

# Using ECC Workload Certificates

(pilot-agent environmental variables)

Jacob Delgado / Aspen Mesh



#IstioCon

# ECC workload certificates

- In various environments, the need for x509 certificates that use Elliptical Curve Cryptography (ECC) is a requirement
- In Istio 1.6, support for workloads to use ECC certificates for mTLS in sidecar-to-sidecar communication was added
  - As of Istio 1.7.7+, 1.8.2+ and 1.9.0+ there is no longer the restriction that a [plugged in CA certificate](#) must use ECC cryptography (using ECDSA P-256) to use this feature
- Only [ECDSA](#) P-256 is supported



# pilot-agent environmental variables

*Disclaimer: Environmental variables and their use are considered experimental. There is no guarantee that they will not be deprecated in a future release. Use at your own discretion.*

- To enable this, users must set the **ECC\_SIGNATURE\_ALGORITHM** environmental variable on sidecar ejection to **ECDSA** for use by **pilot-agent**
  - For **gateways** this environmental variable also must be set on installation/upgrade



# istioctl

## iop.yaml

```
apiVersion: install.istio.io/v1alpha1
kind: IstioOperator
spec:
  meshConfig:
    defaultConfig:
      proxyMetadata:
        ECC_SIGNATURE_ALGORITHM: ECDSA
```

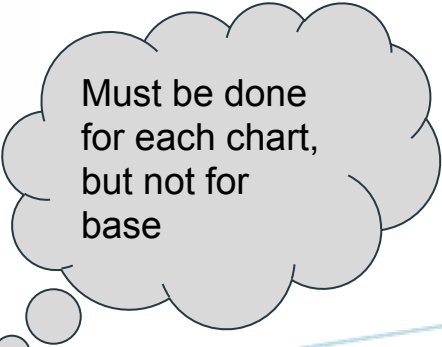
Install with **istioctl install -f iop.yaml**



# helm

- values-overrides.yaml

```
meshConfig:  
  defaultConfig:  
    proxyMetadata:  
      ECC_SIGNATURE_ALGORITHM: ECDSA
```



Must be done  
for each chart,  
but not for  
base

## Install using

```
helm install istiod manifests/charts/istio-control/istio-discovery \  
-n istio-system --values values-overrides.yaml
```

#IstioCon



# Inspection of Workload Certificates

Ensure that workloads within your cluster are using ECC

```
$ istioctl proxy-config secret <POD>.<PODNAMESPACE> -o json | \
jq'.dynamicActiveSecrets[0].secret.tlsCertificate.certificateChain.inlineBytes' | \
sed 's/"//g' | base64 --decode | openssl x509 -noout -text
```

```
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number:
    ...
    Signature Algorithm: sha256WithRSAEncryption
    ...
  Subject:
  Subject Public Key Info:
    Public Key Algorithm: id-ecPublicKey
    Public-Key: (256 bit)
    pub:
    ...
    ASN1 OID: prime256v1
    NIST CURVE: P-256
```

istiod will generate a self-signed CA certificate using RSA if plugged in custom CA certificates aren't specified



# MeshConfig support In Istio 1.10

I am currently working on having ECC be supported in meshConfig for Istio 1.10 as an **Alpha** feature

- There will be a migration path and environmental variables as used in this talk will continue to be supported through at least 1.10 to allow users to migrate towards this feature



# Other environmental variables

There are many other environmental variables that can be set.

For more information see

<https://istio.io/latest/docs/reference/commands/pilot-agent/#envvars>

**Remember: Always look to see if there are *other, better* ways of enabling functionality; environmental variables are considered experimental.**

#IstioCon





# Thank you!

Jacob Delgado  
Aspen Mesh

#IstioCon

