AWS Certificate Manager Private Certificate Authority

AWS Private Certificate Authority Documentation

API Version 2017-08-22

AWS Certificate Manager Private Certificate Authority: AWS Private Certificate Authority Documentation

Table of Contents

Welcome

You can use the ACM PCA API to create a private certificate authority (CA). You must first call the CreateCertificateAuthority (p. 3) operation. If successful, the operation returns an Amazon Resource Name (ARN) for your private CA. Use this ARN as input to the GetCertificateAuthorityCsr (p. 29) operation to retrieve the certificate signing request (CSR) for your private CA certificate. Sign the CSR using the root or an intermediate CA in your on-premises PKI hierarchy, and call the ImportCertificateAuthorityCertificate (p. 32) to import your signed private CA certificate into ACM PCA.

Use your private CA to issue and revoke certificates. These are private certificates that identify and secure client computers, servers, applications, services, devices, and users over SSLS/TLS connections within your organization. Call the IssueCertificate (p. 35) operation to issue a certificate. Call the RevokeCertificate (p. 50) operation to revoke a certificate.

> **Note**
> Certificates issued by your private CA can be trusted only within your organization, not publicly.

Your private CA can optionally create a certificate revocation list (CRL) to track the certificates you revoke. To create a CRL, you must specify a RevocationConfiguration (p. 73) object when you call the CreateCertificateAuthority (p. 3) operation. ACM PCA writes the CRL to an S3 bucket that you specify. You must specify a bucket policy that grants ACM PCA write permission.

You can also call the CreateCertificateAuthorityAuditReport (p. 8) to create an optional audit report that lists every time the CA private key is used. The private key is used for signing when the **IssueCertificate** or **RevokeCertificate** operation is called.

This document was last published on October 11, 2018.

Actions

The following actions are supported:

CreateCertificateAuthority

Creates a private subordinate certificate authority (CA). You must specify the CA configuration, the revocation configuration, the CA type, and an optional idempotency token. The CA configuration specifies the name of the algorithm and key size to be used to create the CA private key, the type of signing algorithm that the CA uses to sign, and X.500 subject information. The CRL (certificate revocation list) configuration specifies the CRL expiration period in days (the validity period of the CRL), the Amazon S3 bucket that will contain the CRL, and a CNAME alias for the S3 bucket that is included in certificates issued by the CA. If successful, this operation returns the Amazon Resource Name (ARN) of the CA.

Request Syntax

```
{
   "CertificateAuthorityConfiguration": {
      "KeyAlgorithm": "string",
      "SigningAlgorithm": "string",
      "Subject": {
         "CommonName": "string",
         "Country": "string",
         "DistinguishedNameQualifier": "string",
         "GenerationQualifier": "string",
         "GivenName": "string",
         "Initials": "string",
         "Locality": "string",
         "Organization": "string",
         "OrganizationalUnit": "string",
         "Pseudonym": "string",
         "SerialNumber": "string",
         "State": "string",
         "Surname": "string",
         "Title": "string"
      }
   },
   "CertificateAuthorityType": "string",
   "IdempotencyToken": "string",
   "RevocationConfiguration": {
      "CrlConfiguration": {
         "CustomCname": "string",
         "Enabled": boolean,
         "ExpirationInDays": number,
         "S3BucketName": "string"
      }
   },
   "Tags": [
      {
         "Key": "string",
         "Value": "string"
      }
   ]
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 76).

The request accepts the following data in JSON format.

CertificateAuthorityConfiguration (p. 3)

Name and bit size of the private key algorithm, the name of the signing algorithm, and X.500 certificate subject information.

Type: CertificateAuthorityConfiguration (p. 69) object

Required: Yes

CertificateAuthorityType (p. 3)

The type of the certificate authority. Currently, this must be **SUBORDINATE**.

Type: String

Valid Values: `SUBORDINATE`

Required: Yes

IdempotencyToken (p. 3)

Alphanumeric string that can be used to distinguish between calls to **CreateCertificateAuthority**. Idempotency tokens time out after five minutes. Therefore, if you call **CreateCertificateAuthority** multiple times with the same idempotency token within a five minute period, ACM PCA recognizes that you are requesting only one certificate. As a result, ACM PCA issues only one. If you change the idempotency token for each call, however, ACM PCA recognizes that you are requesting multiple certificates.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 36.

Pattern: `[\u0009\u000A\u000D\u0020-\u00FF]*`

Required: No

RevocationConfiguration (p. 3)

Contains a Boolean value that you can use to enable a certification revocation list (CRL) for the CA, the name of the S3 bucket to which ACM PCA will write the CRL, and an optional CNAME alias that you can use to hide the name of your bucket in the **CRL Distribution Points** extension of your CA certificate. For more information, see the CrlConfiguration (p. 70) structure.

Type: RevocationConfiguration (p. 73) object

Required: No

Tags (p. 3)

Type: Array of Tag (p. 74) objects

Array Members: Minimum number of 1 item. Maximum number of 50 items.

Required: No

Response Syntax

```
{
   "CertificateAuthorityArn": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

CertificateAuthorityArn (p. 4)

If successful, the Amazon Resource Name (ARN) of the certificate authority (CA). This is of the form:

`arn:aws:acm-pca:`*`region`*`:`*`account`*`:certificate-authority/`*`12345678-1234-1234-1234-123456789012`* .

Type: String

Length Constraints: Minimum length of 5. Maximum length of 200.

Pattern: `arn:[\w+=/,.@-]+:[\w+=/,.@-]+:[\w+=/,.@-]*:[0-9]+:[\w+=,.@-]+(/[\w+=/,.@-]+)*`

Errors

For information about the errors that are common to all actions, see Common Errors (p. 78).

InvalidArgsException

One or more of the specified arguments was not valid.

HTTP Status Code: 400

InvalidPolicyException

The S3 bucket policy is not valid. The policy must give ACM PCA rights to read from and write to the bucket and find the bucket location.

HTTP Status Code: 400

InvalidTagException

The tag associated with the CA is not valid. The invalid argument is contained in the message field.

HTTP Status Code: 400

LimitExceededException

An ACM PCA limit has been exceeded. See the exception message returned to determine the limit that was exceeded.

HTTP Status Code: 400

Examples

Example

Sample Request

```
POST / HTTP/1.1
Host: acm-pca.amazonaws.com
```

```
Accept-Encoding: identity
Content-Length: 512
X-Amz-Target: ACMPrivateCA.CreateCertificateAuthority
X-Amz-Date: 20180515T165448Z
User-Agent: aws-cli/1.15.4 Python/2.7.9 Windows/8 botocore/1.10.4
Content-Type: application/x-amz-json-1.1
Authorization: AWS4-HMAC-SHA256 Credential=AWS_Access_Key_ID/20180515/AWS_Region/acm-pca/
aws4_request,
SignedHeaders=content-type;host;x-amz-date;x-amz-target,
Signature=6fc58aaf789659cb4e0dd0ba484a2562d982b6b8edd56ea0c5c94c2af9aeafbe

{
  "IdempotencyToken": "98256344",
  "CertificateAuthorityConfiguration": {
    "KeyAlgorithm": "RSA_2048",
    "SigningAlgorithm": "SHA256WITHRSA",
    "Subject": {
      "Locality": "Seattle",
      "Country": "US",
      "CommonName": "www.example.com",
      "State": "WA",
      "Organization": "Example Ltd.",
      "OrganizationalUnit": "Corporate"
    }
  },
  "CertificateAuthorityType": "SUBORDINATE",
  "RevocationConfiguration": {
    "CrlConfiguration": {
      "CustomCname": "CRL",
      "Enabled": true,
      "S3BucketName": "your-crl-bucket-name",
      "ExpirationInDays": 3650
    }
  }
}
```

Example

Sample Response

```
HTTP/1.1 200 OK
Date: Tue, 15 May 2018 16:54:56 GMT
Content-Type: application/x-amz-json-1.1
Content-Length: 127
x-amzn-RequestId: eacb346a-d80b-4be6-a1b2-1732c3ae3c38
Connection: keep-alive

{
  "CertificateAuthorityArn": "arn:aws:acm-pca:region:account:certificate-
authority/12345678-1234-1234-1234-123456789012"
}
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go

- AWS SDK for Java
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V2

CreateCertificateAuthorityAuditReport

Creates an audit report that lists every time that the your CA private key is used. The report is saved in the Amazon S3 bucket that you specify on input. The IssueCertificate (p. 35) and RevokeCertificate (p. 50) operations use the private key. You can generate a new report every 30 minutes.

Request Syntax

```
{
   "AuditReportResponseFormat": "string",
   "CertificateAuthorityArn": "string",
   "S3BucketName": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 76).

The request accepts the following data in JSON format.

AuditReportResponseFormat (p. 8)

Format in which to create the report. This can be either **JSON** or **CSV**.

Type: String

Valid Values: `JSON | CSV`

Required: Yes

CertificateAuthorityArn (p. 8)

Amazon Resource Name (ARN) of the CA to be audited. This is of the form:

`arn:aws:acm-pca:`*`region`*`:`*`account`*`:certificate-authority/`*`12345678-1234-1234-1234-123456789012`* .

Type: String

Length Constraints: Minimum length of 5. Maximum length of 200.

Pattern: `arn:[\w+=/,.@-]+:[\w+=/,.@-]+:[\w+=/,.@-]*:[0-9]+:[\w+=,.@-]+(/[\w+=/,.@-]+)*`

Required: Yes

S3BucketName (p. 8)

Name of the S3 bucket that will contain the audit report.

Type: String

Required: Yes

Response Syntax

```
{
```

```
   "AuditReportId": "string",
   "S3Key": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

AuditReportId (p. 8)

An alphanumeric string that contains a report identifier.

Type: String

Length Constraints: Fixed length of 36.

Pattern: `[a-z0-9]{8}-[a-z0-9]{4}-[a-z0-9]{4}-[a-z0-9]{4}-[a-z0-9]{12}`

S3Key (p. 8)

The **key** that uniquely identifies the report file in your S3 bucket.

Type: String

Errors

For information about the errors that are common to all actions, see Common Errors (p. 78).

InvalidArgsException

One or more of the specified arguments was not valid.

HTTP Status Code: 400

InvalidArnException

The requested Amazon Resource Name (ARN) does not refer to an existing resource.

HTTP Status Code: 400

InvalidStateException

The private CA is in a state during which a report cannot be generated.

HTTP Status Code: 400

RequestFailedException

The request has failed for an unspecified reason.

HTTP Status Code: 400

RequestInProgressException

Your request is already in progress.

HTTP Status Code: 400

ResourceNotFoundException

A resource such as a private CA, S3 bucket, certificate, or audit report cannot be found.

HTTP Status Code: 400

Examples

Example

Sample Request

```
POST / HTTP/1.1
Host: acm-pca.amazonaws.com
Accept-Encoding: identity
Content-Length: 216
X-Amz-Target: ACMPrivateCA.CreateCertificateAuthorityAuditReport
X-Amz-Date: 20180226T184819Z
User-Agent: aws-cli/1.14.28 Python/2.7.9 Windows/8 botocore/1.8.32
Content-Type: application/x-amz-json-1.1
Authorization: AWS4-HMAC-SHA256 Credential=AWS_Access_Key_ID/20180226/AWS_Region/acm-pca/
aws4_request,
SignedHeaders=content-type;host;x-amz-date;x-amz-target,
Signature=62380db816189148e510734f0ef2bfec08248fb3f447f64d740f31757e1beda0

{
  "AuditReportResponseFormat": "JSON",
  "S3BucketName": "your-bucket-name",
  "CertificateAuthorityArn": "arn:aws:acm-pca:region:account:certificate-
authority/12345678-1234-1234-1234-123456789012"
}
```

Example

Sample Response

```
HTTP/1.1 200 OK
Date: Tue, 15 May 2018 16:29:03 GMT
Content-Type: application/x-amz-json-1.1
Content-Length: 158
x-amzn-RequestId: e8516078-ff66-4e2a-bc38-eb1aaae2d886
Connection: keep-alive

{
  "AuditReportId": "9654b603-d6a9-4c57-952a-ebcc95631fab",
  "S3Key": "audit-reportPCA_ID/9654b603-d6a9-4c57-952a-ebcc95631fab.json"
}
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java
- AWS SDK for JavaScript
- AWS SDK for PHP V3

- AWS SDK for Python
- AWS SDK for Ruby V2

DeleteCertificateAuthority

Deletes a private certificate authority (CA). You must provide the ARN (Amazon Resource Name) of the private CA that you want to delete. You can find the ARN by calling the ListCertificateAuthorities (p. 39) operation. Before you can delete a CA, you must disable it. Call the UpdateCertificateAuthority (p. 59) operation and set the **CertificateAuthorityStatus** parameter to `DISABLED`.

Additionally, you can delete a CA if you are waiting for it to be created (the **Status** field of the CertificateAuthority (p. 66) is `CREATING`). You can also delete it if the CA has been created but you haven't yet imported the signed certificate (the **Status** is `PENDING_CERTIFICATE`) into ACM PCA.

If the CA is in one of the aforementioned states and you call DeleteCertificateAuthority (p. 12), the CA's status changes to `DELETED`. However, the CA won't be permentantly deleted until the restoration period has passed. By default, if you do not set the `PermanentDeletionTimeInDays` parameter, the CA remains restorable for 30 days. You can set the parameter from 7 to 30 days. The DescribeCertificateAuthority (p. 15) operation returns the time remaining in the restoration window of a Private CA in the `DELETED` state. To restore an eligable CA, call the RestoreCertificateAuthority (p. 47) operation.

Request Syntax

```
{
   "CertificateAuthorityArn": "string",
   "PermanentDeletionTimeInDays": number
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 76).

The request accepts the following data in JSON format.

CertificateAuthorityArn (p. 12)

The Amazon Resource Name (ARN) that was returned when you called CreateCertificateAuthority (p. 3). This must have the following form:

`arn:aws:acm-pca:`*`region`*`:`*`account`*`:certificate-authority/`*`12345678-1234-1234-1234-123456789012`*` .`

Type: String

Length Constraints: Minimum length of 5. Maximum length of 200.

Pattern: `arn:[\w+=/,.@-]+:[\w+=/,.@-]+:[\w+=/,.@-]*:[0-9]+:[\w+=,.@-]+(/[\w+=/,.@-]+)*`

Required: Yes

PermanentDeletionTimeInDays (p. 12)

The number of days to make a CA restorable after it has been deleted. This can be anywhere from 7 to 30 days, with 30 being the default.

Type: Integer

Valid Range: Minimum value of 7. Maximum value of 30.

Required: No

Response Elements

If the action is successful, the service sends back an HTTP 200 response with an empty HTTP body.

Errors

For information about the errors that are common to all actions, see Common Errors (p. 78).

ConcurrentModificationException

A previous update to your private CA is still ongoing.

HTTP Status Code: 400

InvalidArnException

The requested Amazon Resource Name (ARN) does not refer to an existing resource.

HTTP Status Code: 400

InvalidStateException

The private CA is in a state during which a report cannot be generated.

HTTP Status Code: 400

ResourceNotFoundException

A resource such as a private CA, S3 bucket, certificate, or audit report cannot be found.

HTTP Status Code: 400

Examples

Example

Sample Request

```
POST / HTTP/1.1
Host: acm-pca.amazonaws.com
Accept-Encoding: identity
Content-Length: 163
X-Amz-Target: ACMPrivateCA.DeleteCertificateAuthority
X-Amz-Date: 20180515T160248Z
User-Agent: aws-cli/1.15.4 Python/2.7.9 Windows/8 botocore/1.10.4
Content-Type: application/x-amz-json-1.1
Authorization: AWS4-HMAC-SHA256 Credential=AWS_Access_Key_ID/20180515/AWS_Region/acm-pca/
aws4_request,
SignedHeaders=content-type;host;x-amz-date;x-amz-target,
Signature=8f7e5b799989c607156141bc6856eb48acd45def7eecd2b2b7fbaa11f34d7bd1

{"PermanentDeletionTimeInDays": 17, "CertificateAuthorityArn": "arn:aws:acm-pca:us-
west-2:493619779192:certificate-authority/4ce5e894-a076-4ed8-9d5c-42afbd4cbf88"}
```

Example

Sample Response

```
This function does not return a value.
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V2

DescribeCertificateAuthority

Lists information about your private certificate authority (CA). You specify the private CA on input by its ARN (Amazon Resource Name). The output contains the status of your CA. This can be any of the following:

- `CREATING` - ACM PCA is creating your private certificate authority.
- `PENDING_CERTIFICATE` - The certificate is pending. You must use your on-premises root or subordinate CA to sign your private CA CSR and then import it into PCA.
- `ACTIVE` - Your private CA is active.
- `DISABLED` - Your private CA has been disabled.
- `EXPIRED` - Your private CA certificate has expired.
- `FAILED` - Your private CA has failed. Your CA can fail because of problems such a network outage or backend AWS failure or other errors. A failed CA can never return to the pending state. You must create a new CA.
- `DELETED` - Your private CA is within the restoration period, after which it is permanently deleted. The length of time remaining in the CA's restoration period is also included in this operation's output.

Request Syntax

```
{
   "CertificateAuthorityArn": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 76).

The request accepts the following data in JSON format.

CertificateAuthorityArn (p. 15)

The Amazon Resource Name (ARN) that was returned when you called CreateCertificateAuthority (p. 3). This must be of the form:

`arn:aws:acm-pca:region:account:certificate-authority/12345678-1234-1234-1234-123456789012` .

Type: String

Length Constraints: Minimum length of 5. Maximum length of 200.

Pattern: `arn:[\w+=/,.@-]+:[\w+=/,.@-]+:[\w+=/,.@-]*:[0-9]+:[\w+=,.@-]+(/[\w+=/,.@-]+)*`

Required: Yes

Response Syntax

```
{
```

```
   "CertificateAuthority": {
      "Arn": "string",
      "CertificateAuthorityConfiguration": {
         "KeyAlgorithm": "string",
         "SigningAlgorithm": "string",
         "Subject": {
            "CommonName": "string",
            "Country": "string",
            "DistinguishedNameQualifier": "string",
            "GenerationQualifier": "string",
            "GivenName": "string",
            "Initials": "string",
            "Locality": "string",
            "Organization": "string",
            "OrganizationalUnit": "string",
            "Pseudonym": "string",
            "SerialNumber": "string",
            "State": "string",
            "Surname": "string",
            "Title": "string"
         }
      },
      "CreatedAt": number,
      "FailureReason": "string",
      "LastStateChangeAt": number,
      "NotAfter": number,
      "NotBefore": number,
      "RestorableUntil": number,
      "RevocationConfiguration": {
         "CrlConfiguration": {
            "CustomCname": "string",
            "Enabled": boolean,
            "ExpirationInDays": number,
            "S3BucketName": "string"
         }
      },
      "Serial": "string",
      "Status": "string",
      "Type": "string"
   }
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

CertificateAuthority (p. 15)

A CertificateAuthority (p. 66) structure that contains information about your private CA.

Type: CertificateAuthority (p. 66) object

Errors

For information about the errors that are common to all actions, see Common Errors (p. 78).

InvalidArnException

The requested Amazon Resource Name (ARN) does not refer to an existing resource.

HTTP Status Code: 400

ResourceNotFoundException

A resource such as a private CA, S3 bucket, certificate, or audit report cannot be found.

HTTP Status Code: 400

Examples

Example

Sample Request

```
POST / HTTP/1.1
Host: acm-pca.amazonaws.com
Accept-Encoding: identity
Content-Length: 128
X-Amz-Target: ACMPrivateCA.DescribeCertificateAuthority
X-Amz-Date: 20180226T175919Z
User-Agent: aws-cli/1.14.28 Python/2.7.9 Windows/8 botocore/1.8.32
Content-Type: application/x-amz-json-1.1
Authorization: AWS4-HMAC-SHA256 Credential=Access_Key_ID/20180226/AWS_Region/acm-pca/
aws4_request,
SignedHeaders=content-type;host;x-amz-date;x-amz-target,
Signature=953a014106627a76d91f55fd86bb1149bf65d578886bf2371aa4c73c56e16a1d

{"CertificateAuthorityArn": "arn:aws:acm-pca:region:account:certificate-
authority/12345678-1234-1234-1234-123456789012"}
```

Example

Sample Response

```
HTTP/1.1 200 OK
Date: Tue, 15 May 2018 17:09:51 GMT
Content-Type: application/x-amz-json-1.1
Content-Length: 713
x-amzn-RequestId: 8d51e9ff-8ae9-4ccf-816a-8e7d9c3dc1af
Connection: keep-alive

{
  "CertificateAuthority": {
    "Arn": "arn:aws:acm-pca:gh:account:certificate-
authority/12345678-1234-1234-1234-123456789012",
    "CertificateAuthorityConfiguration": {
      "KeyAlgorithm": "RSA_2048",
      "SigningAlgorithm": "SHA256WITHRSA",
      "Subject": {
        "CommonName": "www.example.com",
        "Country": "US",
        "Locality": "Seattle",
        "Organization": "Example Company",
        "OrganizationalUnit": "Corporate",
        "State": "WA"
      }
    },
    "CreatedAt": 1.516130652887E9,
    "LastStateChangeAt": 1.516130652887E9,
    "NotAfter": 1.831494803E9,
```

```
    "NotBefore": 1.516134803E9,
    "RevocationConfiguration": {
      "CrlConfiguration": {
        "CustomCname": "http://somename.crl",
        "Enabled": true,
        "ExpirationInDays": 3650,
        "S3BucketName": "your-bucket-name"
      }
    },
    "Serial": "4118",
    "Status": "ACTIVE",
    "Type": "SUBORDINATE"
  }
}
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V2

DescribeCertificateAuthorityAuditReport

Lists information about a specific audit report created by calling the CreateCertificateAuthorityAuditReport (p. 8) operation. Audit information is created every time the certificate authority (CA) private key is used. The private key is used when you call the IssueCertificate (p. 35) operation or the RevokeCertificate (p. 50) operation.

Request Syntax

```
{
   "AuditReportId": "string",
   "CertificateAuthorityArn": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 76).

The request accepts the following data in JSON format.

AuditReportId (p. 19)

The report ID returned by calling the CreateCertificateAuthorityAuditReport (p. 8) operation.

Type: String

Length Constraints: Fixed length of 36.

Pattern: `[a-z0-9]{8}-[a-z0-9]{4}-[a-z0-9]{4}-[a-z0-9]{4}-[a-z0-9]{12}`

Required: Yes

CertificateAuthorityArn (p. 19)

The Amazon Resource Name (ARN) of the private CA. This must be of the form:

`arn:aws:acm-pca:`*`region`*`:`*`account`*`:certificate-authority/`*`12345678-1234-1234-1234-123456789012`* .

Type: String

Length Constraints: Minimum length of 5. Maximum length of 200.

Pattern: `arn:[\w+=/,.@-]+:[\w+=/,.@-]+:[\w+=/,.@-]*:[0-9]+:[\w+=,.@-]+(/[\w+=/,.@-]+)*`

Required: Yes

Response Syntax

```
{
   "AuditReportStatus": "string",
   "CreatedAt": number,
   "S3BucketName": "string",
   "S3Key": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

AuditReportStatus (p. 19)

Specifies whether report creation is in progress, has succeeded, or has failed.

Type: String

Valid Values: `CREATING | SUCCESS | FAILED`

CreatedAt (p. 19)

The date and time at which the report was created.

Type: Timestamp

S3BucketName (p. 19)

Name of the S3 bucket that contains the report.

Type: String

S3Key (p. 19)

S3 **key** that uniquely identifies the report file in your S3 bucket.

Type: String

Errors

For information about the errors that are common to all actions, see Common Errors (p. 78).

InvalidArgsException

One or more of the specified arguments was not valid.

HTTP Status Code: 400

InvalidArnException

The requested Amazon Resource Name (ARN) does not refer to an existing resource.

HTTP Status Code: 400

ResourceNotFoundException

A resource such as a private CA, S3 bucket, certificate, or audit report cannot be found.

HTTP Status Code: 400

Examples

Example

Sample Request

```
POST / HTTP/1.1
```

```
Host: acm-pca.amazonaws.com
Accept-Encoding: identity
Content-Length: 185
X-Amz-Target: ACMPrivateCA.DescribeCertificateAuthorityAuditReport
X-Amz-Date: 20180226T185916Z
User-Agent: aws-cli/1.14.28 Python/2.7.9 Windows/8 botocore/1.8.32
Content-Type: application/x-amz-json-1.1
Authorization: AWS4-HMAC-SHA256 Credential=AWS_Access_Key_ID/20180226/AWS_Region/acm-pca/
aws4_request,
SignedHeaders=content-type;host;x-amz-date;x-amz-target,
Signature=96531073ea22cc7057267543f332911b97a5db830dca85a74a7324c9737cee7a

{
  "AuditReportId": "11111111-2222-3333-4444-555555555555",
  "CertificateAuthorityArn": "arn:aws:acm-pca:region:account:certificate-
authority/12345678-1234-1234-1234-123456789012"
}
```

Example

Sample Response

```
HTTP/1.1 200 OK
Date: Tue, 15 May 2018 16:33:26 GMT
Content-Type: application/xget-amz-json-1.1
Content-Length: 211
x-amzn-RequestId: 3af6a588-856c-48eb-81ab-f2f08fbc618c
Connection: keep-alive

{
  "AuditReportStatus": "SUCCESS",
  "CreatedAt": 1.526401743081E9,
  "S3BucketName": "your-bucket-name",
  "S3Key": "audit-report/PCA_ID/Audit_Report_ID.json"
}
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V2

GetCertificate

Retrieves a certificate from your private CA. The ARN of the certificate is returned when you call the IssueCertificate (p. 35) operation. You must specify both the ARN of your private CA and the ARN of the issued certificate when calling the **GetCertificate** operation. You can retrieve the certificate if it is in the **ISSUED** state. You can call the CreateCertificateAuthorityAuditReport (p. 8) operation to create a report that contains information about all of the certificates issued and revoked by your private CA.

Request Syntax

```
{
   "CertificateArn": "string",
   "CertificateAuthorityArn": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 76).

The request accepts the following data in JSON format.

CertificateArn (p. 22)

The ARN of the issued certificate. The ARN contains the certificate serial number and must be in the following form:

`arn:aws:acm-pca:`*`region`*`:`*`account`*`:certificate-authority/`*`12345678-1234-1234-1234-123456789012`*`/certificate/`*`286535153982981100925020015808220737245`*

Type: String

Length Constraints: Minimum length of 5. Maximum length of 200.

Pattern: `arn:[\w+=/,.@-]+:[\w+=/,.@-]+:[\w+=/,.@-]*:[0-9]+:[\w+=,.@-]+(/[\w+=/,.@-]+)*`

Required: Yes

CertificateAuthorityArn (p. 22)

The Amazon Resource Name (ARN) that was returned when you called CreateCertificateAuthority (p. 3). This must be of the form:

`arn:aws:acm-pca:`*`region`*`:`*`account`*`:certificate-authority/`*`12345678-1234-1234-1234-123456789012`*` .`

Type: String

Length Constraints: Minimum length of 5. Maximum length of 200.

Pattern: `arn:[\w+=/,.@-]+:[\w+=/,.@-]+:[\w+=/,.@-]*:[0-9]+:[\w+=,.@-]+(/[\w+=/,.@-]+)*`

Required: Yes

Response Syntax

```
{
   "Certificate": "string",
   "CertificateChain": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

Certificate (p. 23)

The base64 PEM-encoded certificate specified by the `CertificateArn` parameter.

Type: String

CertificateChain (p. 23)

The base64 PEM-encoded certificate chain that chains up to the on-premises root CA certificate that you used to sign your private CA certificate.

Type: String

Errors

For information about the errors that are common to all actions, see Common Errors (p. 78).

InvalidArnException

The requested Amazon Resource Name (ARN) does not refer to an existing resource.

HTTP Status Code: 400

InvalidStateException

The private CA is in a state during which a report cannot be generated.

HTTP Status Code: 400

RequestFailedException

The request has failed for an unspecified reason.

HTTP Status Code: 400

RequestInProgressException

Your request is already in progress.

HTTP Status Code: 400

ResourceNotFoundException

A resource such as a private CA, S3 bucket, certificate, or audit report cannot be found.

HTTP Status Code: 400

Examples

Example

Sample Request

```
POST / HTTP/1.1
Host: acm-pca.amazonaws.com
Accept-Encoding: identity
Content-Length: 292
X-Amz-Target: ACMPrivateCA.GetCertificate
X-Amz-Date: 20180226T194913Z
User-Agent: aws-cli/1.14.28 Python/2.7.9 Windows/8 botocore/1.8.32
Content-Type: application/x-amz-json-1.1
Authorization: AWS4-HMAC-SHA256 Credential=AWS_Access_Key_ID/20180226/AWS_Region/
acm-pca/aws4_request, SignedHeaders=content-type;host;x-amz-date;x-amz-target,
 Signature=4fe34fdad8c09d5b608be6f5d4f4939444dd7cdd542ec09b1002182e4ef9fcee

{
  "CertificateArn": "arn:aws:acm-pca:region:account:certificate-
authority/12345678-1234-1234-1234-123456789012/certificate/
e8cbd2bedb122329f97706bcfec990f8",
  "CertificateAuthorityArn": "arn:aws:acm-pca:region:account:certificate-
authority/12345678-1234-1234-1234-123456789012"
}
```

Example

Sample Response

```
HTTP/1.1 200 OK
Date: Tue, 15 May 2018 17:35:47 GMT
Content-Type: application/x-amz-json-1.1
Content-Length: 4184
x-amzn-RequestId: 9f537e0a-993c-4a03-8aec-0fc52c772b84
Connection: keep-alive

{
  "Certificate": "-----BEGIN CERTIFICATE----- base64-encoded certificate -----END
 CERTIFICATE-----",
  "CertificateChain": "-----BEGIN CERTIFICATE----- base64-encoded certificate -----END
 CERTIFICATE-----"
}
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java
- AWS SDK for JavaScript
- AWS SDK for PHP V3

- AWS SDK for Python
- AWS SDK for Ruby V2

GetCertificateAuthorityCertificate

Retrieves the certificate and certificate chain for your private certificate authority (CA). Both the certificate and the chain are base64 PEM-encoded. The chain does not include the CA certificate. Each certificate in the chain signs the one before it.

Request Syntax

```
{
   "CertificateAuthorityArn": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 76).

The request accepts the following data in JSON format.

CertificateAuthorityArn (p. 26)

The Amazon Resource Name (ARN) of your private CA. This is of the form:

`arn:aws:acm-pca:region:account:certificate-authority/12345678-1234-1234-1234-123456789012` .

Type: String

Length Constraints: Minimum length of 5. Maximum length of 200.

Pattern: `arn:[\w+=/,.@-]+:[\w+=/,.@-]+:[\w+=/,.@-]*:[0-9]+:[\w+=,.@-]+(/[\w+=/,.@-]+)*`

Required: Yes

Response Syntax

```
{
   "Certificate": "string",
   "CertificateChain": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

Certificate (p. 26)

Base64-encoded certificate authority (CA) certificate.

Type: String

CertificateChain (p. 26)

Base64-encoded certificate chain that includes any intermediate certificates and chains up to root on-premises certificate that you used to sign your private CA certificate. The chain does not include your private CA certificate.

Type: String

Errors

For information about the errors that are common to all actions, see Common Errors (p. 78).

InvalidArnException

The requested Amazon Resource Name (ARN) does not refer to an existing resource.

HTTP Status Code: 400

InvalidStateException

The private CA is in a state during which a report cannot be generated.

HTTP Status Code: 400

ResourceNotFoundException

A resource such as a private CA, S3 bucket, certificate, or audit report cannot be found.

HTTP Status Code: 400

Examples

Example

Sample Request

```
POST / HTTP/1.1
Host: acm-pca.amazonaws.com
Accept-Encoding: identity
Content-Length: 128
X-Amz-Target: ACMPrivateCA.GetCertificateAuthorityCertificate
X-Amz-Date: 20180226T174831Z
User-Agent: aws-cli/1.14.28 Python/2.7.9 Windows/8 botocore/1.8.32
Content-Type: application/x-amz-json-1.1
Authorization: AWS4-HMAC-SHA256 Credential=Access_Key_ID/20180226/AWS_Region/acm-pca/
aws4_request,
SignedHeaders=content-type;host;x-amz-date;x-amz-target,
Signature=2675f0e4055c234f5b6e155bd3245ca327382d47a16e0c20f2abc802e1f0eab6

{"CertificateAuthorityArn": "arn:aws:acm-pca:AWS_Region:AWS_Account:certificate-
authority/12345678-1234-1234-1234-123456789012"}
```

Example

Sample Response

```
HTTP/1.1 200 OK
```

```
Date: Tue, 15 May 2018 17:43:38 GMT
Content-Type: application/x-amz-json-1.1
Content-Length: 2552
x-amzn-RequestId: 8c607f26-6d9e-4972-a529-02cc5608c81a
Connection: keep-alive

{
  "Certificate": "-----BEGIN CERTIFICATE-----  base64-encoded certificate  -----END
 CERTIFICATE-----",
  "CertificateChain": "-----BEGIN CERTIFICATE-----  base64-encoded certificate chain  -----
END CERTIFICATE-----"
}
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V2

GetCertificateAuthorityCsr

Retrieves the certificate signing request (CSR) for your private certificate authority (CA). The CSR is created when you call the CreateCertificateAuthority (p. 3) operation. Take the CSR to your on-premises X.509 infrastructure and sign it by using your root or a subordinate CA. Then import the signed certificate back into ACM PCA by calling the ImportCertificateAuthorityCertificate (p. 32) operation. The CSR is returned as a base64 PEM-encoded string.

Request Syntax

```
{
   "CertificateAuthorityArn": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 76).

The request accepts the following data in JSON format.

CertificateAuthorityArn (p. 29)

The Amazon Resource Name (ARN) that was returned when you called the CreateCertificateAuthority (p. 3) operation. This must be of the form:

`arn:aws:acm-pca:region:account:certificate-authority/12345678-1234-1234-1234-123456789012`

Type: String

Length Constraints: Minimum length of 5. Maximum length of 200.

Pattern: `arn:[\w+=/,.@-]+:[\w+=/,.@-]+:[\w+=/,.@-]*:[0-9]+:[\w+=,.@-]+(/[\w+=/,.@-]+)*`

Required: Yes

Response Syntax

```
{
   "Csr": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

Csr (p. 29)

The base64 PEM-encoded certificate signing request (CSR) for your private CA certificate.

Type: String

Errors

For information about the errors that are common to all actions, see Common Errors (p. 78).

InvalidArnException

The requested Amazon Resource Name (ARN) does not refer to an existing resource.

HTTP Status Code: 400

InvalidStateException

The private CA is in a state during which a report cannot be generated.

HTTP Status Code: 400

RequestFailedException

The request has failed for an unspecified reason.

HTTP Status Code: 400

RequestInProgressException

Your request is already in progress.

HTTP Status Code: 400

ResourceNotFoundException

A resource such as a private CA, S3 bucket, certificate, or audit report cannot be found.

HTTP Status Code: 400

Examples

Example

Sample Request

```
POST / HTTP/1.1
Host: acm-pca.amazonaws.com
Accept-Encoding: identity
Content-Length: 128
X-Amz-Target: ACMPrivateCA.GetCertificateAuthorityCsr
X-Amz-Date: 20180226T175413Z
User-Agent: aws-cli/1.14.28 Python/2.7.9 Windows/8 botocore/1.8.32
Content-Type: application/x-amz-json-1.1
Authorization: AWS4-HMAC-SHA256 Credential=AWS_Key_ID/20180226/AWS_Region/acm-pca/
aws4_request,
SignedHeaders=content-type;host;x-amz-date;x-amz-target,
Signature=aa5f823a8637e4709fd4b06988934f4ed4f38f2541889a2f6894f09d75f8b071

{"CertificateAuthorityArn": "arn:aws:acm-pca:region:account:certificate-
authority/12345678-1234-1234-1234-123456789012"}
```

Example

Sample Response

```
HTTP/1.1 200 OK
```

```
Date: Tue, 15 May 2018 17:50:52 GMT
Content-Type: application/x-amz-json-1.1
Content-Length: 1098
x-amzn-RequestId: f96921bf-8b07-4e2a-876a-f76946e666d2
Connection: keep-alive

{
  "Csr": "-----BEGIN CERTIFICATE REQUEST----- base64-encoded CSR -----END CERTIFICATE
 REQUEST-----"
}
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V2

ImportCertificateAuthorityCertificate

Imports your signed private CA certificate into ACM PCA. Before you can call this operation, you must create the private certificate authority by calling the CreateCertificateAuthority (p. 3) operation. You must then generate a certificate signing request (CSR) by calling the GetCertificateAuthorityCsr (p. 29) operation. Take the CSR to your on-premises CA and use the root certificate or a subordinate certificate to sign it. Create a certificate chain and copy the signed certificate and the certificate chain to your working directory.

Note
Your certificate chain must not include the private CA certificate that you are importing.

Note
Your on-premises CA certificate must be the last certificate in your chain. The subordinate certificate, if any, that your root CA signed must be next to last. The subordinate certificate signed by the preceding subordinate CA must come next, and so on until your chain is built.

Note
The chain must be PEM-encoded.

Request Syntax

```
{
   "Certificate": blob,
   "CertificateAuthorityArn": "string",
   "CertificateChain": blob
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 76).

The request accepts the following data in JSON format.

Certificate (p. 32)

The PEM-encoded certificate for your private CA. This must be signed by using your on-premises CA.

Type: Base64-encoded binary data object

Length Constraints: Minimum length of 1. Maximum length of 32768.

Required: Yes

CertificateAuthorityArn (p. 32)

The Amazon Resource Name (ARN) that was returned when you called CreateCertificateAuthority (p. 3). This must be of the form:

`arn:aws:acm-pca:region:account:certificate-authority/12345678-1234-1234-1234-123456789012`

Type: String

Length Constraints: Minimum length of 5. Maximum length of 200.

Pattern: `arn:[\w+=/,.@-]+:[\w+=/,.@-]+:[\w+=/,.@-]*:[0-9]+:[\w+=,.@-]+(/[\w+=/,.@-]+)*`

Required: Yes

CertificateChain (p. 32)

A PEM-encoded file that contains all of your certificates, other than the certificate you're importing, chaining up to your root CA. Your on-premises root certificate is the last in the chain, and each certificate in the chain signs the one preceding.

Type: Base64-encoded binary data object

Length Constraints: Minimum length of 0. Maximum length of 2097152.

Required: Yes

Response Elements

If the action is successful, the service sends back an HTTP 200 response with an empty HTTP body.

Errors

For information about the errors that are common to all actions, see Common Errors (p. 78).

CertificateMismatchException

The certificate authority certificate you are importing does not comply with conditions specified in the certificate that signed it.

HTTP Status Code: 400

ConcurrentModificationException

A previous update to your private CA is still ongoing.

HTTP Status Code: 400

InvalidArnException

The requested Amazon Resource Name (ARN) does not refer to an existing resource.

HTTP Status Code: 400

InvalidStateException

The private CA is in a state during which a report cannot be generated.

HTTP Status Code: 400

MalformedCertificateException

One or more fields in the certificate are invalid.

HTTP Status Code: 400

RequestFailedException

The request has failed for an unspecified reason.

HTTP Status Code: 400

RequestInProgressException

Your request is already in progress.

HTTP Status Code: 400

ResourceNotFoundException

A resource such as a private CA, S3 bucket, certificate, or audit report cannot be found.

HTTP Status Code: 400

Examples

Example

Sample Request

```
POST / HTTP/1.1
Host: acm-pca.amazonaws.com
Accept-Encoding: identity
Content-Length: 3375
X-Amz-Target: ACMPrivateCA.ImportCertificateAuthorityCertificate
X-Amz-Date: 20180226T203302Z
User-Agent: aws-cli/1.14.28 Python/2.7.9 Windows/8 botocore/1.8.32
Content-Type: application/x-amz-json-1.1
Authorization: AWS4-HMAC-SHA256 Credential=AWS_Access_Key_ID/20180226/AWS_Region/
acm-pca/aws4_request, SignedHeaders=content-type;host;x-amz-date;x-amz-target,
 Signature=cdf100cc3972f9df2e0f94295a6e378fbac8c1f489363689805504450e605d83

{
 "CertificateChain": "base64-encoded certificate chain",
 "Certificate": "base64-encoded certificate",
 "CertificateAuthorityArn": "arn:aws:acm-pca:region:account:certificate-
authority/12345678-1234-1234-1234-123456789012"
}
```

Example

Sample Response

```
This function does not return a value.
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V2

IssueCertificate

Uses your private certificate authority (CA) to issue a client certificate. This operation returns the Amazon Resource Name (ARN) of the certificate. You can retrieve the certificate by calling the GetCertificate (p. 22) operation and specifying the ARN.

Note
You cannot use the ACM **ListCertificateAuthorities** operation to retrieve the ARNs of the certificates that you issue by using ACM PCA.

Request Syntax

```
{
   "CertificateAuthorityArn": "string",
   "Csr": blob,
   "IdempotencyToken": "string",
   "SigningAlgorithm": "string",
   "Validity": {
      "Type": "string",
      "Value": number
   }
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 76).

The request accepts the following data in JSON format.

CertificateAuthorityArn (p. 35)

The Amazon Resource Name (ARN) that was returned when you called CreateCertificateAuthority (p. 3). This must be of the form:

`arn:aws:acm-pca:region:account:certificate-authority/12345678-1234-1234-1234-123456789012`

Type: String

Length Constraints: Minimum length of 5. Maximum length of 200.

Pattern: `arn:[\w+=/,.@-]+:[\w+=/,.@-]+:[\w+=/,.@-]*:[0-9]+:[\w+=,.@-]+(/[\w+=/,.@-]+)*`

Required: Yes

Csr (p. 35)

The certificate signing request (CSR) for the certificate you want to issue. You can use the following OpenSSL command to create the CSR and a 2048 bit RSA private key.

```
openssl req -new -newkey rsa:2048 -days 365 -keyout private/
test_cert_priv_key.pem -out csr/test_cert_.csr
```

If you have a configuration file, you can use the following OpenSSL command. The `usr_cert` block in the configuration file contains your X509 version 3 extensions.

```
openssl req -new -config openssl_rsa.cnf -extensions usr_cert -newkey
rsa:2048 -days -365 -keyout private/test_cert_priv_key.pem -out csr/
test_cert_.csr
```

Type: Base64-encoded binary data object

Length Constraints: Minimum length of 1. Maximum length of 32768.

Required: Yes

IdempotencyToken (p. 35)

Custom string that can be used to distinguish between calls to the **IssueCertificate** operation. Idempotency tokens time out after one hour. Therefore, if you call **IssueCertificate** multiple times with the same idempotency token within 5 minutes, ACM PCA recognizes that you are requesting only one certificate and will issue only one. If you change the idempotency token for each call, PCA recognizes that you are requesting multiple certificates.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 36.

Pattern: `[\u0009\u000A\u000D\u0020-\u00FF]*`

Required: No

SigningAlgorithm (p. 35)

The name of the algorithm that will be used to sign the certificate to be issued.

Type: String

Valid Values: `SHA256WITHECDSA | SHA384WITHECDSA | SHA512WITHECDSA | SHA256WITHRSA | SHA384WITHRSA | SHA512WITHRSA`

Required: Yes

Validity (p. 35)

The type of the validity period.

Type: Validity (p. 75) object

Required: Yes

Response Syntax

```
{
   "CertificateArn": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

CertificateArn (p. 36)

The Amazon Resource Name (ARN) of the issued certificate and the certificate serial number. This is of the form:

`arn:aws:acm-pca:`*`region`*`:`*`account`*`:certificate-authority/`*`12345678-1234-1234-1234-123456789012`*`/certificate/`*`286535153982981100925020015808220737245`*

Type: String

Length Constraints: Minimum length of 5. Maximum length of 200.

Pattern: `arn:[\w+=/,.@-]+:[\w+=/,.@-]+:[\w+=/,.@-]*:[0-9]+:[\w+=,.@-]+(/[\w+=/,.@-]+)*`

Errors

For information about the errors that are common to all actions, see Common Errors (p. 78).

InvalidArgsException

One or more of the specified arguments was not valid.

HTTP Status Code: 400

InvalidArnException

The requested Amazon Resource Name (ARN) does not refer to an existing resource.

HTTP Status Code: 400

InvalidStateException

The private CA is in a state during which a report cannot be generated.

HTTP Status Code: 400

LimitExceededException

An ACM PCA limit has been exceeded. See the exception message returned to determine the limit that was exceeded.

HTTP Status Code: 400

MalformedCSRException

The certificate signing request is invalid.

HTTP Status Code: 400

ResourceNotFoundException

A resource such as a private CA, S3 bucket, certificate, or audit report cannot be found.

HTTP Status Code: 400

Examples

Example

Sample Request

```
POST / HTTP/1.1
Host: acm-pca.amazonaws.com
```

```
Accept-Encoding: identity
Content-Length: 1680
X-Amz-Target: ACMPrivateCA.IssueCertificate
X-Amz-Date: 20180226T193956Z
User-Agent: aws-cli/1.14.28 Python/2.7.9 Windows/8 botocore/1.8.32
Content-Type: application/x-amz-json-1.1
Authorization: AWS4-HMAC-SHA256 Credential=AWS_Key_ID/20180226/AWS_Region/acm-pca/
aws4_request,
SignedHeaders=content-type;host;x-amz-date;x-amz-target,
Signature=c6cac56b2eac254d53616072c55d2c2c1f24f4670aa16911c76ae492a92fdd00

{
  "IdempotencyToken": "1234",
  "SigningAlgorithm": "SHA256WITHRSA",
  "Validity": {
    "Type": "DAYS",
    "Value": 365
  },
  "CertificateAuthorityArn": "arn:aws:acm-pca:region:account:certificate-
authority/12345678-1234-1234-1234-123456789012",
  "Csr": "LS0tL...tLS0K"
}
```

Example

Sample Response

```
HTTP/1.1 200 OK
Date: Tue, 15 May 2018 18:08:50 GMT
Content-Type: application/x-amz-json-1.1
Content-Length: 163
x-amzn-RequestId: 629173f2-4697-44fa-a599-b757a8da6c7e
Connection: keep-alive

{
    "CertificateArn": "arn:aws:acm-pca:region:account:certificate-
authority/12345678-1234-1234-1234-123456789012/
certificate/e8cbd2bedb122329f97706bcfec990f8"
}
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V2

ListCertificateAuthorities

Lists the private certificate authorities that you created by using the CreateCertificateAuthority (p. 3) operation.

Request Syntax

```
{
   "MaxResults": number,
   "NextToken": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 76).

The request accepts the following data in JSON format.

MaxResults (p. 39)

Use this parameter when paginating results to specify the maximum number of items to return in the response on each page. If additional items exist beyond the number you specify, the `NextToken` element is sent in the response. Use this `NextToken` value in a subsequent request to retrieve additional items.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 1000.

Required: No

NextToken (p. 39)

Use this parameter when paginating results in a subsequent request after you receive a response with truncated results. Set it to the value of the `NextToken` parameter from the response you just received.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 500.

Required: No

Response Syntax

```
{
   "CertificateAuthorities": [
      {
         "Arn": "string",
         "CertificateAuthorityConfiguration": {
            "KeyAlgorithm": "string",
            "SigningAlgorithm": "string",
            "Subject": {
               "CommonName": "string",
```

```
                "Country": "string",
                "DistinguishedNameQualifier": "string",
                "GenerationQualifier": "string",
                "GivenName": "string",
                "Initials": "string",
                "Locality": "string",
                "Organization": "string",
                "OrganizationalUnit": "string",
                "Pseudonym": "string",
                "SerialNumber": "string",
                "State": "string",
                "Surname": "string",
                "Title": "string"
            }
         },
         "CreatedAt": number,
         "FailureReason": "string",
         "LastStateChangeAt": number,
         "NotAfter": number,
         "NotBefore": number,
         "RestorableUntil": number,
         "RevocationConfiguration": {
            "CrlConfiguration": {
               "CustomCname": "string",
               "Enabled": boolean,
               "ExpirationInDays": number,
               "S3BucketName": "string"
            }
         },
         "Serial": "string",
         "Status": "string",
         "Type": "string"
      }
   ],
   "NextToken": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

CertificateAuthorities (p. 39)

Summary information about each certificate authority you have created.

Type: Array of CertificateAuthority (p. 66) objects

NextToken (p. 39)

When the list is truncated, this value is present and should be used for the `NextToken` parameter in a subsequent pagination request.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 500.

Errors

For information about the errors that are common to all actions, see Common Errors (p. 78).

InvalidNextTokenException

The token specified in the `NextToken` argument is not valid. Use the token returned from your previous call to ListCertificateAuthorities (p. 39).

HTTP Status Code: 400

Examples

Example

Sample Request

```
POST / HTTP/1.1
Host: acm-pca.amazonaws.com
Accept-Encoding: identity
Content-Length: 18
X-Amz-Target: ACMPrivateCA.ListCertificateAuthorities
X-Amz-Date: 20180226T150214Z
User-Agent: aws-cli/1.14.28 Python/2.7.9 Windows/8 botocore/1.8.32
Content-Type: application/x-amz-json-1.1
Authorization: AWS4-HMAC-SHA256 Credential=Access_Key_ID/20180226/AWS_Region/acm-pca/
aws4_request,
SignedHeaders=content-type;host;x-amz-date;x-amz-target,
Signature=580fdd5ac17213a3016252fb1b3e1064b507f415f1b55ef1a42c9d7945d620c1

{"MaxResults": 10}
```

Example

Sample Response

```
HTTP/1.1 200 OK
Date: Tue, 15 May 2018 15:56:45 GMT
Content-Type: application/x-amz-json-1.1
Content-Length: 5484
x-amzn-RequestId: 9f96be4c-2204-4232-84df-fe5e44d22b22
Connection: keep-alive

{
  "CertificateAuthorities": [{
    "Arn": "arn:aws:acm-pca:AWS_Region:AWS_Account:certificate-
authority/12345678-1234-1234-1234-123456789012",
    "CertificateAuthorityConfiguration": {
      "KeyAlgorithm": "RSA_2048",
      "SigningAlgorithm": "SHA256WITHRSA",
      "Subject": {
        "CommonName": "www.example.com",
        "Locality": "Seattle",
        "Organization": "Example Corporation",
        "OrganizationalUnit": "Operations",
        "State": "Washington"
      }
    },
    "CreatedAt": 1.510085139623E9,
    "LastStateChangeAt": 1.515616539109E9,
    "NotAfter": 1.825445955E9,
    "NotBefore": 1.510085955E9,
    "RevocationConfiguration": {
```

```
      "CrlConfiguration": {
        "CustomCname": "https://somename.crl",
        "Enabled": true,
        "ExpirationInDays": 3650,
        "S3BucketName": "your-bucket-name"
      }
    },
    "Serial": "4109",
    "Status": "DISABLED",
    "Type": "SUBORDINATE"
  },
  {
    "Arn": "arn:aws:acm-pca:AWS_Region:AWS_Account:certificate-
authority/11111111-2222-3333-4444-555555555555",
    "CertificateAuthorityConfiguration": {
      "KeyAlgorithm": "RSA_4096",
      "SigningAlgorithm": "SHA256WITHRSA",
      "Subject": {
        "CommonName": "www.examplesales.com",
        "Country": "US",
        "Locality": "Spokane",
        "Organization": "Example Sales LLC",
        "OrganizationalUnit": "Corporate",
        "State": "Washington"
      }
    },
    "CreatedAt": 1.517421065699E9,
    "LastStateChangeAt": 1.517421065699E9,
    "RevocationConfiguration": {
      "CrlConfiguration": {
        "CustomCname": "https://somename.crl",
        "Enabled": true,
        "ExpirationInDays": 3650,
        "S3BucketName": "your-bucket-name"
      }
    },
    "Serial": "3611",
    "Status": "PENDING_CERTIFICATE",
    "Type": "SUBORDINATE"
  },
  {
    "Arn": "arn:aws:acm-pca:AWS_Region:AWS_Account:certificate-
authority/99999999-4321-1234-4321-4321-888888888888",
    "CertificateAuthorityConfiguration": {
      "KeyAlgorithm": "RSA_2048",
      "SigningAlgorithm": "SHA256WITHRSA",
      "Subject": {
        "CommonName": "www.company.com",
        "Country": "US",
        "Locality": "Seattle",
        "Organization": "Company Ltd.",
        "OrganizationalUnit": "Sales",
        "State": "Washington"
      }
    },
    "CreatedAt": 1.505332492167E9,
    "LastStateChangeAt": 1.505332492167E9,
    "NotAfter": 1.820697079E9,
    "NotBefore": 1.505337079E9,
    "RevocationConfiguration": {
      "CrlConfiguration": {
        "CustomCname": "https://somename.crl",
        "Enabled": true,
        "ExpirationInDays": 3650,
        "S3BucketName": "your-bucket-name"
      }
```

```
    },
    "Serial": "4100",
    "Status": "ACTIVE",
    "Type": "SUBORDINATE"
  }
 ]
}
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V2

ListTags

Lists the tags, if any, that are associated with your private CA. Tags are labels that you can use to identify and organize your CAs. Each tag consists of a key and an optional value. Call the TagCertificateAuthority (p. 53) operation to add one or more tags to your CA. Call the UntagCertificateAuthority (p. 56) operation to remove tags.

Request Syntax

```
{
   "CertificateAuthorityArn": "string",
   "MaxResults": number,
   "NextToken": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 76).

The request accepts the following data in JSON format.

CertificateAuthorityArn (p. 44)

The Amazon Resource Name (ARN) that was returned when you called the CreateCertificateAuthority (p. 3) operation. This must be of the form:

`arn:aws:acm-pca:region:account:certificate-authority/12345678-1234-1234-1234-123456789012`

Type: String

Length Constraints: Minimum length of 5. Maximum length of 200.

Pattern: `arn:[\w+=/,.@-]+:[\w+=/,.@-]+:[\w+=/,.@-]*:[0-9]+:[\w+=,.@-]+(/[\w+=/,.@-]+)*`

Required: Yes

MaxResults (p. 44)

Use this parameter when paginating results to specify the maximum number of items to return in the response. If additional items exist beyond the number you specify, the **NextToken** element is sent in the response. Use this **NextToken** value in a subsequent request to retrieve additional items.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 1000.

Required: No

NextToken (p. 44)

Use this parameter when paginating results in a subsequent request after you receive a response with truncated results. Set it to the value of **NextToken** from the response you just received.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 500.

Required: No

Response Syntax

```
{
   "NextToken": "string",
   "Tags": [
      {
         "Key": "string",
         "Value": "string"
      }
   ]
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

NextToken (p. 45)

When the list is truncated, this value is present and should be used for the **NextToken** parameter in a subsequent pagination request.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 500.

Tags (p. 45)

The tags associated with your private CA.

Type: Array of Tag (p. 74) objects

Array Members: Minimum number of 1 item. Maximum number of 50 items.

Errors

For information about the errors that are common to all actions, see Common Errors (p. 78).

InvalidArnException

The requested Amazon Resource Name (ARN) does not refer to an existing resource.

HTTP Status Code: 400

ResourceNotFoundException

A resource such as a private CA, S3 bucket, certificate, or audit report cannot be found.

HTTP Status Code: 400

Examples

Example

Sample Request

```
POST / HTTP/1.1
```

```
Host: acm-pca.amazonaws.com
Accept-Encoding: identity
Content-Length: 146
X-Amz-Target: ACMPrivateCA.ListTags
X-Amz-Date: 20180226T164656Z
User-Agent: aws-cli/1.14.28 Python/2.7.9 Windows/8 botocore/1.8.32
Content-Type: application/x-amz-json-1.1
Authorization: AWS4-HMAC-SHA256 Credential=Access_Key_ID/20180226/AWS_Region/acm-pca/
aws4_request,
SignedHeaders=content-type;host;x-amz-date;x-amz-target,
Signature=59cc6594a1df0f441bd39e466755465e52545f57faa8329d907c715bc8a5f97b

{
"MaxResults": 10,
"CertificateAuthorityArn": "arn:aws:acm-pca:region:AWS_Account:certificate-
authority/12345678-1234-1234-1234-123456789012"
}
```

Example

Sample Response

```
HTTP/1.1 200 OK
Date: Tue, 15 May 2018 18:25:09 GMT
Content-Type: application/x-amz-json-1.1
Content-Length: 69
x-amzn-RequestId: 9893f3cb-1bd8-4a15-8394-4f5364963acf
Connection: keep-alive

  "Tags": [{
    "Key": "Admin",
    "Value": "Alice"
  },
  {
    "Key": "Purpose",
    "Value": "Website"
  }]
}
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V2

RestoreCertificateAuthority

Restores a certificate authority (CA) that is in the `DELETED` state. You can restore a CA during the period that you defined in the **PermanentDeletionTimeInDays** parameter of the DeleteCertificateAuthority (p. 12) operation. Currently, you can specify 7 to 30 days. If you did not specify a **PermanentDeletionTimeInDays** value, by default you can restore the CA at any time in a 30 day period. You can check the time remaining in the restoration period of a private CA in the `DELETED` state by calling the DescribeCertificateAuthority (p. 15) or ListCertificateAuthorities (p. 39) operations. The status of a restored CA is set to its pre-deletion status when the **RestoreCertificateAuthority** operation returns. To change its status to `ACTIVE`, call the UpdateCertificateAuthority (p. 59) operation. If the private CA was in the `PENDING_CERTIFICATE` state at deletion, you must use the ImportCertificateAuthorityCertificate (p. 32) operation to import a certificate authority into the private CA before it can be activated. You cannot restore a CA after the restoration period has ended.

Request Syntax

```
{
   "CertificateAuthorityArn": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 76).

The request accepts the following data in JSON format.

CertificateAuthorityArn (p. 47)

The Amazon Resource Name (ARN) that was returned when you called the CreateCertificateAuthority (p. 3) operation. This must be of the form:

`arn:aws:acm-pca:region:account:certificate-authority/12345678-1234-1234-1234-123456789012`

Type: String

Length Constraints: Minimum length of 5. Maximum length of 200.

Pattern: `arn:[\w+=/,.@-]+:[\w+=/,.@-]+:[\w+=/,.@-]*:[0-9]+:[\w+=,.@-]+(/[\w+=/,.@-]+)*`

Required: Yes

Response Elements

If the action is successful, the service sends back an HTTP 200 response with an empty HTTP body.

Errors

For information about the errors that are common to all actions, see Common Errors (p. 78).

InvalidArnException

The requested Amazon Resource Name (ARN) does not refer to an existing resource.

HTTP Status Code: 400

InvalidStateException

The private CA is in a state during which a report cannot be generated.

HTTP Status Code: 400

ResourceNotFoundException

A resource such as a private CA, S3 bucket, certificate, or audit report cannot be found.

HTTP Status Code: 400

Examples

Example

Sample Request

```
POST / HTTP/1.1
Host: acm-pca.amazonaws.com
Accept-Encoding: identity
Content-Length: 128
X-Amz-Target: ACMPrivateCA.RestoreCertificateAuthority
X-Amz-Date: 20180514T174156Z
User-Agent: aws-cli/1.15.4 Python/2.7.9 Windows/8 botocore/1.10.4
Content-Type: application/x-amz-json-1.1
Authorization: AWS4-HMAC-SHA256 Credential=Access_Key_ID/20180514/AWS_Region/
acm-pca/aws4_request, SignedHeaders=content-type;host;x-amz-date;x-amz-target,
 Signature=a47d3316aee9992689407c40f877138c261cef8e73996f608c5ffcaf46c593f8

{"CertificateAuthorityArn": "arn:aws:acm-pca:AWS_region:AWS_Account:certificate-
authority/12345678-1234-1234-1234-123456789012"}
```

Example

Sample Response

```
This function does not return a value.
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V2

RevokeCertificate

Revokes a certificate that you issued by calling the IssueCertificate (p. 35) operation. If you enable a certificate revocation list (CRL) when you create or update your private CA, information about the revoked certificates will be included in the CRL. ACM PCA writes the CRL to an S3 bucket that you specify. For more information about revocation, see the CrlConfiguration (p. 70) structure. ACM PCA also writes revocation information to the audit report. For more information, see CreateCertificateAuthorityAuditReport (p. 8).

Request Syntax

```
{
   "CertificateAuthorityArn": "string",
   "CertificateSerial": "string",
   "RevocationReason": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 76).

The request accepts the following data in JSON format.

CertificateAuthorityArn (p. 50)

Amazon Resource Name (ARN) of the private CA that issued the certificate to be revoked. This must be of the form:

`arn:aws:acm-pca:`*`region`*`:`*`account`*`:certificate-authority/`*`12345678-1234-1234-1234-123456789012`*

Type: String

Length Constraints: Minimum length of 5. Maximum length of 200.

Pattern: `arn:[\w+=/,.@-]+:[\w+=/,.@-]+:[\w+=/,.@-]*:[0-9]+:[\w+=,.@-]+(/[\w+=/,.@-]+)*`

Required: Yes

CertificateSerial (p. 50)

Serial number of the certificate to be revoked. This must be in hexadecimal format. You can retrieve the serial number by calling GetCertificate (p. 22) with the Amazon Resource Name (ARN) of the certificate you want and the ARN of your private CA. The **GetCertificate** operation retrieves the certificate in the PEM format. You can use the following OpenSSL command to list the certificate in text format and copy the hexadecimal serial number.

`openssl x509 -in `*`file_path`*` -text -noout`

You can also copy the serial number from the console or use the DescribeCertificate operation in the *AWS Certificate Manager API Reference*.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 128.

Required: Yes

RevocationReason (p. 50)

Specifies why you revoked the certificate.

Type: String

Valid Values: `UNSPECIFIED | KEY_COMPROMISE | CERTIFICATE_AUTHORITY_COMPROMISE | AFFILIATION_CHANGED | SUPERSEDED | CESSATION_OF_OPERATION | PRIVILEGE_WITHDRAWN | A_A_COMPROMISE`

Required: Yes

Response Elements

If the action is successful, the service sends back an HTTP 200 response with an empty HTTP body.

Errors

For information about the errors that are common to all actions, see Common Errors (p. 78).

ConcurrentModificationException

A previous update to your private CA is still ongoing.

HTTP Status Code: 400

InvalidArnException

The requested Amazon Resource Name (ARN) does not refer to an existing resource.

HTTP Status Code: 400

InvalidStateException

The private CA is in a state during which a report cannot be generated.

HTTP Status Code: 400

RequestAlreadyProcessedException

Your request has already been completed.

HTTP Status Code: 400

RequestFailedException

The request has failed for an unspecified reason.

HTTP Status Code: 400

RequestInProgressException

Your request is already in progress.

HTTP Status Code: 400

ResourceNotFoundException

A resource such as a private CA, S3 bucket, certificate, or audit report cannot be found.

HTTP Status Code: 400

Examples

Example

Sample Request

```
POST / HTTP/1.1
Host: acm-pca.amazonaws.com
Accept-Encoding: identity
Content-Length: 238
X-Amz-Target: ACMPrivateCA.RevokeCertificate
X-Amz-Date: 20180226T200035Z
User-Agent: aws-cli/1.14.28 Python/2.7.9 Windows/8 botocore/1.8.32
Content-Type: application/x-amz-json-1.1
Authorization: AWS4-HMAC-SHA256 Credential=AWS_Access_Key_ID/20180226/AWS_Region/acm-pca/
aws4_request,
SignedHeaders=content-type;host;x-amz-date;x-amz-target,
Signature=ab19c4301eb2e8e9f188f3d478cb1d5a28bfb41de3d54b5006c0738d411cfd86

{
  "CertificateSerial": "e8:cb:d2:be:db:12:23:29:f9:77:06:bc:fe:c9:90:f8",
  "RevocationReason": "KEY_COMPROMISE",
  "CertificateAuthorityArn": "arn:aws:acm-pca:region:account:certificate-
authority/12345678-1234-1234-1234-123456789012"
}
```

Example

Sample Response

```
This function does not return a value.
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V2

TagCertificateAuthority

Adds one or more tags to your private CA. Tags are labels that you can use to identify and organize your AWS resources. Each tag consists of a key and an optional value. You specify the private CA on input by its Amazon Resource Name (ARN). You specify the tag by using a key-value pair. You can apply a tag to just one private CA if you want to identify a specific characteristic of that CA, or you can apply the same tag to multiple private CAs if you want to filter for a common relationship among those CAs. To remove one or more tags, use the UntagCertificateAuthority (p. 56) operation. Call the ListTags (p. 44) operation to see what tags are associated with your CA.

Request Syntax

```
{
   "CertificateAuthorityArn": "string",
   "Tags": [
      {
         "Key": "string",
         "Value": "string"
      }
   ]
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 76).

The request accepts the following data in JSON format.

CertificateAuthorityArn (p. 53)

The Amazon Resource Name (ARN) that was returned when you called CreateCertificateAuthority (p. 3). This must be of the form:

`arn:aws:acm-pca:region:account:certificate-authority/12345678-1234-1234-1234-123456789012`

Type: String

Length Constraints: Minimum length of 5. Maximum length of 200.

Pattern: `arn:[\w+=/,.@-]+:[\w+=/,.@-]+:[\w+=/,.@-]*:[0-9]+:[\w+=,.@-]+(/[\w+=/,.@-]+)*`

Required: Yes

Tags (p. 53)

List of tags to be associated with the CA.

Type: Array of Tag (p. 74) objects

Array Members: Minimum number of 1 item. Maximum number of 50 items.

Required: Yes

Response Elements

If the action is successful, the service sends back an HTTP 200 response with an empty HTTP body.

Errors

For information about the errors that are common to all actions, see Common Errors (p. 78).

InvalidArnException

The requested Amazon Resource Name (ARN) does not refer to an existing resource.

HTTP Status Code: 400

InvalidStateException

The private CA is in a state during which a report cannot be generated.

HTTP Status Code: 400

InvalidTagException

The tag associated with the CA is not valid. The invalid argument is contained in the message field.

HTTP Status Code: 400

ResourceNotFoundException

A resource such as a private CA, S3 bucket, certificate, or audit report cannot be found.

HTTP Status Code: 400

TooManyTagsException

You can associate up to 50 tags with a private CA. Exception information is contained in the exception message field.

HTTP Status Code: 400

Examples

Example

Sample Request

```
POST / HTTP/1.1
Host: acm-pca.amazonaws.com
Accept-Encoding: identity
Content-Length: 180
X-Amz-Target: ACMPrivateCA.TagCertificateAuthority
X-Amz-Date: 20180226T170330Z
User-Agent: aws-cli/1.14.28 Python/2.7.9 Windows/8 botocore/1.8.32
Content-Type: application/x-amz-json-1.1
Authorization: AWS4-HMAC-SHA256 Credential=Access_Key_ID/20180226/AWS_Region/
acm-pca/aws4_request, SignedHeaders=content-type;host;x-amz-date;x-amz-target,
 Signature=823508ca59a8620ec0981fada8b14a1b85e1db9938103e1fe2a7c394e70b1d0b

{
"CertificateAuthorityArn": "arn:aws:acm-pca:AWS_Region:AWS_Account:certificate-
authority/12345678-1234-1234-1234-123456789012",
"Tags": [{
  "Key": "Bob",
  "Value": "DatabaseAdmin"
}]
}
```

Example

Sample Response

```
This function does not return a value.
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V2

UntagCertificateAuthority

Remove one or more tags from your private CA. A tag consists of a key-value pair. If you do not specify the value portion of the tag when calling this operation, the tag will be removed regardless of value. If you specify a value, the tag is removed only if it is associated with the specified value. To add tags to a private CA, use the TagCertificateAuthority (p. 53). Call the ListTags (p. 44) operation to see what tags are associated with your CA.

Request Syntax

```
{
   "CertificateAuthorityArn": "string",
   "Tags": [
      {
         "Key": "string",
         "Value": "string"
      }
   ]
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 76).

The request accepts the following data in JSON format.

CertificateAuthorityArn (p. 56)

The Amazon Resource Name (ARN) that was returned when you called CreateCertificateAuthority (p. 3). This must be of the form:

`arn:aws:acm-pca:region:account:certificate-authority/12345678-1234-1234-1234-123456789012`

Type: String

Length Constraints: Minimum length of 5. Maximum length of 200.

Pattern: `arn:[\w+=/,.@-]+:[\w+=/,.@-]+:[\w+=/,.@-]*:[0-9]+:[\w+=,.@-]+(/[\w+=/,.@-]+)*`

Required: Yes

Tags (p. 56)

List of tags to be removed from the CA.

Type: Array of Tag (p. 74) objects

Array Members: Minimum number of 1 item. Maximum number of 50 items.

Required: Yes

Response Elements

If the action is successful, the service sends back an HTTP 200 response with an empty HTTP body.

Errors

For information about the errors that are common to all actions, see Common Errors (p. 78).

InvalidArnException

The requested Amazon Resource Name (ARN) does not refer to an existing resource.

HTTP Status Code: 400

InvalidStateException

The private CA is in a state during which a report cannot be generated.

HTTP Status Code: 400

InvalidTagException

The tag associated with the CA is not valid. The invalid argument is contained in the message field.

HTTP Status Code: 400

ResourceNotFoundException

A resource such as a private CA, S3 bucket, certificate, or audit report cannot be found.

HTTP Status Code: 400

Examples

Example

Sample Request

```
POST / HTTP/1.1
Host: acm-pca.amazonaws.com
Accept-Encoding: identity
Content-Length: 174
X-Amz-Target: ACMPrivateCA.UntagCertificateAuthority
X-Amz-Date: 20180226T171108Z
User-Agent: aws-cli/1.14.28 Python/2.7.9 Windows/8 botocore/1.8.32
Content-Type: application/x-amz-json-1.1
Authorization: AWS4-HMAC-SHA256 Credential=Access_Key_ID/20180226/AWS_Region/acm-pca/
aws4_request,
SignedHeaders=content-type;host;x-amz-date;x-amz-target,
Signature=a19a10be912304e7e36677a2e8e6f573dcc3bc506fb886a3e273d194cbfcb2e2

{
  "CertificateAuthorityArn": "arn:aws:acm-pca:AWS_Region:AWS_Account:certificate-
authority/12345678-1234-1234-1234-123456789012",
  "Tags": [{
    "Key": "Alice",
    "Value": "Admin"
  }]
}
```

Example

Sample Response

```
This function does not return a value.
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V2

UpdateCertificateAuthority

Updates the status or configuration of a private certificate authority (CA). Your private CA must be in the `ACTIVE` or `DISABLED` state before you can update it. You can disable a private CA that is in the `ACTIVE` state or make a CA that is in the `DISABLED` state active again.

Request Syntax

```
{
   "CertificateAuthorityArn": "string",
   "RevocationConfiguration": {
      "CrlConfiguration": {
         "CustomCname": "string",
         "Enabled": boolean,
         "ExpirationInDays": number,
         "S3BucketName": "string"
      }
   },
   "Status": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 76).

The request accepts the following data in JSON format.

CertificateAuthorityArn (p. 59)

Amazon Resource Name (ARN) of the private CA that issued the certificate to be revoked. This must be of the form:

`arn:aws:acm-pca:`*`region`*`:`*`account`*`:certificate-authority/`*`12345678-1234-1234-1234-123456789012`*

Type: String

Length Constraints: Minimum length of 5. Maximum length of 200.

Pattern: `arn:[\w+=/,.@-]+:[\w+=/,.@-]+:[\w+=/,.@-]*:[0-9]+:[\w+=,.@-]+(/[\w+=/,.@-]+)*`

Required: Yes

RevocationConfiguration (p. 59)

Revocation information for your private CA.

Type: RevocationConfiguration (p. 73) object

Required: No

Status (p. 59)

Status of your private CA.

Type: String

Valid Values: `CREATING | PENDING_CERTIFICATE | ACTIVE | DELETED | DISABLED | EXPIRED | FAILED`

Required: No

Response Elements

If the action is successful, the service sends back an HTTP 200 response with an empty HTTP body.

Errors

For information about the errors that are common to all actions, see Common Errors (p. 78).

ConcurrentModificationException

A previous update to your private CA is still ongoing.

HTTP Status Code: 400

InvalidArgsException

One or more of the specified arguments was not valid.

HTTP Status Code: 400

InvalidArnException

The requested Amazon Resource Name (ARN) does not refer to an existing resource.

HTTP Status Code: 400

InvalidPolicyException

The S3 bucket policy is not valid. The policy must give ACM PCA rights to read from and write to the bucket and find the bucket location.

HTTP Status Code: 400

InvalidStateException

The private CA is in a state during which a report cannot be generated.

HTTP Status Code: 400

ResourceNotFoundException

A resource such as a private CA, S3 bucket, certificate, or audit report cannot be found.

HTTP Status Code: 400

Examples

Example

Sample Request

```
POST / HTTP/1.1
Host: acm-pca.amazonaws.com
Accept-Encoding: identity
```

```
Content-Length: 323
X-Amz-Target: ACMPrivateCA.UpdateCertificateAuthority
X-Amz-Date: 20180226T172929Z
User-Agent: aws-cli/1.14.28 Python/2.7.9 Windows/8 botocore/1.8.32
Content-Type: application/x-amz-json-1.1
Authorization: AWS4-HMAC-SHA256 Credential=Access_Key_ID/20180226/AWS_Region/acm-pca/
aws4_request,
SignedHeaders=content-type;host;x-amz-date;x-amz-target,
Signature=f11213b3c4da1754a811fcd72ea637b8acbe41fb7b5e3541806d0418a3323dd8

{
  "Status": "ACTIVE",
  "RevocationConfiguration": {
    "CrlConfiguration": {
      "CustomCname": "https://somename.crl",
      "Enabled": true,
      "S3BucketName": "your-bucket-name",
      "ExpirationInDays": 3650
    }
  },
  "CertificateAuthorityArn": "arn:aws:acm-pca:AWS_Region:AWS_Account:certificate-
authority/12345678-1234-1234-1234-123456789012"
}
```

Example

Sample Response

```
This function does not return a value.
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V2

Data Types

The AWS Certificate Manager Private Certificate Authority API contains several data types that various actions use. This section describes each data type in detail.

> **Note**
> The order of each element in a data type structure is not guaranteed. Applications should not assume a particular order.

The following data types are supported:

ASN1Subject

Contains information about the certificate subject. The certificate can be one issued by your private certificate authority (CA) or it can be your private CA certificate. The **Subject** field in the certificate identifies the entity that owns or controls the public key in the certificate. The entity can be a user, computer, device, or service. The **Subject** must contain an X.500 distinguished name (DN). A DN is a sequence of relative distinguished names (RDNs). The RDNs are separated by commas in the certificate. The DN must be unique for each entity, but your private CA can issue more than one certificate with the same DN to the same entity.

Contents

CommonName

Fully qualified domain name (FQDN) associated with the certificate subject.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 64.

Required: No

Country

Two-digit code that specifies the country in which the certificate subject located.

Type: String

Pattern: `[A-Za-z]{2}`

Required: No

DistinguishedNameQualifier

Disambiguating information for the certificate subject.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 64.

Pattern: `[a-zA-Z0-9'()+-.?:/= ]*`

Required: No

GenerationQualifier

Typically a qualifier appended to the name of an individual. Examples include Jr. for junior, Sr. for senior, and III for third.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 3.

Required: No

GivenName

First name.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 16.

Required: No

Initials

Concatenation that typically contains the first letter of the **GivenName**, the first letter of the middle name if one exists, and the first letter of the **SurName**.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 5.

Required: No

Locality

The locality (such as a city or town) in which the certificate subject is located.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 128.

Required: No

Organization

Legal name of the organization with which the certificate subject is affiliated.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 64.

Required: No

OrganizationalUnit

A subdivision or unit of the organization (such as sales or finance) with which the certificate subject is affiliated.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 64.

Required: No

Pseudonym

Typically a shortened version of a longer **GivenName**. For example, Jonathan is often shortened to John. Elizabeth is often shortened to Beth, Liz, or Eliza.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 128.

Required: No

SerialNumber

The certificate serial number.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 64.

Required: No

State

State in which the subject of the certificate is located.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 128.

Required: No

Surname

Family name. In the US and the UK, for example, the surname of an individual is ordered last. In Asian cultures the surname is typically ordered first.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 40.

Required: No

Title

A title such as Mr. or Ms., which is pre-pended to the name to refer formally to the certificate subject.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 64.

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java
- AWS SDK for Ruby V2

CertificateAuthority

Contains information about your private certificate authority (CA). Your private CA can issue and revoke X.509 digital certificates. Digital certificates verify that the entity named in the certificate **Subject** field owns or controls the public key contained in the **Subject Public Key Info** field. Call the CreateCertificateAuthority (p. 3) operation to create your private CA. You must then call the GetCertificateAuthorityCertificate (p. 26) operation to retrieve a private CA certificate signing request (CSR). Take the CSR to your on-premises CA and sign it with the root CA certificate or a subordinate certificate. Call the ImportCertificateAuthorityCertificate (p. 32) operation to import the signed certificate into AWS Certificate Manager (ACM).

Contents

Arn

Amazon Resource Name (ARN) for your private certificate authority (CA). The format is *12345678-1234-1234-1234-123456789012* .

Type: String

Length Constraints: Minimum length of 5. Maximum length of 200.

Pattern: `arn:[\w+=/,.@-]+:[\w+=/,.@-]+:[\w+=/,.@-]*:[0-9]+:[\w+=,.@-]+(/[\w+=/,.@-]+)*`

Required: No

CertificateAuthorityConfiguration

Your private CA configuration.

Type: CertificateAuthorityConfiguration (p. 69) object

Required: No

CreatedAt

Date and time at which your private CA was created.

Type: Timestamp

Required: No

FailureReason

Reason the request to create your private CA failed.

Type: String

Valid Values: `REQUEST_TIMED_OUT | UNSUPPORTED_ALGORITHM | OTHER`

Required: No

LastStateChangeAt

Date and time at which your private CA was last updated.

Type: Timestamp

Required: No

NotAfter

Date and time after which your private CA certificate is not valid.

Type: Timestamp

Required: No

NotBefore

Date and time before which your private CA certificate is not valid.

Type: Timestamp

Required: No

RestorableUntil

The period during which a deleted CA can be restored. For more information, see the `PermanentDeletionTimeInDays` parameter of the DeleteCertificateAuthorityRequest (p. 72) operation.

Type: Timestamp

Required: No

RevocationConfiguration

Information about the certificate revocation list (CRL) created and maintained by your private CA.

Type: RevocationConfiguration (p. 73) object

Required: No

Serial

Serial number of your private CA.

Type: String

Required: No

Status

Status of your private CA.

Type: String

Valid Values: `CREATING | PENDING_CERTIFICATE | ACTIVE | DELETED | DISABLED | EXPIRED | FAILED`

Required: No

Type

Type of your private CA.

Type: String

Valid Values: `SUBORDINATE`

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++

- AWS SDK for Go
- AWS SDK for Java
- AWS SDK for Ruby V2

CertificateAuthorityConfiguration

Contains configuration information for your private certificate authority (CA). This includes information about the class of public key algorithm and the key pair that your private CA creates when it issues a certificate, the signature algorithm it uses used when issuing certificates, and its X.500 distinguished name. You must specify this information when you call the CreateCertificateAuthority (p. 3) operation.

Contents

KeyAlgorithm

Type of the public key algorithm and size, in bits, of the key pair that your key pair creates when it issues a certificate.

Type: String

Valid Values: `RSA_2048 | RSA_4096 | EC_prime256v1 | EC_secp384r1`

Required: Yes

SigningAlgorithm

Name of the algorithm your private CA uses to sign certificate requests.

Type: String

Valid Values: `SHA256WITHECDSA | SHA384WITHECDSA | SHA512WITHECDSA | SHA256WITHRSA | SHA384WITHRSA | SHA512WITHRSA`

Required: Yes

Subject

Structure that contains X.500 distinguished name information for your private CA.

Type: ASN1Subject (p. 63) object

Required: Yes

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java
- AWS SDK for Ruby V2

CrlConfiguration

Contains configuration information for a certificate revocation list (CRL). Your private certificate authority (CA) creates base CRLs. Delta CRLs are not supported. You can enable CRLs for your new or an existing private CA by setting the **Enabled** parameter to `true`. Your private CA writes CRLs to an S3 bucket that you specify in the **S3BucketName** parameter. You can hide the name of your bucket by specifying a value for the **CustomCname** parameter. Your private CA copies the CNAME or the S3 bucket name to the **CRL Distribution Points** extension of each certificate it issues. Your S3 bucket policy must give write permission to ACM PCA.

Your private CA uses the value in the **ExpirationInDays** parameter to calculate the **nextUpdate** field in the CRL. The CRL is refreshed at 1/2 the age of next update or when a certificate is revoked. When a certificate is revoked, it is recorded in the next CRL that is generated and in the next audit report. Only time valid certificates are listed in the CRL. Expired certificates are not included.

CRLs contain the following fields:

- **Version**: The current version number defined in RFC 5280 is V2. The integer value is 0x1.
- **Signature Algorithm**: The name of the algorithm used to sign the CRL.
- **Issuer**: The X.500 distinguished name of your private CA that issued the CRL.
- **Last Update**: The issue date and time of this CRL.
- **Next Update**: The day and time by which the next CRL will be issued.
- **Revoked Certificates**: List of revoked certificates. Each list item contains the following information.
  - **Serial Number**: The serial number, in hexadecimal format, of the revoked certificate.
  - **Revocation Date**: Date and time the certificate was revoked.
  - **CRL Entry Extensions**: Optional extensions for the CRL entry.
    - **X509v3 CRL Reason Code**: Reason the certificate was revoked.
- **CRL Extensions**: Optional extensions for the CRL.
  - **X509v3 Authority Key Identifier**: Identifies the public key associated with the private key used to sign the certificate.
  - **X509v3 CRL Number:**: Decimal sequence number for the CRL.
- **Signature Algorithm**: Algorithm used by your private CA to sign the CRL.
- **Signature Value**: Signature computed over the CRL.

Certificate revocation lists created by ACM PCA are DER-encoded. You can use the following OpenSSL command to list a CRL.

```
openssl crl -inform DER -text -in crl_path -noout
```

Contents

CustomCname

Name inserted into the certificate **CRL Distribution Points** extension that enables the use of an alias for the CRL distribution point. Use this value if you don't want the name of your S3 bucket to be public.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 253.

Required: No

Enabled

Boolean value that specifies whether certificate revocation lists (CRLs) are enabled. You can use this value to enable certificate revocation for a new CA when you call the CreateCertificateAuthority (p. 3) operation or for an existing CA when you call the UpdateCertificateAuthority (p. 59) operation.

Type: Boolean

Required: Yes

ExpirationInDays

Number of days until a certificate expires.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 5000.

Required: No

S3BucketName

Name of the S3 bucket that contains the CRL. If you do not provide a value for the **CustomCname** argument, the name of your S3 bucket is placed into the **CRL Distribution Points** extension of the issued certificate. You can change the name of your bucket by calling the UpdateCertificateAuthority (p. 59) operation. You must specify a bucket policy that allows ACM PCA to write the CRL to your bucket.

Type: String

Length Constraints: Minimum length of 3. Maximum length of 255.

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java
- AWS SDK for Ruby V2

DeleteCertificateAuthorityRequest

Contents

CertificateAuthorityArn

The Amazon Resource Name (ARN) that was returned when you called CreateCertificateAuthority (p. 3). This must have the following form:

`arn:aws:acm-pca:`*`region`*`:`*`account`*`:certificate-authority/`*`12345678-1234-1234-1234-123456789012`*` .`

Type: String

Length Constraints: Minimum length of 5. Maximum length of 200.

Pattern: `arn:[\w+=/,.@-]+:[\w+=/,.@-]+:[\w+=/,.@-]*:[0-9]+:[\w+=,.@-]+(/[\w+=/,.@-]+)*`

Required: Yes

PermanentDeletionTimeInDays

The number of days to make a CA restorable after it has been deleted. This can be anywhere from 7 to 30 days, with 30 being the default.

Type: Integer

Valid Range: Minimum value of 7. Maximum value of 30.

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java
- AWS SDK for Ruby V2

RevocationConfiguration

Certificate revocation information used by the CreateCertificateAuthority (p. 3) and UpdateCertificateAuthority (p. 59) operations. Your private certificate authority (CA) can create and maintain a certificate revocation list (CRL). A CRL contains information about certificates revoked by your CA. For more information, see RevokeCertificate (p. 50).

Contents

CrlConfiguration

Configuration of the certificate revocation list (CRL), if any, maintained by your private CA.

Type: CrlConfiguration (p. 70) object

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java
- AWS SDK for Ruby V2

Tag

Tags are labels that you can use to identify and organize your private CAs. Each tag consists of a key and an optional value. You can associate up to 50 tags with a private CA. To add one or more tags to a private CA, call the TagCertificateAuthority (p. 53) operation. To remove a tag, call the UntagCertificateAuthority (p. 56) operation.

Contents

Key

Key (name) of the tag.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `[\p{L}\p{Z}\p{N}_.:\/=+\-@]*`

Required: Yes

Value

Value of the tag.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 256.

Pattern: `[\p{L}\p{Z}\p{N}_.:\/=+\-@]*`

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java
- AWS SDK for Ruby V2

Validity

Length of time for which the certificate issued by your private certificate authority (CA), or by the private CA itself, is valid in days, months, or years. You can issue a certificate by calling the IssueCertificate (p. 35) operation.

Contents

Type

Specifies whether the `Value` parameter represents days, months, or years.

Type: String

Valid Values: `END_DATE | ABSOLUTE | DAYS | MONTHS | YEARS`

Required: Yes

Value

Time period.

Type: Long

Valid Range: Minimum value of 1.

Required: Yes

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java
- AWS SDK for Ruby V2

Common Parameters

The following list contains the parameters that all actions use for signing Signature Version 4 requests with a query string. Any action-specific parameters are listed in the topic for that action. For more information about Signature Version 4, see Signature Version 4 Signing Process in the *Amazon Web Services General Reference*.

Action

The action to be performed.

Type: string

Required: Yes

Version

The API version that the request is written for, expressed in the format YYYY-MM-DD.

Type: string

Required: Yes

X-Amz-Algorithm

The hash algorithm that you used to create the request signature.

Condition: Specify this parameter when you include authentication information in a query string instead of in the HTTP authorization header.

Type: string

Valid Values: `AWS4-HMAC-SHA256`

Required: Conditional

X-Amz-Credential

The credential scope value, which is a string that includes your access key, the date, the region you are targeting, the service you are requesting, and a termination string ("aws4_request"). The value is expressed in the following format: *access_key*/*YYYYMMDD*/*region*/*service*/aws4_request.

For more information, see Task 2: Create a String to Sign for Signature Version 4 in the *Amazon Web Services General Reference*.

Condition: Specify this parameter when you include authentication information in a query string instead of in the HTTP authorization header.

Type: string

Required: Conditional

X-Amz-Date

The date that is used to create the signature. The format must be ISO 8601 basic format (YYYYMMDD'T'HHMMSS'Z'). For example, the following date time is a valid X-Amz-Date value: `20120325T120000Z`.

Condition: X-Amz-Date is optional for all requests; it can be used to override the date used for signing requests. If the Date header is specified in the ISO 8601 basic format, X-Amz-Date is

not required. When X-Amz-Date is used, it always overrides the value of the Date header. For more information, see Handling Dates in Signature Version 4 in the *Amazon Web Services General Reference*.

Type: string

Required: Conditional

X-Amz-Security-Token

The temporary security token that was obtained through a call to AWS Security Token Service (AWS STS). For a list of services that support temporary security credentials from AWS Security Token Service, go to AWS Services That Work with IAM in the *IAM User Guide*.

Condition: If you're using temporary security credentials from the AWS Security Token Service, you must include the security token.

Type: string

Required: Conditional

X-Amz-Signature

Specifies the hex-encoded signature that was calculated from the string to sign and the derived signing key.

Condition: Specify this parameter when you include authentication information in a query string instead of in the HTTP authorization header.

Type: string

Required: Conditional

X-Amz-SignedHeaders

Specifies all the HTTP headers that were included as part of the canonical request. For more information about specifying signed headers, see Task 1: Create a Canonical Request For Signature Version 4 in the *Amazon Web Services General Reference*.

Condition: Specify this parameter when you include authentication information in a query string instead of in the HTTP authorization header.

Type: string

Required: Conditional

Common Errors

This section lists the errors common to the API actions of all AWS services. For errors specific to an API action for this service, see the topic for that API action.

AccessDeniedException

You do not have sufficient access to perform this action.

HTTP Status Code: 400

IncompleteSignature

The request signature does not conform to AWS standards.

HTTP Status Code: 400

InternalFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

InvalidAction

The action or operation requested is invalid. Verify that the action is typed correctly.

HTTP Status Code: 400

InvalidClientTokenId

The X.509 certificate or AWS access key ID provided does not exist in our records.

HTTP Status Code: 403

InvalidParameterCombination

Parameters that must not be used together were used together.

HTTP Status Code: 400

InvalidParameterValue

An invalid or out-of-range value was supplied for the input parameter.

HTTP Status Code: 400

InvalidQueryParameter

The AWS query string is malformed or does not adhere to AWS standards.

HTTP Status Code: 400

MalformedQueryString

The query string contains a syntax error.

HTTP Status Code: 404

MissingAction

The request is missing an action or a required parameter.

HTTP Status Code: 400

MissingAuthenticationToken

The request must contain either a valid (registered) AWS access key ID or X.509 certificate.

HTTP Status Code: 403

MissingParameter

A required parameter for the specified action is not supplied.

HTTP Status Code: 400

OptInRequired

The AWS access key ID needs a subscription for the service.

HTTP Status Code: 403

RequestExpired

The request reached the service more than 15 minutes after the date stamp on the request or more than 15 minutes after the request expiration date (such as for pre-signed URLs), or the date stamp on the request is more than 15 minutes in the future.

HTTP Status Code: 400

ServiceUnavailable

The request has failed due to a temporary failure of the server.

HTTP Status Code: 503

ThrottlingException

The request was denied due to request throttling.

HTTP Status Code: 400

ValidationError

The input fails to satisfy the constraints specified by an AWS service.

HTTP Status Code: 400