

Binary Authorization

Google's BCID (Borg Caller ID)


BCID is an internal tool at Google whose mission is to help ensure that all code running in production is properly reviewed and authorized.

BCID GOAL'S

To ensure that jobs have been "LGTM'd"



BCID's goals are **Data Protection** and **Change Management**.



Jobs that have access to *user data*

Internal tool



Customer facing

Binary Authorization



BCID

How can we ensure that the customer
CI/CD pipeline is used and used
correctly?

Binary Authorization provides deployment control for Google's Container Engine (GKE).

Let's get started on the MVP UX flow.

Security

Security Command Center

Identity-aware proxy

Cryptographic keys

Binary authorization

Welcome to Binary Authorization

Binary Authorization provides deployment control for Google Kubernetes Engine (GKE). [Learn more](#)

Binary authorization set-up

Define your Binary Authorization policy to restrict the deployment behaviors for this project.

Binary Authorization policy uses previously defined Attestors from the current projects or other projects you have access to.

→ [Configure BinAuthZ policy](#)

→ [Create Attestors](#)

Binary Authorization docs

Learn more about Binary Authorization capabilities and its features.

Check out our quick start Codelab.

→ [View documentation](#)

→ [View Codelab](#)

Security

- Security Command Center
- Identity-aware proxy
- Cryptographic keys
- Binary authorization

Binary Authorization

EDIT POLICY

PERMISSIONS

POLICY ATTESTORS

Binary authorization lets you restrict which images can be deployed to a Kubernetes Engine cluster by making sure they pass through the appropriate checkpoints in your deployment workflow. [Learn more](#)

Policy deployment rules

Project default rule	Allow only images that have been approved by all of the following attestors: <ul style="list-style-type: none"> • Dev Signer This is for the dev Signer • Trusted builder Centralized secure build pipeline for all production jobs
Cluster-specific rules	-
Dry run mode	Not enabled
Images exempt from policy	-

Security

- Security Command Center
- Identity-aware proxy
- Cryptographic keys
- Binary authorization

Binary Authorization [EDIT POLICY](#)

[PERMISSIONS](#)

POLICY ATTESTORS

Binary authorization lets you restrict which images can be deployed to a Kubernetes Engine cluster by making sure they pass through the appropriate checkpoints in your deployment workflow. [Learn more](#)

Policy deployment rules

Project default rule	<p>Allow only images that have been approved by all of the following attestors:</p> <ul style="list-style-type: none"> Dev Signer This is for the dev Signer Trusted builder Centralized secure build pipeline for all production jobs
Cluster-specific rules	<ul style="list-style-type: none"> ClusterFoo Default: Allow all images ClusterBar Default: Allow all images ClusterFB Attestors required: Dev signer, Prod reviewer
Dry run mode	Not enabled
Images exempt from policy	<pre>gcr.io/google-appengine/nodejs* docker.io/nginx*</pre>

Security

Security Command Center

Identity-aware proxy

Cryptographic keys

Binary authorization

← Edit policy

Deployment rules

Applies to this project and all clusters that don't have a cluster-specific rule. When a container image is deployed, a deployment rule will be applied unless the image is exempted as specified in the section below.

Project default rule ⓘ

- Allow all images
- Disallow all images
- Allow only images that have been approved by all of the following attestors

ADD ATTESTORS

Dry run mode ⓘ

- Audit log but do not block disallowed images

Cluster-specific rules

Deployment rules for specific clusters. Project default rules won't apply to a cluster if a cluster-specific rule is defined.

Active clusters [3], Cluster rules [0] ▼

Images exempt from deployment rules

Images listed here are exempt from deployment rule checks. Wildcards (*) are allowed in image paths.

Image paths [0] ▼

SAVE POLICY CANCEL

Security

Security Command Center

Identity-aware proxy


Cryptographic keys

Binary authorization


← Edit policy

Deployment rules

Applies to this project and all clusters that don't have a cluster-specific rule. When a container image is deployed, a deployment rule will be applied unless the image is exempted as specified in the section below.

Project default rule 

- Allow all images
- Disallow all images
- Allow only images that have been approved by all of the following attestors

[ADD ATTESTORS](#)Dry run mode 

- Audit log but do not block disallowed images

Cluster-specific rules

Deployment rules for specific clusters. Project default rules won't apply to a cluster if a cluster-specific rule is defined.

Active clusters [3], Cluster rules [0] 

Images exempt from deployment rules

Images listed here are exempt from deployment rule checks. Wildcards (*) are allowed in image paths.

Image paths [0] [SAVE POLICY](#) [CANCEL](#)

Security

- Security Command Center
- Identity-aware proxy
- Cryptographic keys
- Binary authorization

← Edit policy

Deployment rules

Applies to this project and all clusters that don't have a cluster-specific rule. When a container image is deployed, a deployment rule will be applied unless the image is exempted as specified in the section below.

Project default rule

- Allow all images
- Disallow all images
- Allow only images that have been attested

ADD ATTESTORS

Dry run mode

- Audit log but do not block disallowed images

Cluster-specific rules

Deployment rules for specific clusters

Active clusters [3], Cluster rules [0]

Images exempt from deployment rules

Images listed here are exempt from deployment rules

Image paths [0]

SAVE POLICY CANCEL

Add attestors

Attestors have the authority to make statements about an image. [Learn more](#)

Filter attestors

Attestors	Description
<input type="checkbox"/> custom approver	This is a new attestor
<input checked="" type="checkbox"/> Trusted Builder	Centralized secure build pipeline for all production jobs
<input type="checkbox"/> QA Signer	Team performs functionality tests and integration tests
<input checked="" type="checkbox"/> Dev Signer	This is for the dev Signer
<input type="checkbox"/> Legal	Legal team reviews for policy violations
<input type="checkbox"/> Prod reviewer	Reviews for production readiness
<input type="checkbox"/> Sec scanner	Security scanner for known vulnerabilities

+ CREATE NEW ATTESTOR

CANCEL ADD 2 ATTESTORS

Security

- Security Command Center
- Identity-aware proxy
- Cryptographic keys
- Binary authorization

← Edit policy

Deployment rules

Applies to this project and all clusters that don't have a cluster-specific rule. When a container image is deployed, a deployment rule will be applied unless the image is exempted as specified in the section below.

Project default rule

- Allow all images
- Disallow all images
- Allow only images that have been approved by all of the following attestors

Approvers	Description		
Trusted Builder	This is for the Trusted Builder	'Add' pending	
Dev Signer	This is for the dev Signer	'Add' pending	

ADD ATTESTORS

Dry run mode

- Audit log but do not block disallowed images

Cluster-specific rules

Deployment rules for specific clusters. Project default rules won't apply to a cluster if a cluster-specific rule is defined.

Active clusters [3], Cluster rules [0]

Images exempt from deployment rules

Images listed here are exempt from deployment rule checks. Wildcards (*) are allowed in image paths.

Image paths [0]

SAVE POLICY CANCEL

be applied unless the image is exempted as specified in the section below.

Cryptographic keys

Binary authorization

Project default rule ?

- Allow all images
- Disallow all images
- Allow only images that have been approved by all of the following attestors

Approvers	Description		
<input checked="" type="checkbox"/> Trusted Builder	This is for the Trusted Builder	'Add' pending	
<input checked="" type="checkbox"/> Dev Signer	This is for the dev Signer	'Add' pending	

ADD ATTESTORS

Dry run mode ?

- Audit log but do not block disallowed images

Cluster-specific rules

Deployment rules for specific clusters. Project default rules won't apply to a cluster if a cluster-specific rule is defined.

Filter clusters ^

Name	Rule description	
<input checked="" type="checkbox"/> ClusterFoo	Default: Allow all images	⋮
<input checked="" type="checkbox"/> CusterBar	Default: Allow all images	⋮
<input checked="" type="checkbox"/> ClusterFB	Default: Allow all images	⋮
<input type="checkbox"/> ⚠ SomeCluster	-	⋮
<input type="checkbox"/> ⚠ Cluster01	-	⋮
<input type="checkbox"/> ❌ Cluster02	-	⋮
<input type="checkbox"/> ❌ Cluster03	-	⋮

[+ ADD CLUSTER SPECIFIC RULE](#)

Binary Authorization enabled

No GKE cluster of that name

Binary Authorization disabled

- Edit
- Delete
- Enable in GKE console

Images exempt from deployment rules

Images listed here are exempt from deployment rule checks. Wildcards (*) are allowed in image paths.

Image paths [0] v

SAVE POLICY CANCEL

- Identity-aware proxy
- Cryptographic keys
- Binary authorization

be applied unless the image is exempted as specified in the section below.

Project default rule ⓘ

- Allow all images
- Disallow all images
- Allow only images that have been approved by all of the following attestors

Approvers	Description		
Trusted Builder	This is for the Trusted Builder	'Add' pending	
Dev Signer	This is for the dev Signer	'Add' pending	

ADD ATTESTORS

Dry run mode ⓘ

- Audit log but do not block

Cluster-specific rules

Deployment rules for specific c

Filter clusters

Name
ClusterFoo
ClusterBar
ClusterFB
SomeCluster
Cluster01
Cluster02
Cluster03

ADD CLUSTER SPEC

Edit cluster specific rule for ClusterFB

Project default rules ⓘ

- Allow all images
- Disallow all images
- Allow only images that have been approved by all of the following attestors

Filter attestors

Attestors	Description
<input type="checkbox"/> custom approver	This is a new attestor
<input type="checkbox"/> Trusted Builder	Centralized secure build pipeline for all production jobs
<input type="checkbox"/> QA Signer	Team performs functionality tests and integration tests
<input type="checkbox"/> Dev Signer	This is for the dev Signer
<input type="checkbox"/> Legal	Legal team reviews for policy violations
<input type="checkbox"/> Prod reviewer	Reviews for production readiness
<input type="checkbox"/> Sec scanner	Security scanner for known vulnerabilities

+ CREATE NEW ATTESTOR

Dry run mode ⓘ

- Audit log but do not block disallowed images

CANCEL ADD

Images exempt from deplo

Images listed here are exempt from deployment rule checks. Wildcards (*) are allowed in image paths.

Image paths [0]

SAVE POLICY CANCEL

- Identity-aware proxy
- Cryptographic keys
- Binary authorization

Project default rule ?

- Allow all images
- Disallow all images
- Allow only images that have been approved by all of the following attestors

Approvers	Description		
Trusted Builder	This is for the Trusted Builder	'Add' pending	
Dev Signer	This is for the dev Signer	'Add' pending	

ADD ATTESTORS

Dry run mode ?

- Audit log but do not block

Cluster-specific rules

Deployment rules for specific c

Filter clusters

Name
ClusterFoo
CusterBar
ClusterFB
SomeCluster
Cluster01
Cluster02
Cluster03

[+ ADD CLUSTER SPEC](#)

Edit cluster specific rule for ClusterFB

Project default rules ?

- Allow all images
- Disallow all images
- Allow only images that have been approved by all of the following attestors

Filter attestors

Attestors	Description
<input type="checkbox"/> custom approver	This is a new attestor
<input type="checkbox"/> Trusted Builder	Centralized secure build pipeline for all production jobs
<input type="checkbox"/> QA Signer	Team performs functionality tests and integration tests
<input checked="" type="checkbox"/> Dev Signer	This is for the dev Signer
<input type="checkbox"/> Legal	Legal team reviews for policy violations
<input checked="" type="checkbox"/> Prod reviewer	Reviews for production readiness
<input type="checkbox"/> Sec scanner	Security scanner for known vulnerabilities

[+ CREATE NEW ATTESTOR](#)

Dry run mode ?

- Audit log but do not block disallowed images

CANCEL ADD

Images exempt from deplo

Images listed here are exempt from deployment rule checks. Wildcards (*) are allowed in image paths.

Image paths [0]

SAVE POLICY CANCEL

Identity-aware proxy

Cryptographic keys

Binary authorization

Applied to this project and all clusters that don't have a cluster-specific rule. When a container image is deployed, a deployment rule will be applied unless the image is exempted as specified in the section below.

Project default rule ⓘ

- Allow all images
- Disallow all images
- Allow only images that have been approved by all of the following attestors

Approvers	Description		
Trusted Builder	This is for the Trusted Builder	'Add' pending	
Dev Signer	This is for the dev Signer	'Add' pending	

[ADD ATTESTORS](#)

Dry run mode ⓘ

- Audit log but do not block disallowed images

Cluster-specific rules

Deployment rules for specific clusters. Project default rules won't apply to a cluster if a cluster-specific rule is defined.

Filter clusters ⌵

Name	Rule description	
ClusterFoo	Default: Allow all images	
ClusterBar	Default: Allow all images	
ClusterFB	Attestors required: Dev signer, Prod reviewer	
SomeCluster	-	
Cluster01	-	
Cluster02	-	
Cluster03	-	

[+ ADD CLUSTER SPECIFIC RULE](#)

Edit

Delete

Enable in GKE console

Images exempt from deployment rules

Images listed here are exempt from deployment rule checks. Wildcards (*) are allowed in image paths.

Image paths [0] ⌵

[SAVE POLICY](#) [CANCEL](#)

Identity-aware proxy

Cryptographic keys

Binary authorization

Applied to this project and all clusters that don't have a cluster-specific rule. When a container image is deployed, a deployment rule will be applied unless the image is exempted as specified in the section below.

Project default rule

- Allow all images
- Disallow all images
- Allow only images that have been approved by all of the following attestors

Approvers	Description		
Trusted Builder	This is for the Trusted Builder	'Add' pending	
Dev Signer	This is for the dev Signer	'Add' pending	

ADD ATTESTORS

Dry run mode

- Audit log but do not block disal

Cluster-specific rules

Deployment rules for specific cluster

Filter clusters

Name	Rule	
ClusterFoo	Default: Allow all images	⋮
CusterBar	Default: Allow all images	⋮
ClusterFB	Attestors required: Dev signer, Prod reviewer	⋮
SomeCluster	-	⋮
Cluster01	-	⋮
Cluster02	-	⋮
Cluster03	-	⋮

ADD CLUSTER SPECIFIC RULE

Remove deployment rule override for ClusterFB

Removing this override will remove the requirement of having approvers authorize on this cluster and revert back to the default deployment rule which will always allow all images.

CLOSE REMOVE

Images exempt from deployment rules

Images listed here are exempt from deployment rule checks. Wildcards (*) are allowed in image paths.

SAVE POLICY CANCEL

Identity-aware proxy

Cryptographic keys

Binary authorization

Applied to this project and all clusters that don't have a cluster-specific rule. When a container image is deployed, a deployment rule will be applied unless the image is exempted as specified in the section below.

Project default rule ⓘ

- Allow all images
- Disallow all images
- Allow only images that have been approved by all of the following attestors

Approvers	Description		
Trusted Builder	This is for the Trusted Builder	'Add' pending	
Dev Signer	This is for the dev Signer	'Add' pending	

[ADD ATTESTORS](#)

Dry run mode ⓘ

- Audit log but do not block disallowed images

Cluster-specific rules

Deployment rules for specific clusters. Project default rules won't apply to a cluster if a cluster-specific rule is defined.

Filter clusters ^

Name	Rule description	
ClusterFoo	Default: Allow all images	
CusterBar	Default: Allow all images	
ClusterFB	Default: Allow all images	
SomeCluster	-	
Cluster01	-	
Cluster02	-	
Cluster03	-	

[+ ADD CLUSTER SPECIFIC RULE](#)

Images exempt from deployment rules

Images listed here are exempt from deployment rule checks. Wildcards (*) are allowed in image paths.

Image paths [0]

[SAVE POLICY](#) [CANCEL](#)

Identity-aware proxy





Cryptographic keys

Binary authorization

Applied to this project and all clusters that don't have a cluster-specific rule. When a container image is deployed, a deployment rule will be applied unless the image is exempted as specified in the section below.

Project default rule

- Allow all images
- Disallow all images
- Allow only images that have been approved by all of the following attestors

Approvers	Description		
 Trusted Builder	This is for the Trusted Builder	'Add' pending	
 Dev Signer	This is for the dev Signer	'Add' pending	


[ADD ATTESTORS](#)

Dry run mode

- Audit log but do not block disallowed images

Cluster-specific rules

Deployment rules for specific clusters. Project default rules won't apply to a cluster if a cluster-specific rule is defined.

Active clusters [3], Cluster rules [1] 'Add' pending 

Images exempt from deployment rules

Images listed here are exempt from deployment rule checks. Wildcards (*) are allowed in image paths.








Image path		
gcr.io/google-appengine/nodejs*		
docker.io/nginx*		

[+ ADD IMAGE PATH](#)

[SAVE POLICY](#) [CANCEL](#)

Identity-aware proxy




Cryptographic keys

Binary authorization

Applied to this project and all clusters that don't have a cluster-specific rule. When a container image is deployed, a deployment rule will be applied unless the image is exempted as specified in the section below.

Project default rule

- Allow all images
- Disallow all images
- Allow only images that have been approved by all of the following attestors

Approvers	Description		
 Trusted Builder	This is for the Trusted Builder	'Add' pending	
 Dev Signer	This is for the dev Signer	'Add' pending	

[ADD ATTESTORS](#)

Dry run mode

- Audit log but do not block disallowed images

Cluster-specific rules

Deployment rules for specific clusters. Project default rules won't apply to a cluster if a cluster-specific rule is defined.

Active clusters **[3]**, Cluster rules **[1]** 'Add' pending 

Images exempt from deployment rules

Images listed here are exempt from deployment rule checks. Wildcards (*) are allowed in image paths.










Image path

gcr.io/google-appengine/nodejs*		
docker.io/nginx*		
gcr.io/testlabs/payment@sha256:aba48d60ba4410ec921f9d2e816		

[+ ADD IMAGE PATH](#)

[SAVE POLICY](#) [CANCEL](#)

- Identity-aware proxy
- Cryptographic keys
- Binary authorization

Applied to this project and all clusters that don't have a cluster-specific rule. When a container image is deployed, a deployment rule will be applied unless the image is exempted as specified in the section below.

Project default rule ⓘ

- Allow all images
- Disallow all images
- Allow only images that have been approved by all of the following attestors

Approvers	Description		
Trusted Builder	This is for the Trusted Builder	'Add' pending	
Dev Signer	This is for the dev Signer	'Add' pending	

[ADD ATTESTORS](#)

Dry run mode ⓘ

- Audit log but do not block disallowed images

Cluster-specific rules

Deployment rules for specific clusters. Project default rules won't apply to a cluster if a cluster-specific rule is defined.

Active clusters [3], Cluster rules [1] 'Add' pending

Images exempt from deployment rules

Images listed here are exempt from deployment rule checks. Wildcards (*) are allowed in image paths.

Image path

gcr.io/google-appengine/nodejs*		
docker.io/nginx*		
gcr.io/testlabs/payment@sha256:aba48d60ba...	'Add' pending	

[+ ADD IMAGE PATH](#)

[SAVE POLICY](#) [CANCEL](#)

Identity-aware proxy

Cryptographic keys

Binary authorization

Applied to this project and all clusters that don't have a cluster-specific rule. When a container image is deployed, a deployment rule will be applied unless the image is exempted as specified in the section below.

Project default rule ⓘ

- Allow all images
- Disallow all images
- Allow only images that have been approved by all of the following attestors

Approvers	Description		
Trusted Builder	This is for the Trusted Builder	'Add' pending	
Dev Signer	This is for the dev Signer	'Add' pending	

ADD ATTESTORS

Dry run mode ⓘ

- Audit log but do not block

Cluster-specific rules

Deployment rules for specific clusters

Active clusters [3], Cluster rules

Images exempt from deployment

Images listed here are exempt from deployment rule checks. Wildcards (*) are allowed in image paths.

Image path		
gcr.io/google-appengine/nodejs*		
docker.io/nginx*		
gcr.io/testlabs/payment@sha256:aba48d60ba...	'Add' pending	

ADD IMAGE PATH

SAVE POLICY CANCEL

Save policy

You are navigating away from the policy page before hitting the 'save policy' button

In order to save changes made for this policy, hit the "save policy" button found on the bottom of the policy page.

LEAVE STAY

Security

- Security Command Center
- Identity-aware proxy
- Cryptographic keys
- Binary authorization

Binary Authorization [+ CREATE ATTESTOR](#)

[PERMISSIONS](#)

POLICY ATTESTORS

Attestors have the authority to make statements about an image. [Learn more](#)

 Filter attestors

<input type="checkbox"/>	Name	Description	Public Keys	Last Updated
--------------------------	------	-------------	-------------	--------------

Security

- Security Command Center
- Identity-aware proxy
- Cryptographic keys
- Binary authorization

Binary Authorization [+ CREATE ATTESTOR](#)

[PERMISSIONS](#)

POLICY ATTESTORS

Attestors have the authority to make statements about an image. [Learn more](#)

Filter attestors

<input type="checkbox"/>	Name	Description	Public Keys	Last Updated	
<input type="checkbox"/>	✔ Trusted Builder	This is for the Trusted Builder	1	April 1, 2018 - 8:00 AM	⋮
<input type="checkbox"/>	✔ Dev Signer	This is for the Dev Signer	1	April 1, 2018 - 8:00 AM	⋮

Security

- Security Command Center
- Identity-aware proxy
- Cryptographic keys
- Binary authorization

← Create attestor

Attestors have the authority to make statements about an image. [Learn more](#)

Attestor name

Make sure that your name is easy to identify.

Create default analysis note

A corresponding note needs to be created in Container Analysis directly prior to creating an attestor in Binary Authorization. [Learn more](#)

Container analysis note name

Description (Optional)

The description is shown during rule setup to provide additional context for attestors.

PGP public keys

Learn more about key generation and how to set one up. [Learn more](#)

Add a PGP public key

Name (optional)

PASTE KEY or UPLOAD KEY

DONE

CANCEL

ADD KEY

CREATE

CANCEL

Security

- Security Command Center
- Identity-aware proxy
- Cryptographic keys
- Binary authorization

← Create attestor

Attestors have the authority to make statements about an image. [Learn more](#)

Attestor name
QA

Make sure that your name is easy to identify.

Create default analysis note

A corresponding note needs to be created in Container Analysis directly prior to creating an attestor in Binary Authorization. [Learn more](#)

Container analysis note name

Description (Optional)
This is the QA team

The description is shown during rule setup to provide additional context for attestors.

PGP public keys

Learn more about key generation and how to set one up. [Learn more](#)

Add a PGP public key

Name (optional)
Key version 1.0.0

PASTE KEY or UPLOAD KEY

```

---BEGIN PGP PUBLIC KEY BLOCK---
Version: BCPG C# v1.6.1.0

IAjwker83lkjslkjf,lakjsldkdfjllklakjsldkfljllkallsllsllskdfjsf13120893a

```

DONE CANCEL

ADD KEY

CREATE CANCEL

Security

- Security Command Center
- Identity-aware proxy
- Cryptographic keys
- Binary authorization

Binary Authorization [+ CREATE ATTESTOR](#)

[PERMISSIONS](#)

POLICY ATTESTORS

Attestors have the authority to make statements about an image. [Learn more](#)

Filter attestors

Close, Refresh, Filter icons

<input type="checkbox"/>	Name	Description	Public Keys	Last Updated	
<input type="checkbox"/>	✔ QA	This is the QA team	2	April 1, 2018 - 8:00 AM	⋮
<input type="checkbox"/>	✔ Trusted Builder	This is for the Trusted Builder	1	April 1, 2018 - 8:00 AM	⋮
<input type="checkbox"/>	✔ Dev Signer	This is for the Dev Signer	1	April 1, 2018 - 8:00 AM	⋮

Security

- Security Command Center
- Identity-aware proxy
- Cryptographic keys
- Binary authorization

← "QA" attester [EDIT](#) [DELETE](#) [DISABLE](#)

Attester name ⓘ

QA

Container analysis note name ⓘ

projects/some_project/notes/some_note

Description (optional) ⓘ

This is the QA team

Public keys ⓘ

Name: Key version 1.0.0 ID: 5252E2D910...

Name: legal change ID: 728282D910...

Security

- Security Command Center
- Identity-aware proxy
- Cryptographic keys
- Binary authorization

← "QA" attester [EDIT](#) [DELETE](#) [DISABLE](#)

Attester name ⓘ

QA

Container analysis note name ⓘ

projects/some_project/notes/some_note

Description (optional) ⓘ

This is the QA team

Public keys ⓘ

Name: Key-version 1.0.0 ID: 5252E2D910... Pending deletion [UNDO](#)

Name: legal change ID: 728282D910... [EDIT](#)

[SAVE CHANGES](#) [CANCEL](#)

Security

- Security Command Center
- Identity-aware proxy
- Cryptographic keys
- Binary authorization

← "QA" attestor EDIT DELETE DISABLE

Attestor name ⓘ

QA

Container analysis note name ⓘ

projects/some_project/notes/some_note

Description (optional) ⓘ

This is the QA team

Public keys ⓘ

ID: 5252E2D910 🗑️ ⬆️

Name (optional)
Key version 1.0.0

```

---BEGIN PGP PUBLIC KEY BLOCK---
Version: BCPG C# v1.6.1.0

IAjwker83lkjslkf;lakjsldkfjllklakjsdlkfkjllkallslslslskdfjsf13120893aoiu7
833nbskksfhI9920709833nbskksfhI9920709IAjwker83lkjslkf;lakjsldkfj
llklakjsldkfjllklakjsdlkfkjllkallslslslskdfjsf13120893aoiu7
  
```

NEXT CANCEL

Name: legal change ID: 728282D910... ⌵

SAVE CHANGES CANCEL

Security

- Security Command Center
- Identity-aware proxy
- Cryptographic keys
- Binary authorization

Binary Authorization [+ CREATE ATTESTOR](#)

[PERMISSIONS](#)

POLICY ATTESTORS

Attestors have the authority to make statements about an image. [Learn more](#)

Filter attestors

Close, Refresh, Filter icons

<input type="checkbox"/>	Name	Description	Public Keys	Last Updated	
<input type="checkbox"/>	✔ QA	This is the QA team	2	April 1, 2018 - 8:00 AM	⋮
<input type="checkbox"/>	✔ Trusted Builder	This is for the Trusted Builder	1	April 1, 2018 - 8:00 AM	⋮
<input type="checkbox"/>	✔ Dev Signer	This is for the Dev Signer	1	April 1, 2018 - 8:00 AM	⋮

- Edit
- Disable
- Delete

Security

- Security Command Center
- Identity-aware proxy
- Cryptographic keys
- Binary authorization

Binary Authorization [+ CREATE ATTESTOR](#)

[PERMISSIONS](#)


POLICY ATTESTORS

Attestors have the authority to make statements about an image. [Learn more](#)

Filter attestors

<input type="checkbox"/>	Name	Description	Public Keys	Last Updated	
<input type="checkbox"/>	<input checked="" type="checkbox"/> QA	This is the QA team	2	April 1, 2018 - 8:00 AM	⋮
<input type="checkbox"/>	<input checked="" type="checkbox"/> Trusted Builder	This is for the Trusted Builder	1	April 1, 2018 - 8:00 AM	⋮
<input type="checkbox"/>	<input checked="" type="checkbox"/> Dev Signer			18 - 8:00 AM	⋮

Disable "Dev Signer" attestor

 Disabling this attestor will affect your policy if it's part of your deployment rule

Are you sure you want to disable?

[CLOSE](#) [YES, DISABLE](#)

Security

- Security Command Center
- Identity-aware proxy
- Cryptographic keys
- Binary authorization

Binary Authorization [+ CREATE ATTESTOR](#)

[PERMISSIONS](#)

POLICY ATTESTORS

Attestors have the authority to make statements about an image. [Learn more](#)

Filter attestors

<input type="checkbox"/>	Name	Description	Public Keys	Last Updated	
<input type="checkbox"/>	QA	This is the QA team	2	April 1, 2018 - 8:00 AM	
<input type="checkbox"/>	Trusted Builder	This is for the Trusted Builder	1	April 1, 2018 - 8:00 AM	
<input type="checkbox"/>	Dev Signer	This is for the Dev Signer	1	April 1, 2018 - 8:00 AM	

Security

- Security Command Center
- Identity-aware proxy
- Cryptographic keys
- Binary authorization

Binary Authorization [+ CREATE ATTESTOR](#)

[PERMISSIONS](#)

POLICY ATTESTORS

Attestors have the authority to make statements about an image. [Learn more](#)

Filter attestors

Close, Refresh, Filter icons

<input type="checkbox"/>	Name	Description	Public Keys	Last Updated	
<input type="checkbox"/>	<input checked="" type="checkbox"/> QA	This is the QA team	2	April 1, 2018 - 8:00 AM	⋮
<input type="checkbox"/>	<input checked="" type="checkbox"/> Trusted Builder	This is for the Trusted Builder	1	April 1, 2018 - 8:00 AM	⋮
<input type="checkbox"/>	<input type="checkbox"/> Dev Signer	This is for the Dev Signer	1	April 1, 2018 - 8:00 AM	⋮

- Edit
- Enable
- Delete

Security

- Security Command Center
- Identity-aware proxy
- Cryptographic keys
- Binary authorization

Binary Authorization [+ CREATE ATTESTOR](#)

[PERMISSIONS](#)


POLICY ATTESTORS

Attestors have the authority to make statements about an image. [Learn more](#)

Filter attestors

<input type="checkbox"/>	Name	Description	Public Keys	Last Updated	
<input type="checkbox"/>	<input checked="" type="checkbox"/> QA	This is the QA team	2	April 1, 2018 - 8:00 AM	⋮
<input type="checkbox"/>	<input checked="" type="checkbox"/> Trusted Builder			18 - 8:00 AM	⋮
<input type="checkbox"/>	<input type="checkbox"/> Dev Signer			18 - 8:00 AM	⋮

Delete "Dev Signer" approver

 Deleting this approver may potentially affect your policy.

Deleting "Dev Signer" is permanent. Consider disabling this approver as an alternative.

[CLOSE](#) [DELETE](#)

Security

- Security Command Center
- Identity-aware proxy
- Cryptographic keys
- Binary authorization

Binary Authorization [+ CREATE ATTESTOR](#)

[PERMISSIONS](#)

POLICY ATTESTORS

Attestors have the authority to make statements about an image. [Learn more](#)

Filter attestors

<input type="checkbox"/>	Name	Description	Public Keys	Last Updated	
<input type="checkbox"/>	<input checked="" type="checkbox"/> QA	This is the QA team	2	April 1, 2018 - 8:00 AM	<input type="button" value="vertical dots"/>
<input type="checkbox"/>	<input checked="" type="checkbox"/> Trusted Builder	This is for the Trusted Builder	1	April 1, 2018 - 8:00 AM	<input type="button" value="vertical dots"/>