COALFIRE RAMPCON

06.09 — 06.10.2025 • WASHINGTON D.C.

Container Encryption:

FIPS Validated and compliant encryption for cloud native workloads

Jason Macallister | Senior Manager | Coalfire
Merle Infanger | Technical Senior Manager | Coalfire


Cloud service providers seeking FedRAMP authorization must implement and enforce FIPS validated cryptography for containerized workloads.

Agenda

1. Describe the requirements for FIPS validated data-in-transit encryption for containerized workloads
2. Identify the challenge for implementing implementing data-in-transit encryption for containerized workloads
3. Determine what AWS, GCP, and Azure provide to assist with this challenge
4. Propose options to address remaining FedRAMP cloud service provider responsibilities for data in-transit encryption

What the FedRAMP Baseline Says

- The cloud service provider must protect the integrity and confidentiality of transmitted information.
- The method for protecting the confidentiality of transmitted information is through encryption.
- Where encryption occurs, Federal Information Processing Standards (FIPS) validated or National Security Agency (NSA) approved cryptography must be used.
- Encryption for data-at-rest and data-in-transit is a federal mandate.
- When leveraging encryption from underlying FedRAMP authorized IaaS/PaaS providers, CSPs must understand their responsibility for encryption.

How This Applies to Containers

From SC-8, Additional FedRAMP Requirements and Guidance:

"For clarity, this control applies to **all** data in transit. Examples include the following data flows:
- Crossing the system boundary
- Between compute instances - **including containers**
- From a compute instance to storage
- Replication between availability zones
- Transmission of backups to storage
- From a load balancer to a compute instance
- Flows from management tools required for their work – e.g., log collection, scanning, etc."

From FedRAMP vulnerability scanning requirements version 2.0 2/15/2024:

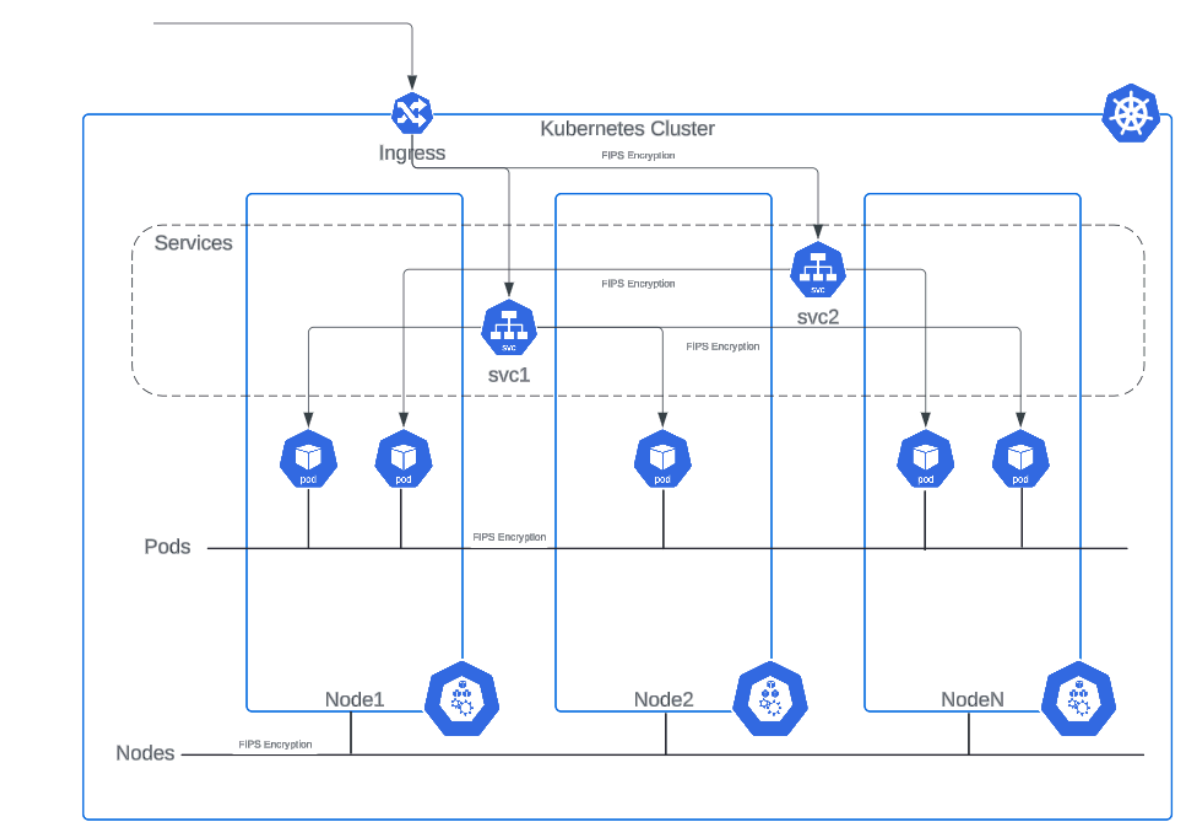
"FedRAMP considers any data in transit, whether that be from one container to another container, from a container to a sidecar inside the same host virtual machine, or from a container to any other source outside that container, that SC-8 controls must be applied to this data in transit. SC-8 protection (usually encryption) is required when data is in transit from one memory processing space to another."

Recent Clarifying FedRAMP Guidance and Insights

Container to container data-in-transit encryption includes:

- From container to container – including on the same host (worker node)
- From container to container – including within the same pod where more than one containers exists within a pod*
- From container to sidecar – including on the same host*
- From container to any other source outside the container
- Data in transit from one memory processing space to another*

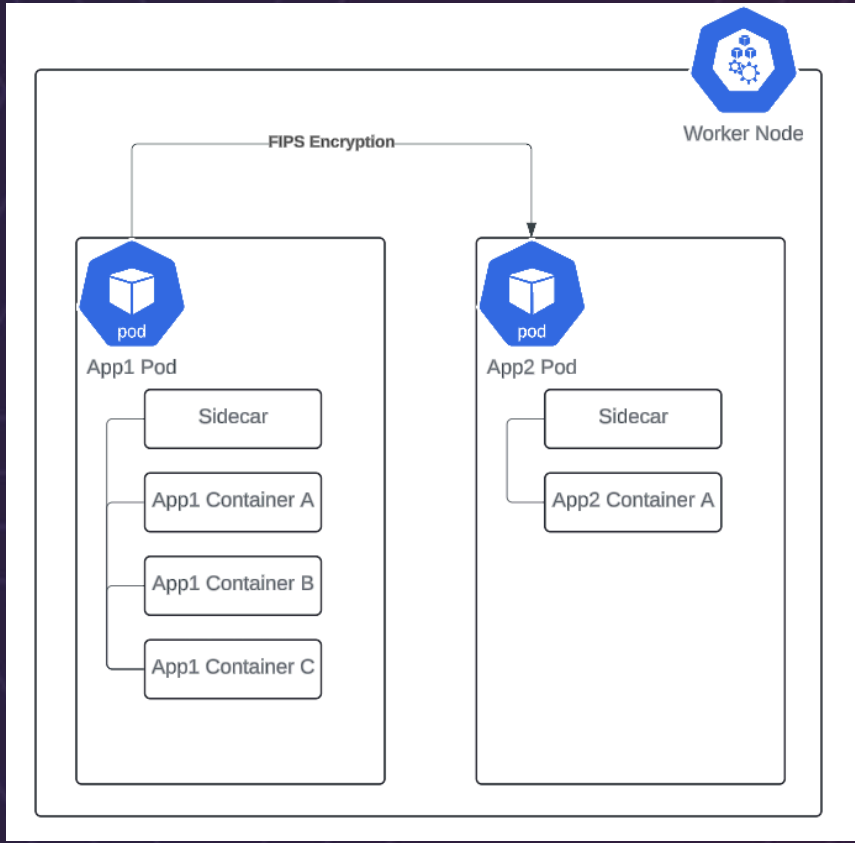
Kubernetes Workload Communication Model



Agenda Topic title:

JASON MACALLISTER | MERLE INFANGER

Kubernetes Pod Construct



Agenda Topic title:

JASON MACALLISTER | MERLE INFANGER

FIPS encryption can be challenging

- FIPS by itself isn't easy, and it can lead to many application-level concerns.
- Can you as a prospective seller to the US Government ensure that your control plane, your images, and your data in transit are fully FIPS compliant using FIPS validated modules?
- Meeting FIPS isn’t easy when you do it yourself, thankfully Cloud Providers like AWS, Azure, and GCP do take some (not all) of the load off.
- There are other technologies or approaches beyond what underlying IaaS/PaaS providers offer that can bridge the gap to full compliance.

What to Know Relative to These Requirements

- **What can be inherited from the IaaS/PaaS provider?**
  - Inheritance from AWS, GCP, and Azure for EKS, GKE, and AKS respectively
- **After the IaaS/PaaS provider what remaining customer responsibility exists?**
  - Container network intra-node, intra-cluster, intra-pod
  - Cluster node configuration where applicable
  - Container network traffic coming into services within the cluster and leaving the cluster
- **What options exist to facilitate meeting the remaining customer responsibilities?**
  - ChainGuard - FIPS at the container
  - ServiceMesh – FIPS for overlay network on which containers reside
  - Refactor Application – Refactoring application architecture to account for FIPS encryption requirements for data-at-rest, data-in-transit, other cryptographic functions.

What Can Be Inherited from Amazon Web Services

Let's talk EKS responsibilities

- **You receive a control plane managed by AWS what does this do for you?**
  - You have automated etcd backups of all your configurations
  - You have management endpoints capable of FIPS
  - Your high availability options can be managed through ASGs
- **You receive a control plane managed by AWS what doesn't this do for you?**
  - Node images don't come with FIPS out of the box
  - Node images don't come with CIS/STIG hardening out of the box
  - Encryption in transit is on you
  - You can leverage KMS to encrypt root EBS volumes and other data stores
  - IAM role mappings are on you to manage

What Can Be Inherited from Google Cloud Platform

Let's talk GKE responsibilities

- **You receive a control plane managed by Google what does this do for you?**
  - You have automated etcd backups of all your configurations
  - You have management endpoints capable of FIPS
  - Your high availability options can be managed through managed node groups
  - GKE claims full responsibility for nodes (cos_containerd, recommended)
  - GKE provides inheritable encryption for data in transit between nodes and between control plane and nodes
- **You receive a control plane managed by Google what doesn't this do for you?**
  - Encryption in transit is on you
  - Cluster nodes cannot be configured for FIPS, Google performs encryption with the underlying network
  - Cluster role mappings are on you to maintain

What Can Be Inherited from Azure

Let's talk AKS responsibilities

- **You receive a control plane managed by Microsoft what does this do for you?**
  - You have automated etcd backups of all your configurations
  - You have management endpoints capable of FIPS

- **You receive a control plane managed by Microsoft what doesn't this do for you?**
  - Node images don't come with FIPS out of the box
  - Node images don't come with CIS/STIG hardening out of the box
  - Encryption in transit is on you
  - You can leverage Cloud Native encryption to encrypt root volumes and other data stores
  - User permission mappings are on you to manage

Solutions for What Remains

Agenda Topic title:

JASON MACALLISTER | MERLE INFANGER

COALFIRE RAMPCON
06.09 — 06.10.2025 • WASHINGTON D.C.

Chainguard for Solving for FIPS

Let's start with what Chainguard really is? Base containers to save your day!

- A solution starting at the image level
- You don't need to roll your own encryption solution into your applications
- A claimed "0 CVE Environment"
- Built in Image Signing to meet further requirements of development
- Base encryption leveraged from OpenSSL 3.0.8 for FIPS 140-2
- Active development of OpenSSL 3.1 bases for FIPS 140-3

Chainguard. Where The Challenge Starts.

How may it fall short?

- A FIPS Compliant base image might not mean all encryption in transit is truly FIPS.
- What if your base runtime is missing?

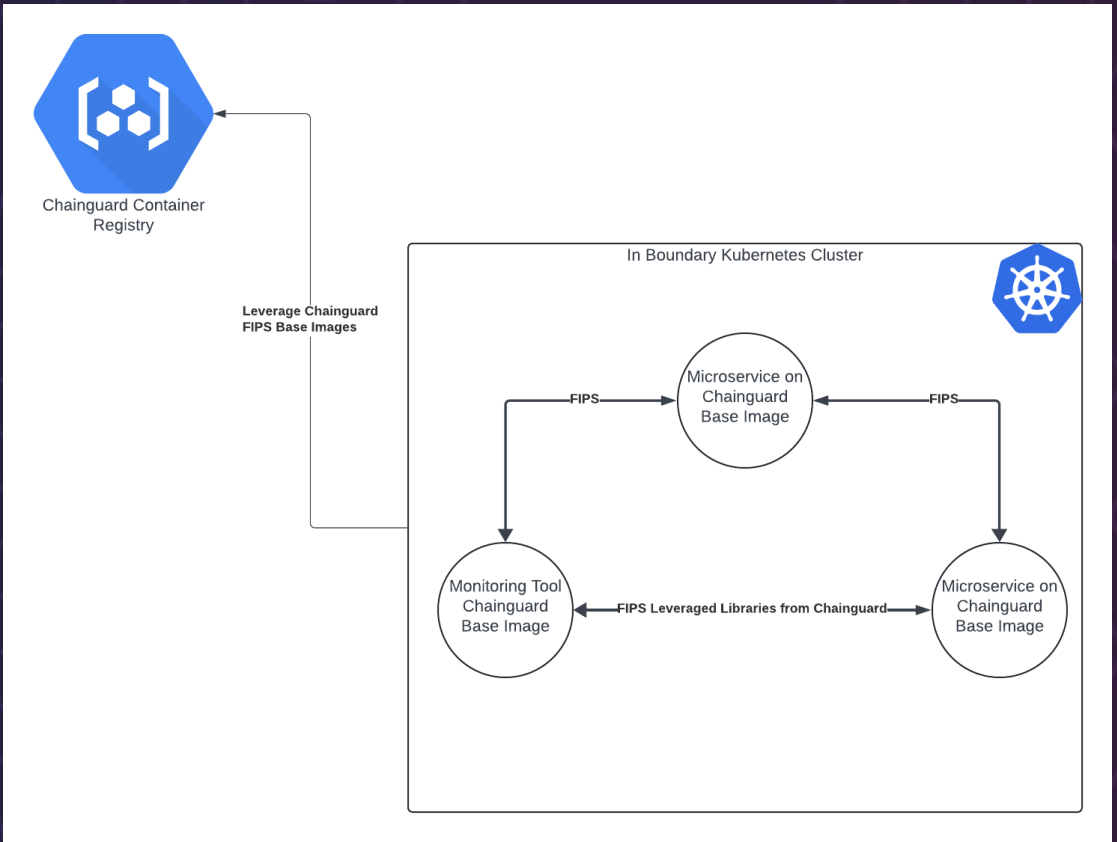
Technical implementation?

- Migrating your base containers can be a headache!

Difficulty

- Unless you're adopting Chainguard everywhere this can cause development divergence.

What Does This Look Like



Agenda Topic title:

JASON MACALLISTER | MERLE INFANGER

Service Mesh: What, Why, How

What are our Service Mesh Options

- Anthos (GCP), AppMesh (AWS), Istio for AKS (Azure), Buoyant, Tetrate
- These options are common pattern solutions seen by Coalfire for ATO and the "Native" solutions provided by our Big Three of Cloud

Why it qualifies

- As of time of writing FIPS remains our biggest challenge for all things FedRAMP. It probably always will be!
- Sidecar based mTLS encryption is leveraged with FIPS validated cryptography. Meaning that all of you inter-node encryption will meet Federal mandates!

How do I adopt this approach?

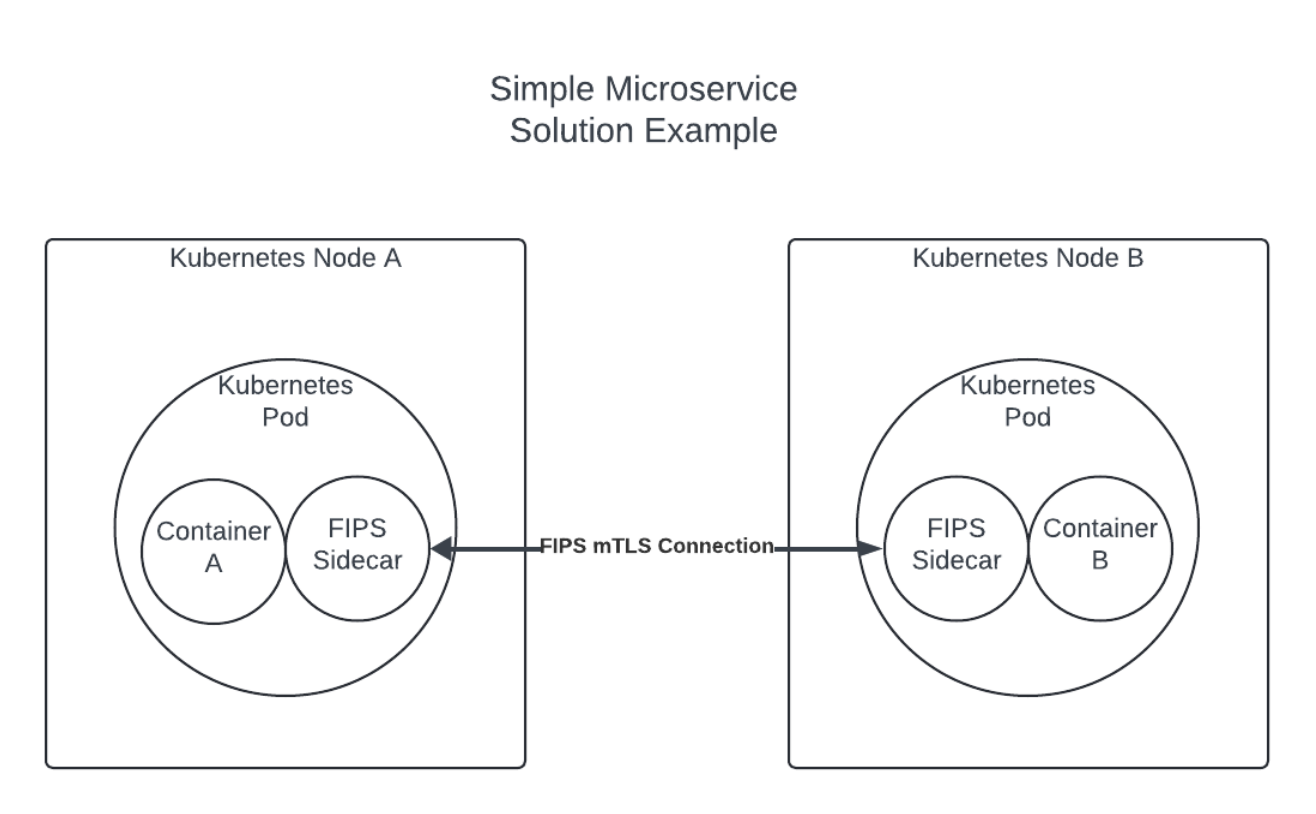
- Are you already using LinkerD or Istio? This is a great time to consider Buoyant or Tetrate for everyone's favorite thing, responsibility offload.
- Do you need to ensure FIPS in your Kubernetes application and you don't know where to start? A service mesh may be the easiest way to batten down the hatches.

Service Mesh: Why Not

- Service Mesh has recently been brought into question as a result of March 16 2024 https://www.fedramp.gov/assets/resources/documents/Vulnerability_Scanning_Requirements_for_Containers.pdf
- Implementation is the name of the game. Is a service mesh right for you?
- Do you leverage the other uses of a Service Mesh?
  - Service Discovery
  - Load Balancing
  - Traffic Management & Splitting
  - Request Mirroring
  - Monitoring
  - Security – You guessed, FIPS mTLS here

Are you already using a service mesh? If so this is a great approach forward. Do you need a fast path to FIPS mTLS? A service mesh *might* be right for you!

What Does This Look Like



Refactor Applications for FIPS

What this means?

- Well you can do it all! But that's an uphill battle.
- This means building your images on your own FIPS base image.
- This means ensuring your network exposed services leverage FIPS 140-2/140-3

Why it qualifies

- If you're building it yourself you can ensure FIPS is everywhere!
- You can ensure that services only employ FIPS encryption to communicate
- You maintain full control of your software development processes and images from the ground up!

JASON MACALLISTER | MERLE INFANGER

Refactor Applications for FIPS

Challenges with this option:

- Maintaining this approach with consistency
- Higher development effort
- Development pipelines checking for FIPS

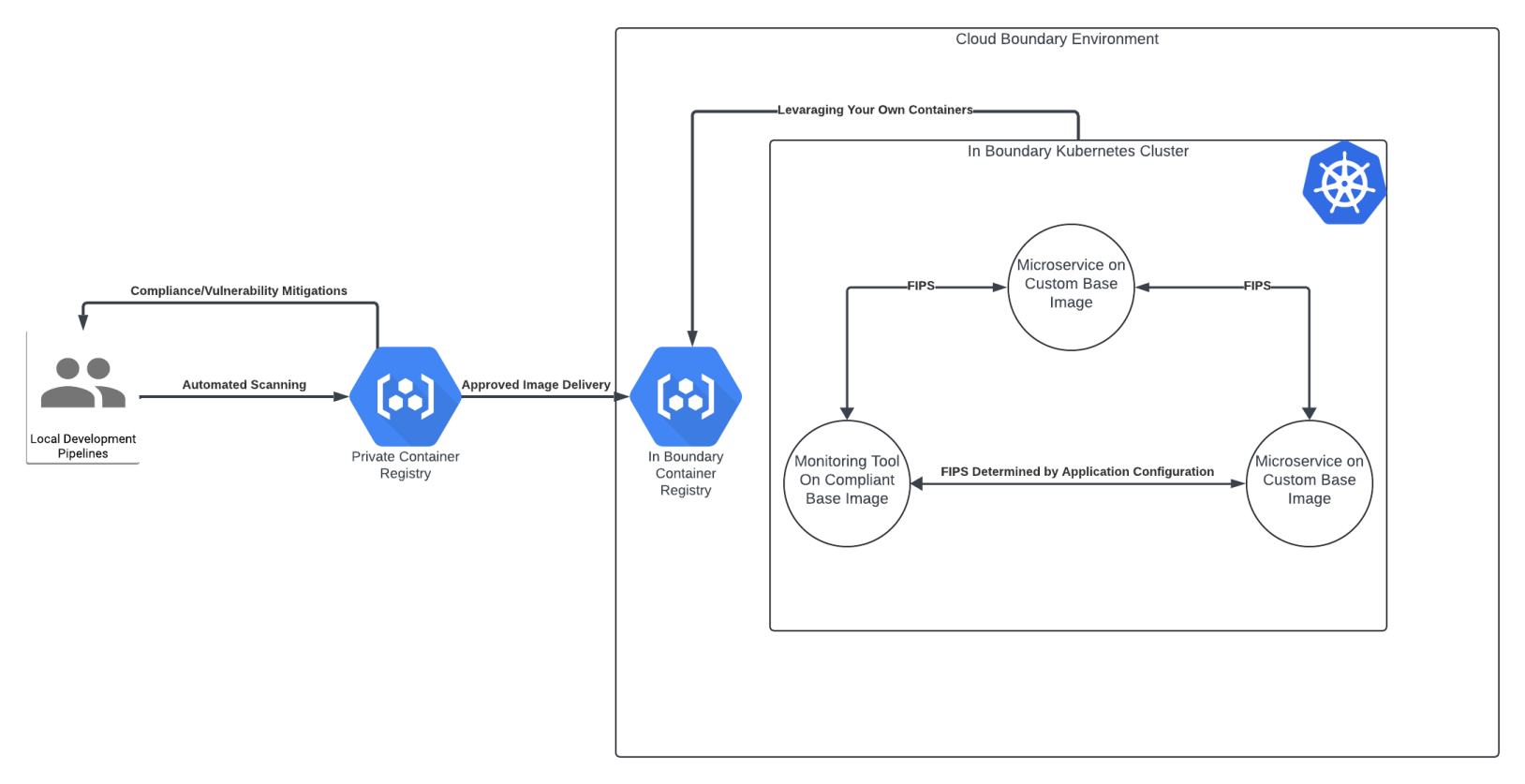
Why it may fall short

- Vendor supplied container images that are not alterable

Other Considerations

- Providing evidence that applications is using proper cryptographic libraries and providers for application-initiated data-in-transit communications

Application Layer Encryption Enforcement



Agenda Topic title:

JASON MACALLISTER | MERLE INFANGER

What is the correct answer for your workloads to address the FedRAMP FIPS requirements?

Agenda Topic title:

JASON MACALLISTER | MERLE INFANGER