MAGENTA Circle (SG) '$'** **MAGENTA Triangle (OD) '%'**
ADLink **RED Square (EN + SG) '#'** **RED Circle (SG) '$'** **RED Triangle (OD) '%'**
OCI (not secure) **ORANGE Triangle '%'**

DDS

Subscribing	*Expected Result*
All (**Secure**) RTI, TwinOaks, Kongsberg, ADLink	Square: **BLUE**, **GREEN**, **MAGENTA**, **RED** Circle: **BLUE**, **GREEN**, **MAGENTA**, **RED** Triangle: **BLUE**, **GREEN**, **MAGENTA**, **RED**, **ORANGE**
All (**Not Secure**) RTI, TwinOaks, Kongsberg, ADLink, OCI	Square: Circle: Triangle: **BLUE**, **GREEN**, **MAGENTA**, **RED**, **ORANGE**
Wireshark	Can see Triangle metadata & data Can see Circle metadata, but it is signed Cannot see Square metadata—it is encrypted

ShapeSizes:
Square -> 35 '#'
Circle -> 36 '$'
Triangle -> 37 '%'

Also peek at Discovery – It is all clear

SC#5: Secure Discovery

- **Objective:** Illustrates that discovery information also be protected.
- **Governance File:** Specifies domain 0 as a "protected domain." `Governance_SC5_ProtectedDomain5.xml`
  - Topic Triangle data and metadata **are neither encrypted nor signed**—sent over regular discovery
  - Topic Circle data and metadata are **signed**, but not encrypted—sent over secure discovery
  - Topic Square data and metadata are **encrypted** and signed—sent over secure discovery
- **Permission Files:** Each vendor has its own permissions file. `Permissions_JoinDomain_<VENDOR>.xml`.
- **Applications:** Secure Shapes Demo

Publishing
RTI **BLUE Square (EN + SG)** **BLUE Circle (SG)** **BLUE Triangle (OD)**
TwinOaks **GREEN Square (EN + SG)** **GREEN Circle (SG)** **GREEN Triangle (OD)**
Kongsberg **MAGENTA Square (EN+SG)** **MAGENTA Circle (SG)** **MAGENTA Triangle (OD)**
ADLink **RED Square (EN + SG)** **RED Circle (SG)** **RED Triangle (OD)**
OCI **ORANGE Triangle (OD)**

DDS

Subscribing	*Expected Result*
Square + Circle + Triangle	
All (**Secure**) **RTI, TwinOaks, Kongsberg**	Square: **BLUE**, **GREEN**, **MAGENTA**, **RED** Circle: **BLUE**, **GREEN**, **MAGENTA**, **RED** Triangle: **BLUE**, **GREEN**, **MAGENTA** , **RED**, **ORANGE**
All (**Not Secure**) **RTI, TwinOaks, Kongsberg, OCI, ADLink**	Square: Circle: Triangle: **BLUE**, **GREEN**, **MAGENTA**, **RED**, **ORANGE**
Wireshark	Can see Triangle discovery in the clear Cannot see Circle discovery Cannot see Square discovery

SC#6: Topic-Level Access Control

- **Objective:** Illustrates fine-grain access control at the Topic level.
- **Governance File:** Specifies domain 0 as a "protected domain." Indicates that Square
  - All topics are **protected for read/write access**.
  - All topics are sent over **secure discovery**
  - All topics **encrypt and sign** metadata
  - `Governance_SC6_ProtectedDomain6.xml`

- **Permission Files:** Each vendor has its own permissions file. `Permissions_TopicLevel_<VENDOR>.xml`.
- **Applications:** Secure Shapes Demo

Publishing	*Subscribing*	*Expected Result*
RTI Write Perm: **Squares** **BLUE Square** **BLUE Circle** **BLUE Triangle**	RTI Read Perm: **Circle + Triangle** Subscribes: **Square, Circle, Triangle**	Receives: Square: none Circle: **GREEN, RED** Triangle: none
TwinOaks Write Perm: **Circle** **GREEN Square** **GREEN Circle** **GREEN Triangle**	Twin Oaks Read Perm: **Square+Triangle** Subscribes: **Square, Circle, Triangle**	Receives: Square: **BLUE, MAGENTA** Circle: none Triangle: none
Kongsberg Write Perm: **Square** **MAGENTA Square** **MAGENTA Circle** **MAGENTA Triangle**	Kongsberg Read Perm: **Square + Circle** Subscribes: **Square, Circle, Triangle**	Receives: Square: **BLUE** Circle: **GREEN, RED** Triangle: none
ADLink Write Perm: **Circle** **RED Square** **RED Circle** **RED Triangle**	ADLink Read Perm: **Square + Circle** Subscribes: **Square, Circle, Triangle**	Receives: Square: **BLUE, MAGENTA** Circle: **GREEN, RED** Triangle: none
OCI (**Not Secure**) **ORANGE Triangle**	OCI (**Not Secure**)	Triangle: **ORANGE**

More powerful that other secure middleware technologies

- **Standard & Interoperable**
- **Scalable**: Supports multicast
- **Fine-grain**: Control at the Topic-level
- **Flexible**: Build your own plugins
- **Generic**: Works over any Transport
- **Transparent**: No changes to Application Code!

Questions?

TWINOAKS COMPUTING INC.
PRACTICAL MIDDLEWARE EXPERTISE

rti
Your systems.
Working as one.

KONGSBERG

OCI | WE ARE SOFTWARE ENGINEERS.

ADLINK
Leading EDGE COMPUTING