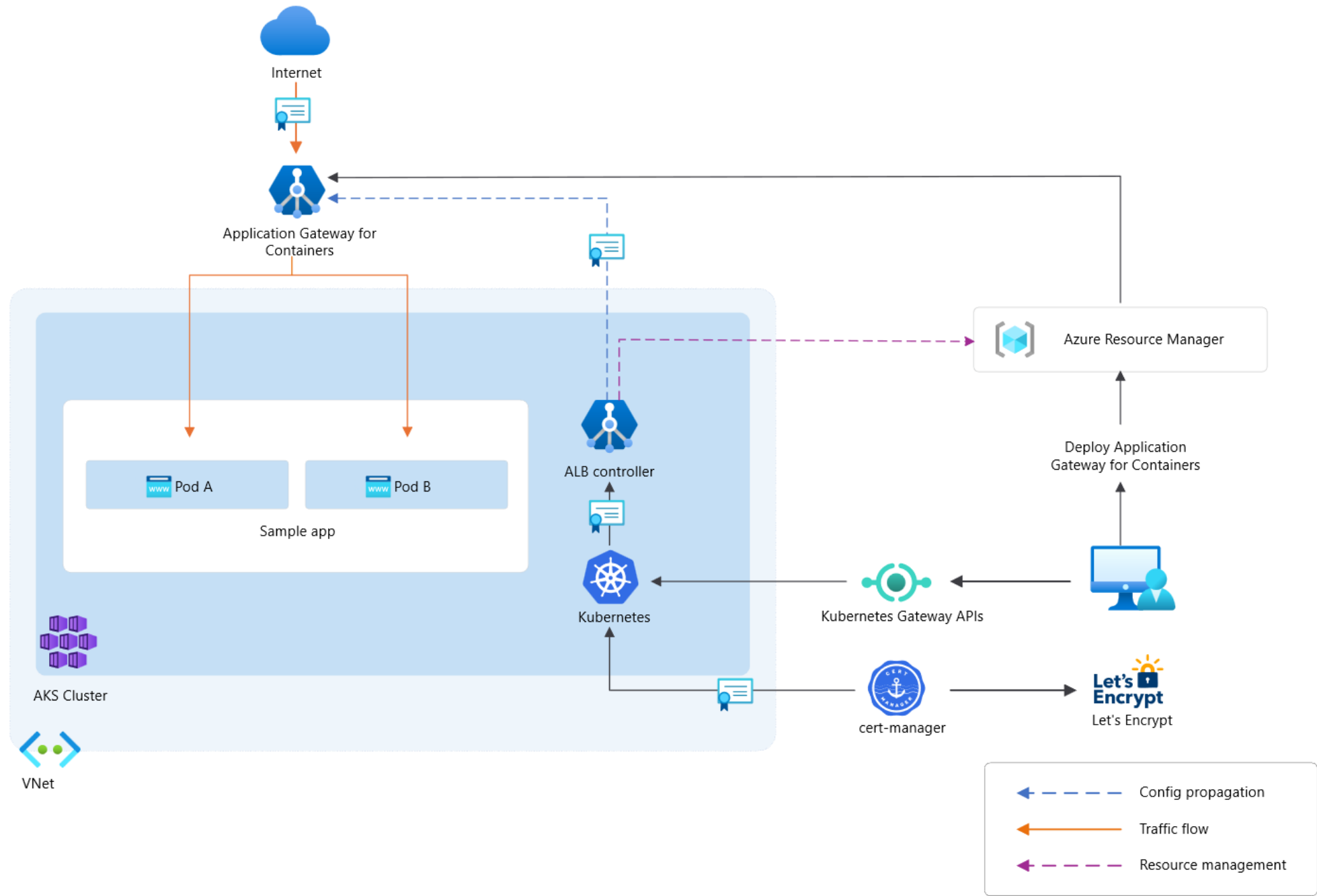# Cert-Manager Azure DNS Wildcard Certificates

Agenda

1. Certificate Management
2. Certificate Validation Approaches
3. HTTP-01 Challenge
4. DNS-01 Challenge
5. Demo

Internet

Application Gateway for Containers

Azure Resource Manager

ALB controller

Deploy Application Gateway for Containers

Pod A   Pod B

Sample app

Kubernetes

Kubernetes Gateway APIs

AKS Cluster

VNet

cert-manager

Let's Encrypt

Let's Encrypt

Config propagation

Traffic flow

Resource management

Certification Management

Cluster Issuer uses Cert-Manager to get a TLS certificate

Cert-Manager uses Certificate Authority (CA)

Certificates are automatically renewed

Certificate Validation Approaches

Let's Encrypt uses ACME (Automated Certificate Management Environment)

HTTP-01Challenge

DNS-01 Challenge

HTTP-01 Challenge

Only supported for specific domains

Cert-Manager places a specific file at a well-known URL

Let's Encrypt makes a HTTP request to verify the file

Does not work for wildcard certificates

DNS-01 Challenge

Cert-Manager creates TXT record in DNS

- Configure authentication
- AKS uses Entra Workload Identity

Let's Encrypt queries the DNS to find the record

Must be used for wildcard certificates

Wildcard Certificates

Create wildcard certificate

Attach it to HTTPS listener

Re-use certificate whenever necessary

Deploy Pull Requests and use wildcard certificate

Demo