
AWS
re:Invent

SEC304

Using certificate-based authentication on containers and web servers on AWS

Kevin Rioles
Principal Architect
BlackSky

Ram Ramani
Security Solutions Architect
AWS

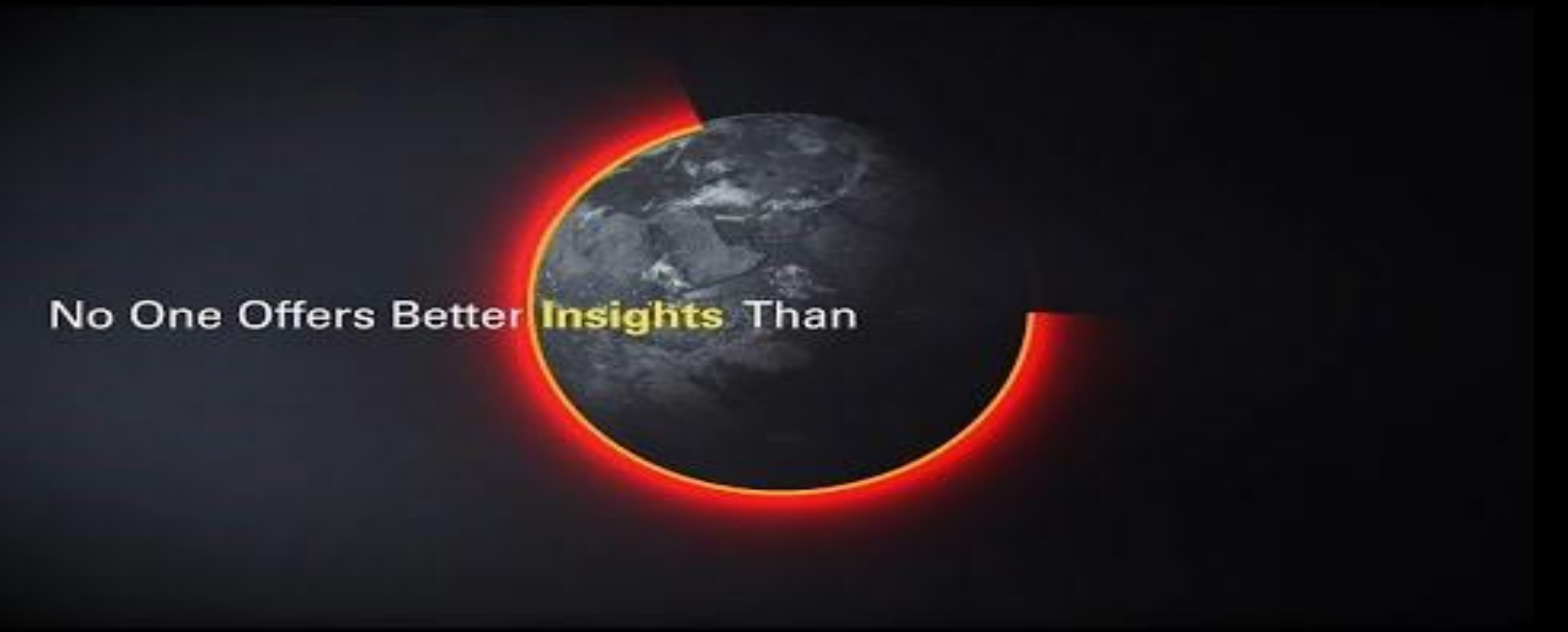
Josh Rosenthol
Product Manager, ACM and ACM Private CA
AWS

AWS re:Invent

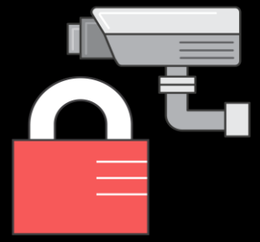
© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

BLACK SKY

Be The First To Know



ACM Private Certificate Authority (CA)



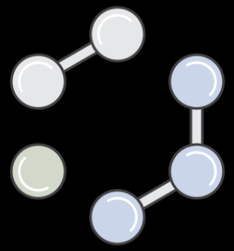
Secure and managed private certificate authority



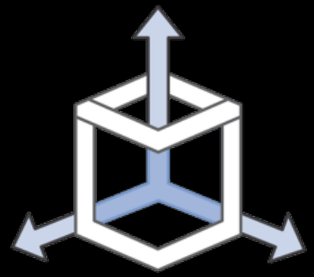
Root CA and complete CA hierarchies



Enable developer agility



Flexibility to customize



Manage certificate authorities centrally



Pay-as-you-go pricing

Key takeaways

After watching this presentation you will learn about:

- BlackSky's architectural choices for deploying TLS Everywhere
- An example of how BlackSky generated and deployed certificates for its containers and transient instances
- Deployment best practices for TLS Everywhere



© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Program goal

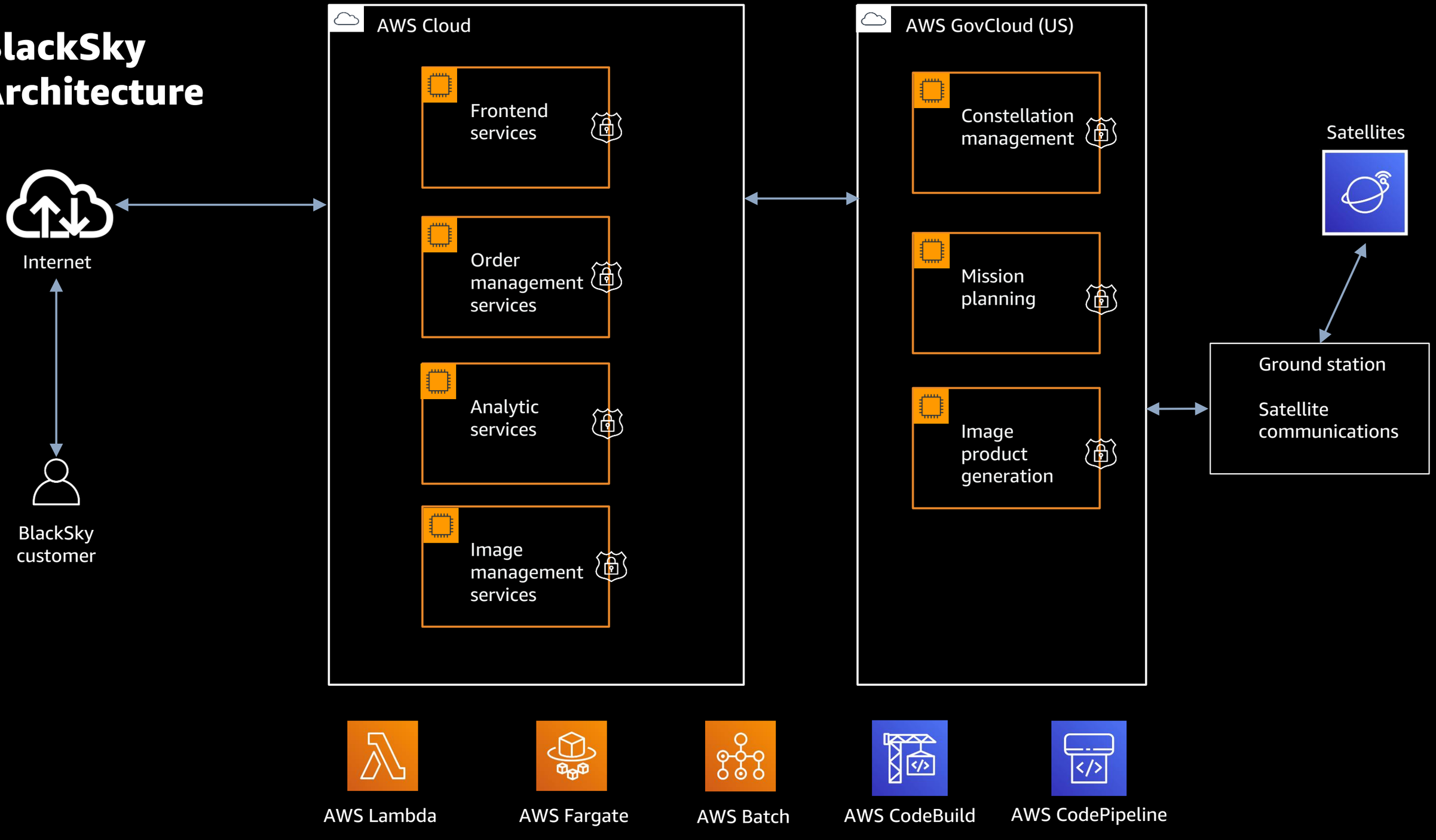
We monitor activities and facilities worldwide by harnessing the world's emerging sensor networks, including our own satellite constellation. BlackSky's on-demand satellites can image a location from dawn to dusk. We process millions of observations daily from space, air, IoT, foreign news, social media, industry publications, financial reports while including environmental and asset sensors.

BlackSky needed to protect all of its communications (external and internal) for the access and transmission of this highly sensitive data.

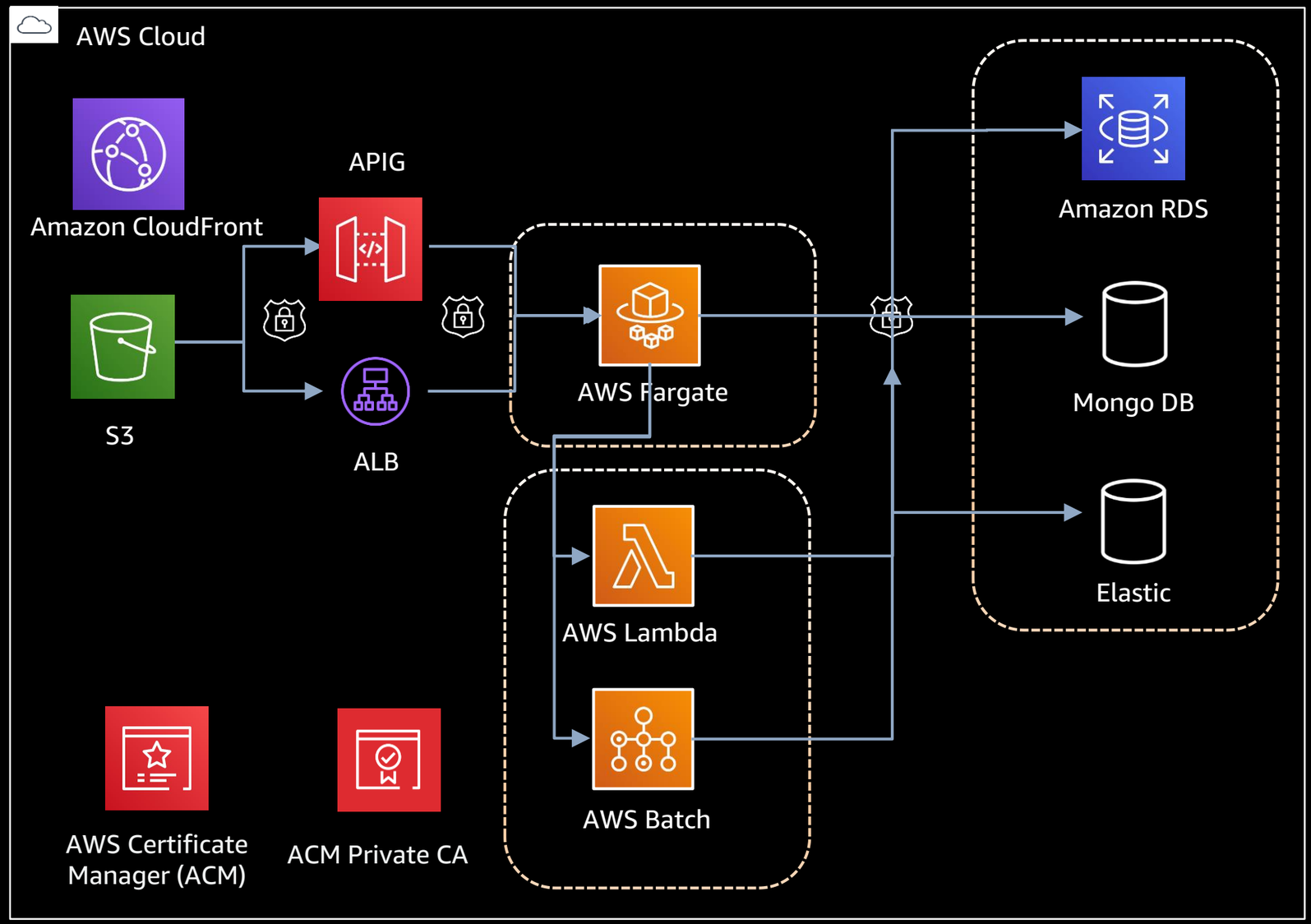


© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

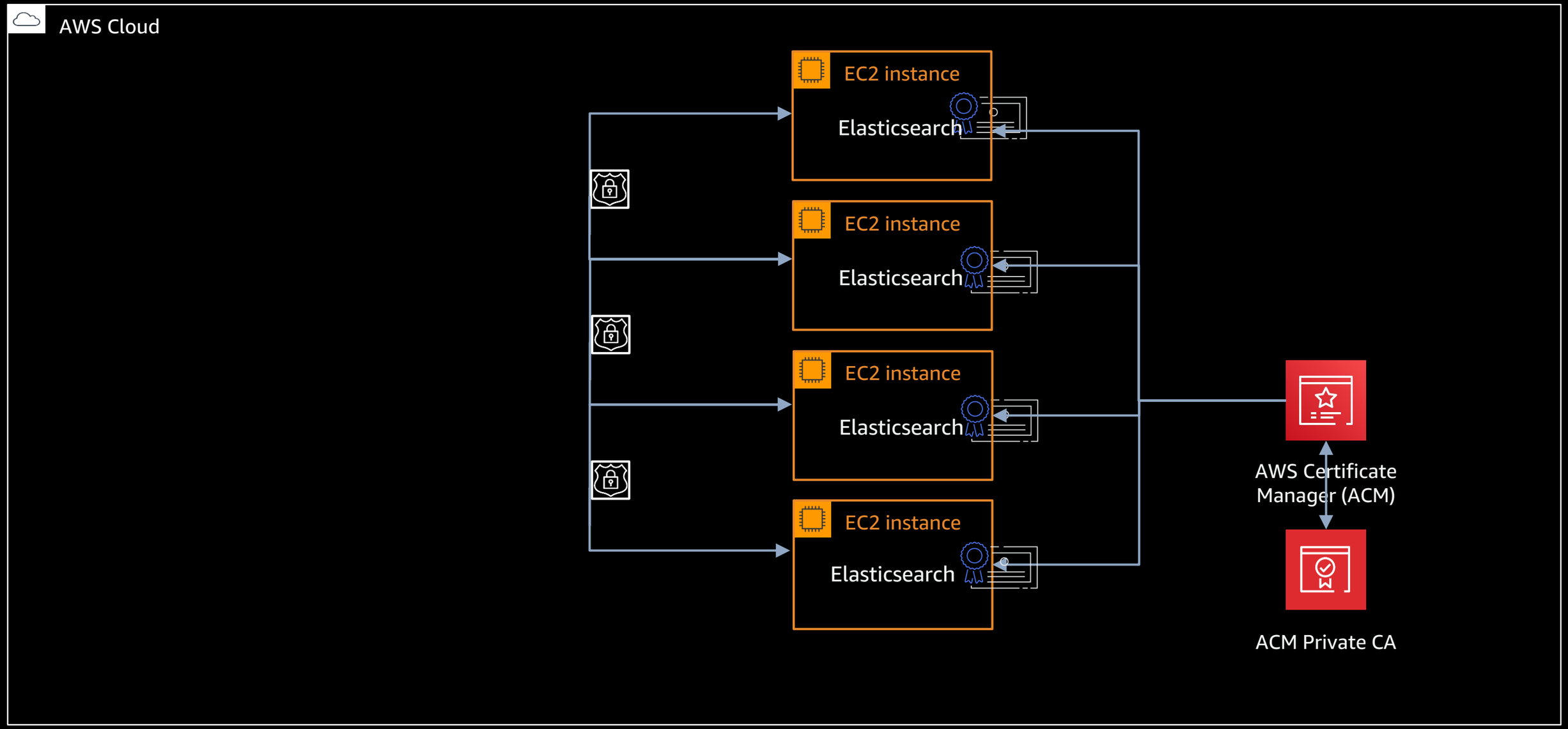
BlackSky Architecture



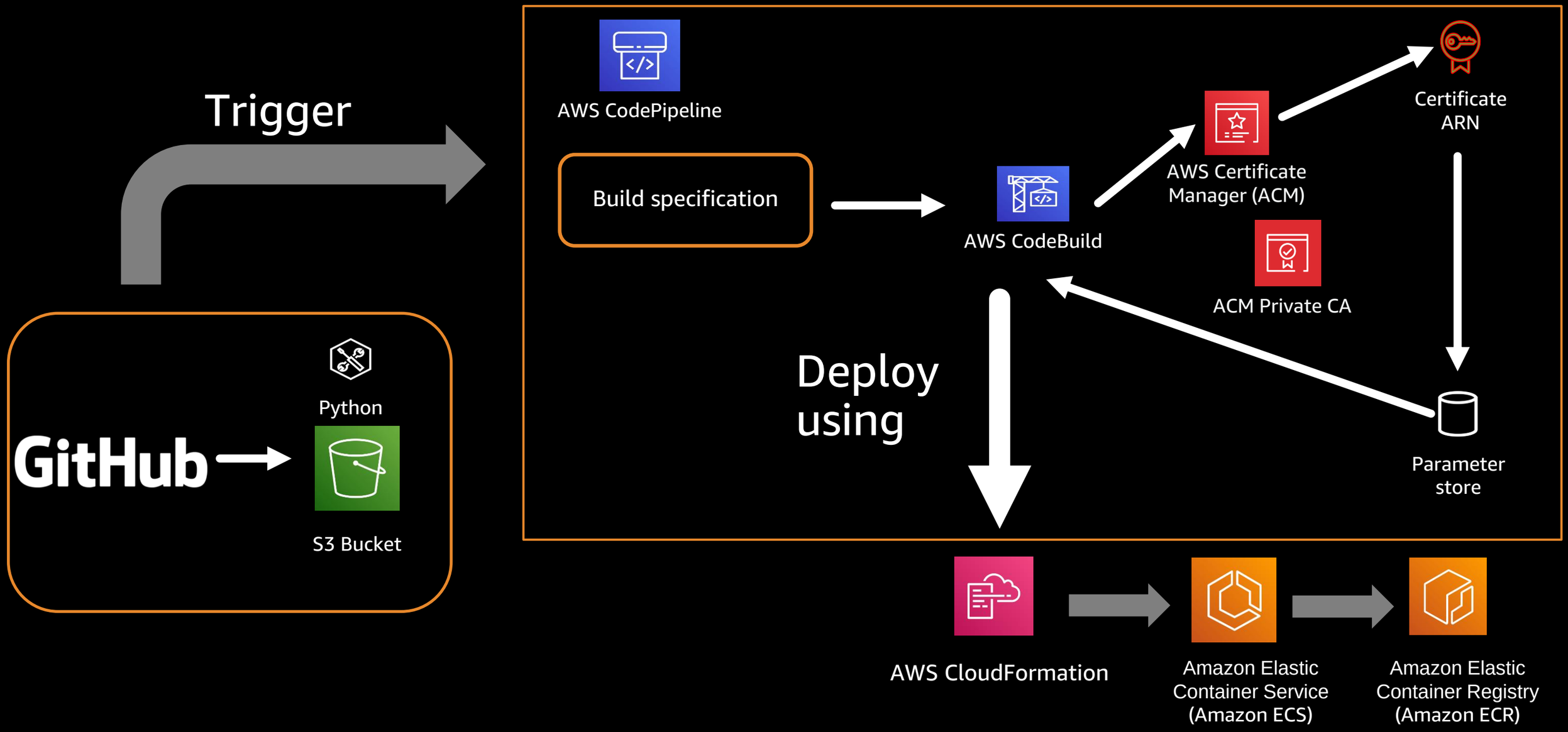
BlackSky front end



Amazon Elasticsearch instance-to-instance TLS using ACM Private Certificates



CI/CD pipeline for certificate deployment on containers

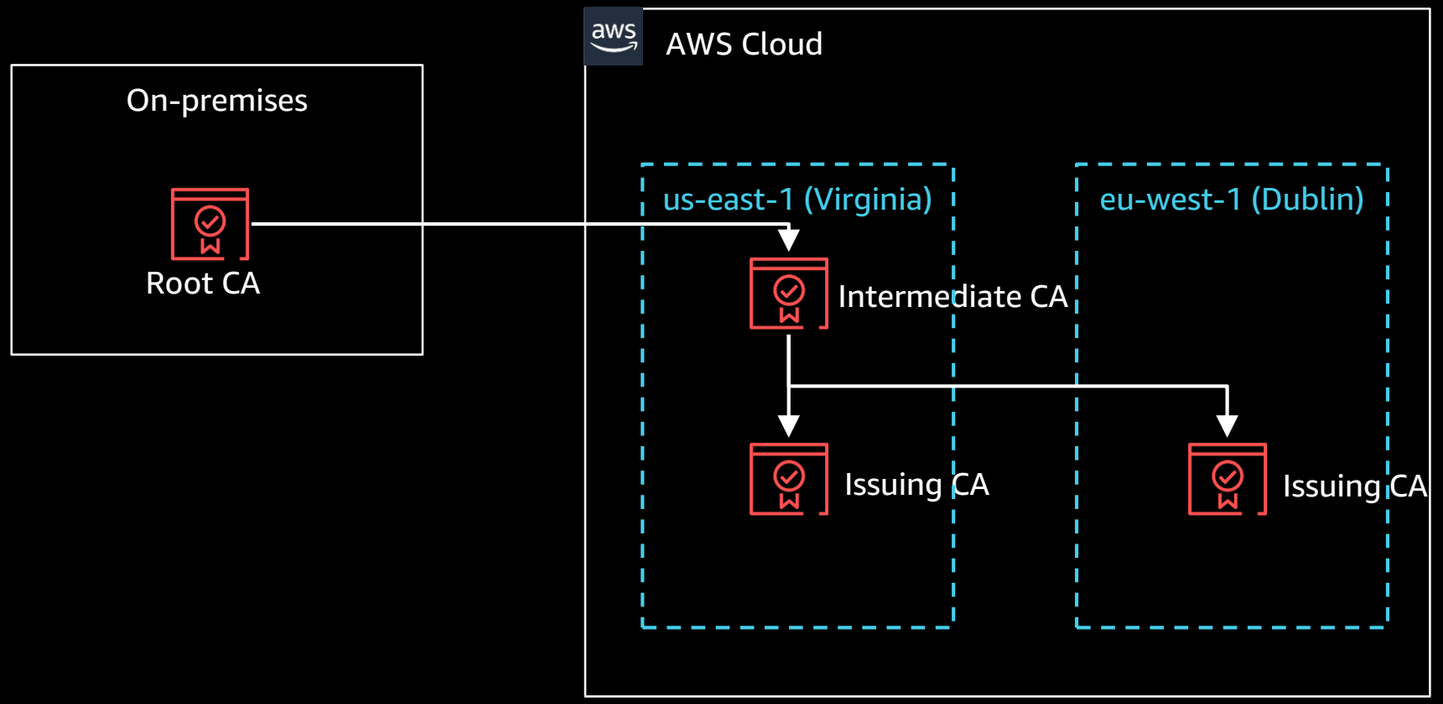


Deployment recommendations

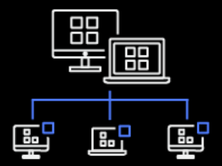


© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Deployment best practices: Hybrid deployment



Deployment best practices: Automation



Scale

Ensure PKI can handle certificate load & locations



Rapid delivery

API, CloudFormation, and similar build tools



Reliability

PKI down can result in service down



Speed

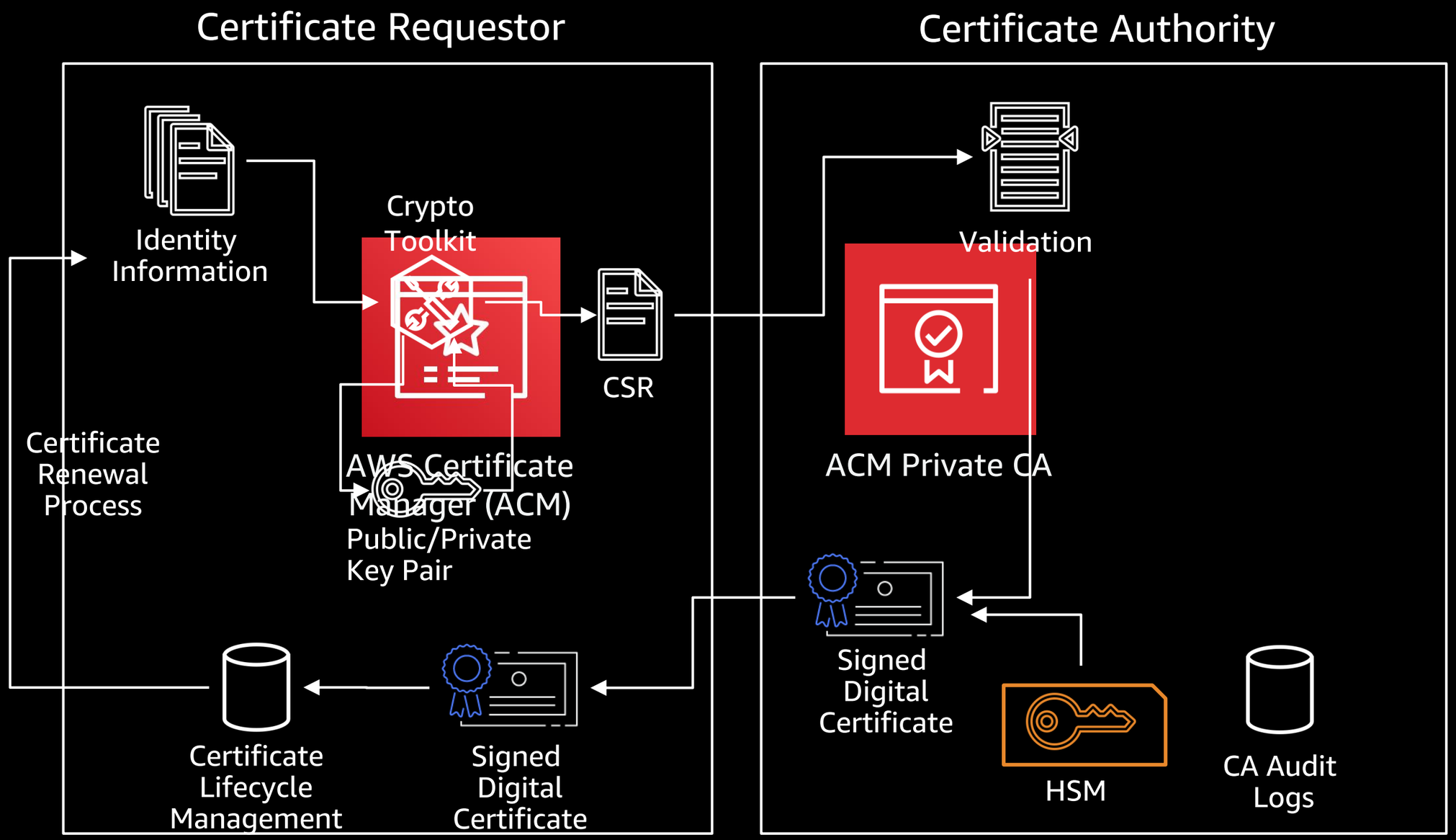
Estimate cert generation rate and scale to meet



Security

Build based on security best practices

PKI lesson learned: Secure and managed



Conclusion

BlackSky implemented TLS everywhere on its native AWS infrastructure, building certificate creation and management through a combination of ACM Private CA and an on-premises CA.

Its TLS infrastructure identifies the components in the network and allows for secure communications of the sensitive satellite imagery across the BlackSky environment.



© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Getting started

Learn about your organization’s current PKI needs

Try setting up a trial for ACM Private CA

Use ACM to issue a public or private certificate



© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Where can you find more information

AWS blog “How to host and manage an entire private certificate infrastructure in AWS”	https://aws.amazon.com/blogs/security/how-to-host-and-manage-an-entire-private-certificate-infrastructure-in-aws/
ACM Private CA service page	https://aws.amazon.com/certificate-manager/private-certificate-authority/
ACM service page	https://aws.amazon.com/certificate-manager/?nc=sn&loc=0
ACM Private CA hands-on lab	https://github.com/aws-samples/data-protection/tree/master/usecase-7

Thank you!



AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.



Please complete the session survey

AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.