
AWS
re:Invent
NOV. 28 – DEC. 2, 2022 | LAS VEGAS, NV

SEC334

Understanding the evolution of cloud-based PKI use cases

Todd Cignetti

GM, AWS Private Certificate Authority
AWS

Param Sharma

Principal Software Engineer, AWS Private Certificate Authority
AWS

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

What we'll cover

Introduction

PKI 101

Cloud-based PKI use cases

Discussion and Q&A

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

What is an X.509 certificate?



- Allow web browsers to identify and establish encrypted network connections
- Used within a cryptographic system known as a public key infrastructure (PKI)

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            f2:16:ad:85:d8:42:d1:8a:3f:33:fa:cc:c8:50:a8:9e
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: O=Example CA
        Validity
            Not Before: Jan 30 18:46:53 2018 GMT
            Not After : Jan 31 19:46:53 2018 GMT
        Subject: C=US, ST=VA, L=Herndon, O=Amazon, OU=AWS, CN=example.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:ba:a6:8a:aa:91:0b:63:e8:08:de:ca:e7:59:a4:
                    69:4c:e9:ea:26:04:d5:31:54:f5:ec:cb:4e:af:27:
                    ...
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            X509v3 Authority Key Identifier:
                keyid:84:8C:AC:03:A2:38:D9:B6:81:7C:DF:F1:95:C3:28:31:D5:F7:88:42
            X509v3 Subject Key Identifier:
                97:06:15:F1:EA:EC:07:83:4C:19:A9:2F:AF:BA:BB:FC:B2:3B:55:D8
            X509v3 Key Usage: critical
                Digital Signature, Key Encipherment
            X509v3 Extended Key Usage:
                TLS Web Server Authentication, TLS Web Client Authentication
            X509v3 CRL Distribution Points:
                Full Name:
                  URI:http://example.com/crl

    Signature Algorithm: sha256WithRSAEncryption
         69:03:15:0c:fb:a9:39:a3:30:63:b2:d4:fb:cc:8f:48:a3:46:
         69:60:a7:33:4a:f4:74:88:c6:b6:b6:b8:ab:32:c2:a0:98:c6:
```

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            f2:16:ad:85:d8:42:d1:8a:3f:33:fa:cc:c8:50:a8:9e
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: O=Example CA
        Validity
            Not Before: Jan 30 18:46:53 2018 GMT
            Not After : Jan 31 19:46:53 2018 GMT
        Subject: C=US, ST=VA, L=Herndon, O=Amazon, OU=AWS, CN=example.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:ba:a6:8a:aa:91:0b:63:e8:08:de:ca:e7:59:a4:
                    69:4c:e9:ea:26:04:d5:31:54:f5:ec:cb:4e:af:27:
                    ...
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            X509v3 Authority Key Identifier:
                keyid:84:8C:AC:03:A2:38:D9:B6:81:7C:DF:F1:95:C3:28:31:D5:F7:88:42
            X509v3 Subject Key Identifier:
                97:06:15:F1:EA:EC:07:83:4C:19:A9:2F:AF:BA:BB:FC:B2:3B:55:D8
            X509v3 Key Usage: critical
                Digital Signature, Key Encipherment
            X509v3 Extended Key Usage:
                TLS Web Server Authentication, TLS Web Client Authentication
            X509v3 CRL Distribution Points:
                Full Name:
                  URI:http://example.com/crl

    Signature Algorithm: sha256WithRSAEncryption
         69:03:15:0c:fb:a9:39:a3:30:63:b2:d4:fb:cc:8f:48:a3:46:
         69:60:a7:33:4a:f4:74:88:c6:b6:b6:b8:ab:32:c2:a0:98:c6:
```

aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Public vs. private



Public

- Commercial certificate authority
- Certificate trust already included
- Generally SSL/TLS certificates
- Certificates require domain validation

Private

- Self-managed certificate authority
- Self-managed certificate trust
- Range of certificate types and options
- No validation required

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

What is the role of private certificates?

Issue certificates to encrypt data in transit (TLS) + identify and authenticate endpoints



Certificates provide a unique digital identity to endpoints

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

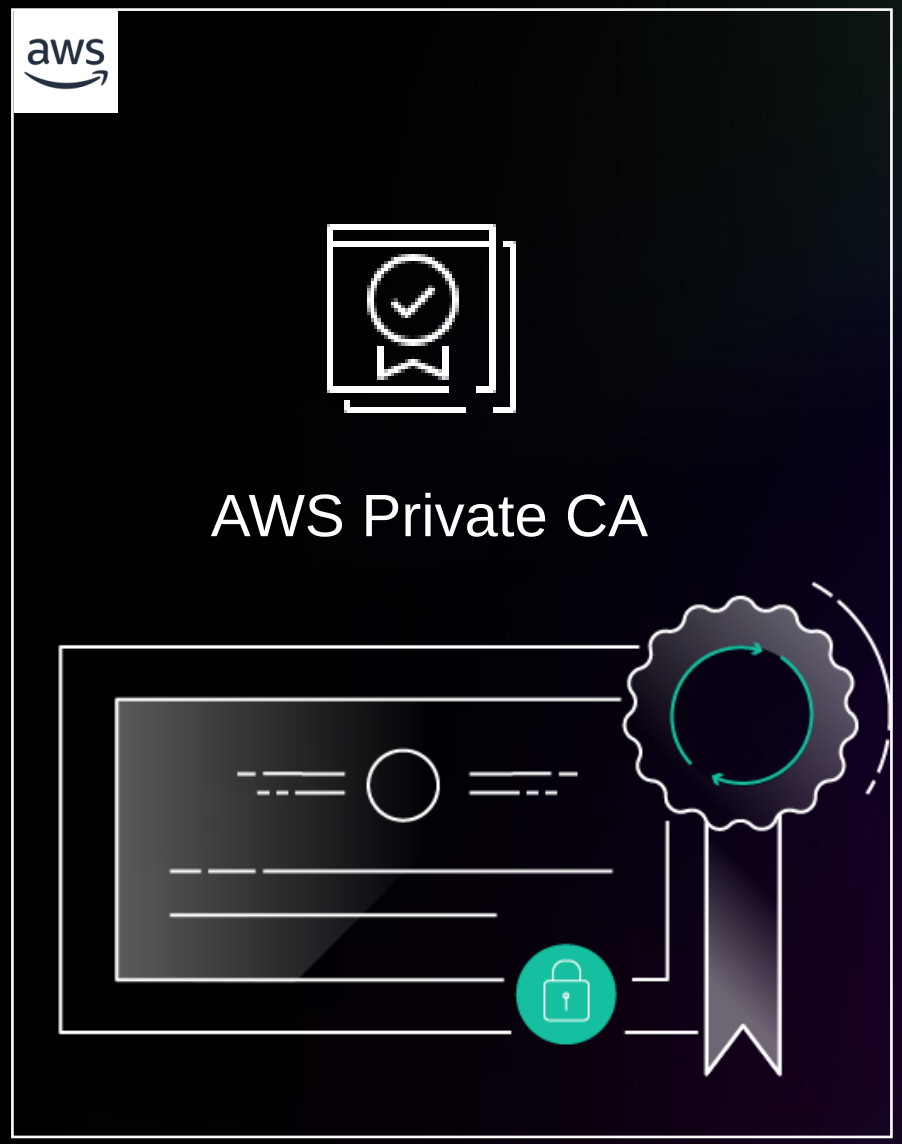
Evolution of cloud PKI: Drivers

- Migration from data centers and traditional firewalled infrastructure
- Evolving security and application architectures
  - Zero trust
  - Service mesh, microservices, and distributed applications
  - From long to short lifetime resources (e.g., servers → containers)
    - Need high capacity and high availability
  - Certificate-based authentication
  - Secure endpoint identification and TLS connections between endpoints
- IoT
  - Scale, customization, high availability, and/or bulk issuance

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Evolution of use cases



AWS resources

- Implement end-to-end encryption to AWS resources or on-premises servers

IOT and devices apps

- Issue certificates for IoT or manufactured devices

Service mesh and containers

- Provide real-time certificates for service meshes and container workloads

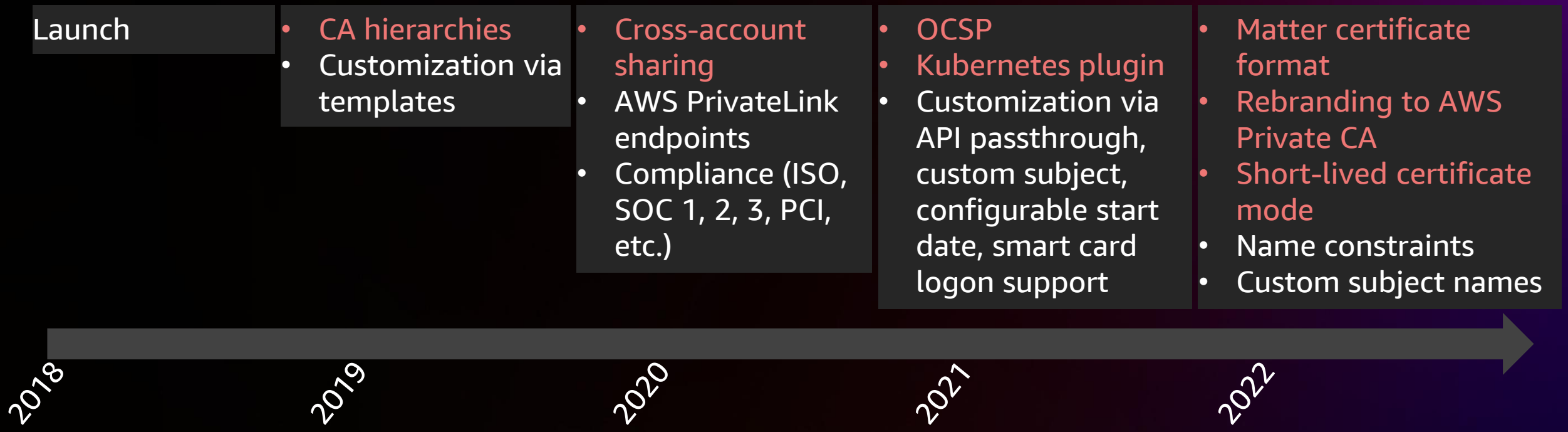
Identity

- Issue identity certificates for devices, machines, and users

aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Evolution of AWS Private CA

- AWS Private CA launched in April 2018
  - Secure, scalable, customizable, high-availability SDKs and API-based automation
  - Subordinate CAs, CRL-based revocation, audit reports, FIPS 140-2 protected CA keys



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Conversation starters

- CA hierarchies
- On-premises vs. cloud-based service
- Revocation
  - CRLs
  - OCSP
- Use cases
  - Containers
  - Hosts/instances
  - IoT
  - Matter PKI
  - Service meshes
- Certificate formats and customization
  - Matter device IDs
  - Service mesh IDs (SPIFFE id)
  - Name constraints
  - Custom extensions and subject names
- Short-lived certificates for AuthN
  - IAM Roles Anywhere
  - Amazon AppStream 2.0
  - Amazon WorkSpaces

aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Thank you!



Please complete the session survey in the **mobile app**

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.