亚马逊云科技

API Reference

Amazon Private Certificate Authority

API Version 2017-08-22

Amazon Private Certificate Authority: API Reference

Table of Contents

Welcome

This is the *Amazon Private Certificate Authority API Reference*. It provides descriptions, syntax, and usage examples for each of the actions and data types involved in creating and managing a private certificate authority (CA) for your organization.

The documentation for each action shows the API request parameters and the JSON response. Alternatively, you can use one of the Amazon SDKs to access an API that is tailored to the programming language or platform that you prefer. For more information, see Amazon SDKs.

Each Amazon Private CA API operation has a quota that determines the number of times the operation can be called per second. Amazon Private CA throttles API requests at different rates depending on the operation. Throttling means that Amazon Private CA rejects an otherwise valid request because the request exceeds the operation's quota for the number of requests per second. When a request is throttled, Amazon Private CA returns a ThrottlingException error. Amazon Private CA does not guarantee a minimum request rate for APIs.

To see an up-to-date list of your Amazon Private CA quotas, or to request a quota increase, log into your Amazon account and visit the Service Quotas console.

This document was last published on July 3, 2025.

Actions

The following actions are supported:

- CreateCertificateAuthority
- CreateCertificateAuthorityAuditReport
- CreatePermission
- DeleteCertificateAuthority
- DeletePermission
- DeletePolicy
- DescribeCertificateAuthority
- DescribeCertificateAuthorityAuditReport
- GetCertificate
- GetCertificateAuthorityCertificate
- GetCertificateAuthorityCsr
- GetPolicy
- ImportCertificateAuthorityCertificate
- IssueCertificate
- ListCertificateAuthorities
- ListPermissions
- ListTags
- PutPolicy
- RestoreCertificateAuthority
- RevokeCertificate
- TagCertificateAuthority
- UntagCertificateAuthority
- UpdateCertificateAuthority

CreateCertificateAuthority

Creates a root or subordinate private certificate authority (CA). You must specify the CA configuration, an optional configuration for Online Certificate Status Protocol (OCSP) and/or a certificate revocation list (CRL), the CA type, and an optional idempotency token to avoid accidental creation of multiple CAs. 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, and X.500 subject information. The OCSP configuration can optionally specify a custom URL for the OCSP responder. The CRL 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 action returns the Amazon Resource Name (ARN) of the CA.

> **Note**
>
> Both Amazon Private CA and the IAM principal must have permission to write to the S3 bucket that you specify. If the IAM principal making the call does not have permission to write to the bucket, then an exception is thrown. For more information, see Access policies for CRLs in Amazon S3.

Amazon Private CA assets that are stored in Amazon S3 can be protected with encryption. For more information, see Encrypting Your CRLs.

Request Syntax

```
{
   "CertificateAuthorityConfiguration": {
      "CsrExtensions": {
         "KeyUsage": {
            "CRLSign": boolean,
            "DataEncipherment": boolean,
            "DecipherOnly": boolean,
            "DigitalSignature": boolean,
            "EncipherOnly": boolean,
            "KeyAgreement": boolean,
            "KeyCertSign": boolean,
            "KeyEncipherment": boolean,
            "NonRepudiation": boolean
         },
```

```
      "SubjectInformationAccess": [
         {
            "AccessLocation": {
               "DirectoryName": {
                  "CommonName": "string",
                  "Country": "string",
                  "CustomAttributes": [
                     {
                        "ObjectIdentifier": "string",
                        "Value": "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"
               },
               "DnsName": "string",
               "EdiPartyName": {
                  "NameAssigner": "string",
                  "PartyName": "string"
               },
               "IpAddress": "string",
               "OtherName": {
                  "TypeId": "string",
                  "Value": "string"
               },
               "RegisteredId": "string",
               "Rfc822Name": "string",
               "UniformResourceIdentifier": "string"
            },
            "AccessMethod": {
               "AccessMethodType": "string",
               "CustomObjectIdentifier": "string"
            }
         }
```

```
         ]
      },
      "KeyAlgorithm": "string",
      "SigningAlgorithm": "string",
      "Subject": {
         "CommonName": "string",
         "Country": "string",
         "CustomAttributes": [
            {
               "ObjectIdentifier": "string",
               "Value": "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",
   "KeyStorageSecurityStandard": "string",
   "RevocationConfiguration": {
      "CrlConfiguration": {
         "CrlDistributionPointExtensionConfiguration": {
            "OmitExtension": boolean
         },
         "CrlType": "string",
         "CustomCname": "string",
         "CustomPath": "string",
         "Enabled": boolean,
         "ExpirationInDays": number,
         "S3BucketName": "string",
         "S3ObjectAcl": "string"
      },
      "OcspConfiguration": {
```

```
         "Enabled": boolean,
         "OcspCustomCname": "string"
      }
   },
   "Tags": [
      {
         "Key": "string",
         "Value": "string"
      }
   ],
   "UsageMode": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

CertificateAuthorityConfiguration

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

Type: CertificateAuthorityConfiguration object

Required: Yes

CertificateAuthorityType

The type of the certificate authority.

Type: String

Valid Values: `ROOT | SUBORDINATE`

Required: Yes

IdempotencyToken

Custom string that can be used to distinguish between calls to the **CreateCertificateAuthority** action. Idempotency tokens for **CreateCertificateAuthority** time out after five minutes. Therefore, if you call **CreateCertificateAuthority** multiple times with the same idempotency

token within five minutes, Amazon Private CA recognizes that you are requesting only certificate authority and will issue only one. If you change the idempotency token for each call, Amazon Private CA recognizes that you are requesting multiple certificate authorities.

Type: String

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

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

Required: No

KeyStorageSecurityStandard

Specifies a cryptographic key management compliance standard for handling and protecting CA keys.

Default: FIPS_140_2_LEVEL_3_OR_HIGHER

> **Note**
>
> Some Amazon Regions don't support the default value. When you create a CA in these Regions, you must use `CCPC_LEVEL_1_OR_HIGHER` for the `KeyStorageSecurityStandard` parameter. If you don't, the operation returns an `InvalidArgsException` with this message: "A certificate authority cannot be created in this region with the specified security standard."
> For information about security standard support in different Amazon Regions, see Storage and security compliance of Amazon Private CA private keys.

Type: String

Valid Values: `FIPS_140_2_LEVEL_2_OR_HIGHER | FIPS_140_2_LEVEL_3_OR_HIGHER | CCPC_LEVEL_1_OR_HIGHER`

Required: No

RevocationConfiguration

Contains information to enable support for Online Certificate Status Protocol (OCSP), certificate revocation list (CRL), both protocols, or neither. By default, both certificate validation mechanisms are disabled.

The following requirements apply to revocation configurations.

- A configuration disabling CRLs or OCSP must contain only the `Enabled=False` parameter, and will fail if other parameters such as `CustomCname` or `ExpirationInDays` are included.
- In a CRL configuration, the `S3BucketName` parameter must conform to Amazon S3 bucket naming rules.
- A configuration containing a custom Canonical Name (CNAME) parameter for CRLs or OCSP must conform to RFC2396 restrictions on the use of special characters in a CNAME.
- In a CRL or OCSP configuration, the value of a CNAME parameter must not include a protocol prefix such as "http://" or "https://".

For more information, see the OcspConfiguration and CrlConfiguration types.

Type: RevocationConfiguration object

Required: No

Tags

Key-value pairs that will be attached to the new private CA. You can associate up to 50 tags with a private CA. For information using tags with IAM to manage permissions, see Controlling Access Using IAM Tags.

Type: Array of Tag objects

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

Required: No

UsageMode

Specifies whether the CA issues general-purpose certificates that typically require a revocation mechanism, or short-lived certificates that may optionally omit revocation because they expire quickly. Short-lived certificate validity is limited to seven days.

The default value is GENERAL_PURPOSE.

Type: String

Valid Values: `GENERAL_PURPOSE | SHORT_LIVED_CERTIFICATE`

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

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

Errors

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

InvalidArgsException

One or more of the specified arguments was not valid.

HTTP Status Code: 400

InvalidPolicyException

The resource policy is invalid or is missing a required statement. For general information about IAM policy and statement structure, see Overview of JSON Policies.

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 Amazon Private CA quota has been exceeded. See the exception message returned to determine the quota that was exceeded.

HTTP Status Code: 400

Examples

Example

This example illustrates one usage of CreateCertificateAuthority.

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: 20210310T165448Z
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,
         "ExpirationInDays":7,
         "S3BucketName":"amzn-s3-demo-bucket"
      },
      "OcspConfiguration":{
         "Enabled":false
      }
   }
}
```

Example

This example illustrates one usage of CreateCertificateAuthority.

Sample Response

```
HTTP/1.1 200 OK
Date: Tue, 10 March 2021 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 Amazon SDKs, see the following:

- Amazon Command Line Interface
- Amazon SDK for .NET
- Amazon SDK for C++
- Amazon SDK for Go v2
- Amazon SDK for Java V2
- Amazon SDK for JavaScript V3
- Amazon SDK for Kotlin
- Amazon SDK for PHP V3
- Amazon SDK for Python
- Amazon SDK for Ruby V3

CreateCertificateAuthorityAuditReport

Creates an audit report that lists every time that your CA private key is used to issue a certificate. The IssueCertificate and RevokeCertificate actions use the private key.

To save the audit report to your designated Amazon S3 bucket, you must create a bucket policy that grants Amazon Private CA permission to access and write to it. For an example policy, see Prepare an Amazon S3 bucket for audit reports.

Amazon Private CA assets that are stored in Amazon S3 can be protected with encryption. For more information, see Encrypting Your Audit Reports.

> **Note**
>
> You can generate a maximum of one 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.

The request accepts the following data in JSON format.

AuditReportResponseFormat

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

Type: String

Valid Values: `JSON | CSV`

Required: Yes

CertificateAuthorityArn

The 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+=/,.@-]+:acm-pca:[\w+=/,.@-]*:[0-9]*:[\w+=,.@-]+(/[\w+=,.@-]+)*`

Required: Yes

S3BucketName

The name of the S3 bucket that will contain the audit report.

Type: String

Length Constraints: Minimum length of 3. Maximum length of 63.

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

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

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

Type: String

Length Constraints: Minimum length of 0. Maximum length of 1024.

Errors

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

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 state of the private CA does not allow this action to occur.

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, audit report, or policy cannot be found.

HTTP Status Code: 400

Examples

Example

This example illustrates one usage of CreateCertificateAuthorityAuditReport.

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

This example illustrates one usage of CreateCertificateAuthorityAuditReport.

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-report/PCA_ID/9654b603-d6a9-4c57-952a-ebcc95631fab.json"
}
```

See Also

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

- Amazon Command Line Interface
- Amazon SDK for .NET
- Amazon SDK for C++
- Amazon SDK for Go v2
- Amazon SDK for Java V2
- Amazon SDK for JavaScript V3
- Amazon SDK for Kotlin
- Amazon SDK for PHP V3
- Amazon SDK for Python
- Amazon SDK for Ruby V3

CreatePermission

Grants one or more permissions on a private CA to the Amazon Certificate Manager (ACM) service principal (`acm.amazonaws.com`). These permissions allow ACM to issue and renew ACM certificates that reside in the same Amazon account as the CA.

You can list current permissions with the ListPermissions action and revoke them with the DeletePermission action.

About Permissions

- If the private CA and the certificates it issues reside in the same account, you can use `CreatePermission` to grant permissions for ACM to carry out automatic certificate renewals.
- For automatic certificate renewal to succeed, the ACM service principal needs permissions to create, retrieve, and list certificates.
- If the private CA and the ACM certificates reside in different accounts, then permissions cannot be used to enable automatic renewals. Instead, the ACM certificate owner must set up a resource-based policy to enable cross-account issuance and renewals. For more information, see Using a Resource Based Policy with Amazon Private CA.

Request Syntax

```
{
   "Actions": [ "string" ],
   "CertificateAuthorityArn": "string",
   "Principal": "string",
   "SourceAccount": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

Actions

The actions that the specified Amazon service principal can use. These include `IssueCertificate`, `GetCertificate`, and `ListPermissions`.

Type: Array of strings

Array Members: Minimum number of 1 item. Maximum number of 3 items.

Valid Values: `IssueCertificate | GetCertificate | ListPermissions`

Required: Yes

CertificateAuthorityArn

The Amazon Resource Name (ARN) of the CA that grants the permissions. You can find the ARN by calling the ListCertificateAuthorities action. 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+=/,.@-]+:acm-pca:[\w+=/,.@-]*:[0-9]*:[\w+=,.@-]+(/[\w+=,.@-]+)*`

Required: Yes

Principal

The Amazon service or identity that receives the permission. At this time, the only valid principal is `acm.amazonaws.com`.

Type: String

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

Pattern: `[^*]+`

Required: Yes

SourceAccount

The ID of the calling account.

Type: String

Length Constraints: Fixed length of 12.

Pattern: `[0-9]+`

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.

InvalidArnException

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

HTTP Status Code: 400

InvalidStateException

The state of the private CA does not allow this action to occur.

HTTP Status Code: 400

LimitExceededException

An Amazon Private CA quota has been exceeded. See the exception message returned to determine the quota that was exceeded.

HTTP Status Code: 400

PermissionAlreadyExistsException

The designated permission has already been given to the user.

HTTP Status Code: 400

RequestFailedException

The request has failed for an unspecified reason.

HTTP Status Code: 400

ResourceNotFoundException

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

HTTP Status Code: 400

Examples

Example

This example illustrates one usage of CreatePermission.

Sample Request

```
POST / HTTP/1.1
Host: acm.us-east-1.privateca/latest/APIReference/
X-Amz-Target: CertificateManager.CreatePermission
X-Amz-Date: 20190207T170903Z
User-Agent: aws-cli/1.10.20 Python/2.7.3 Linux/3.13.0-83-generic botocore/1.4.11
Content-Type: application/x-amz-json-1.1
Authorization: AUTHPARAMS,
SignedHeaders=content-type;host;user-agent;x-amz-date;x-amz-target,
Signature=379429306c5e89b9b4be5b35e29c26cc1da38215d8055a5ed0bdda57bcc881cc

{
  "Actions": {
    "IssueCertificate",
    "GetCertificate",
    "ListPermissions"
  },
  "CertificateArn":"arn:aws:acm:us-east-1:111122223333:certificate-
authority/01234567-89ab-cdef-0123-0123456789ab",
  "Principal":"acm.amazonaws.com",
  "SourceAccount":"012345678901"
}
```

Example

This example illustrates one usage of CreatePermission.

Sample Response

```
HTTP/1.1 200 OK
x-amzn-RequestId: 3c8d676d-025e-11e6-8823-93164b47113c
Content-Type: application/x-amz-json-1.1
Content-Length: 0
```

```
Date: Thu, Feb 7 2019 17:09:05 GMT
```

See Also

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

- Amazon Command Line Interface
- Amazon SDK for .NET
- Amazon SDK for C++
- Amazon SDK for Go v2
- Amazon SDK for Java V2
- Amazon SDK for JavaScript V3
- Amazon SDK for Kotlin
- Amazon SDK for PHP V3
- Amazon SDK for Python
- Amazon SDK for Ruby V3

DeleteCertificateAuthority

Deletes a private certificate authority (CA). You must provide the Amazon Resource Name (ARN) of the private CA that you want to delete. You can find the ARN by calling the ListCertificateAuthorities action.

> **Note**
>
> Deleting a CA will invalidate other CAs and certificates below it in your CA hierarchy.

Before you can delete a CA that you have created and activated, you must disable it. To do this, call the UpdateCertificateAuthority action and set the **CertificateAuthorityStatus** parameter to `DISABLED`.

Additionally, you can delete a CA if you are waiting for it to be created (that is, the status of the CA is `CREATING`). You can also delete it if the CA has been created but you haven't yet imported the signed certificate into Amazon Private CA (that is, the status of the CA is `PENDING_CERTIFICATE`).

When you successfully call DeleteCertificateAuthority, the CA's status changes to `DELETED`. However, the CA won't be permanently 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 action returns the time remaining in the restoration window of a private CA in the `DELETED` state. To restore an eligible CA, call the RestoreCertificateAuthority action.

> **Important**
>
> A private CA can be deleted if it is in the `PENDING_CERTIFICATE`, `CREATING`, `EXPIRED`, `DISABLED`, or `FAILED` state. To delete a CA in the `ACTIVE` state, you must first disable it, or else the delete request results in an exception. If you are deleting a private CA in the `PENDING_CERTIFICATE` or `DISABLED` state, you can set the length of its restoration period to 7-30 days. The default is 30. During this time, the status is set to `DELETED` and the CA can be restored. A private CA deleted in the `CREATING` or `FAILED` state has no assigned restoration period and cannot be restored.

Request Syntax

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

Request Parameters

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

The request accepts the following data in JSON format.

CertificateAuthorityArn

The Amazon Resource Name (ARN) that was returned when you called CreateCertificateAuthority. 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+=/,.@-]+:acm-pca:[\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

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.

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 state of the private CA does not allow this action to occur.

HTTP Status Code: 400

ResourceNotFoundException

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

HTTP Status Code: 400

Examples

Example

This example illustrates one usage of DeleteCertificateAuthority.

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

This example illustrates one usage of DeleteCertificateAuthority.

Sample Response

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

See Also

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

- Amazon Command Line Interface
- Amazon SDK for .NET
- Amazon SDK for C++
- Amazon SDK for Go v2
- Amazon SDK for Java V2
- Amazon SDK for JavaScript V3
- Amazon SDK for Kotlin
- Amazon SDK for PHP V3
- Amazon SDK for Python
- Amazon SDK for Ruby V3

DeletePermission

Revokes permissions on a private CA granted to the Amazon Certificate Manager (ACM) service principal (acm.amazonaws.com).

These permissions allow ACM to issue and renew ACM certificates that reside in the same Amazon account as the CA. If you revoke these permissions, ACM will no longer renew the affected certificates automatically.

Permissions can be granted with the CreatePermission action and listed with the ListPermissions action.

About Permissions

- If the private CA and the certificates it issues reside in the same account, you can use `CreatePermission` to grant permissions for ACM to carry out automatic certificate renewals.
- For automatic certificate renewal to succeed, the ACM service principal needs permissions to create, retrieve, and list certificates.
- If the private CA and the ACM certificates reside in different accounts, then permissions cannot be used to enable automatic renewals. Instead, the ACM certificate owner must set up a resource-based policy to enable cross-account issuance and renewals. For more information, see Using a Resource Based Policy with Amazon Private CA.

Request Syntax

```
{
   "CertificateAuthorityArn": "string",
   "Principal": "string",
   "SourceAccount": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

CertificateAuthorityArn

The Amazon Resource Number (ARN) of the private CA that issued the permissions. You can find the CA's ARN by calling the ListCertificateAuthorities action. 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+=/,.@-]+:acm-pca:[\w+=/,.@-]*:[0-9]*:[\w+=,.@-]+(/[\w+=,.@-]+)*`

Required: Yes

Principal

The Amazon service or identity that will have its CA permissions revoked. At this time, the only valid service principal is `acm.amazonaws.com`

Type: String

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

Pattern: `[^*]+`

Required: Yes

SourceAccount

The Amazon account that calls this action.

Type: String

Length Constraints: Fixed length of 12.

Pattern: `[0-9]+`

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.

InvalidArnException

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

HTTP Status Code: 400

InvalidStateException

The state of the private CA does not allow this action to occur.

HTTP Status Code: 400

RequestFailedException

The request has failed for an unspecified reason.

HTTP Status Code: 400

ResourceNotFoundException

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

HTTP Status Code: 400

See Also

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

- Amazon Command Line Interface
- Amazon SDK for .NET
- Amazon SDK for C++
- Amazon SDK for Go v2
- Amazon SDK for Java V2
- Amazon SDK for JavaScript V3
- Amazon SDK for Kotlin
- Amazon SDK for PHP V3

- Amazon SDK for Python
- Amazon SDK for Ruby V3

DeletePolicy

Deletes the resource-based policy attached to a private CA. Deletion will remove any access that the policy has granted. If there is no policy attached to the private CA, this action will return successful.

If you delete a policy that was applied through Amazon Resource Access Manager (RAM), the CA will be removed from all shares in which it was included.

The Amazon Certificate Manager Service Linked Role that the policy supports is not affected when you delete the policy.

The current policy can be shown with GetPolicy and updated with PutPolicy.

About Policies

- A policy grants access on a private CA to an Amazon customer account, to Amazon Organizations, or to an Amazon Organizations unit. Policies are under the control of a CA administrator. For more information, see Using a Resource Based Policy with Amazon Private CA.
- A policy permits a user of Amazon Certificate Manager (ACM) to issue ACM certificates signed by a CA in another account.
- For ACM to manage automatic renewal of these certificates, the ACM user must configure a Service Linked Role (SLR). The SLR allows the ACM service to assume the identity of the user, subject to confirmation against the Amazon Private CA policy. For more information, see Using a Service Linked Role with ACM.
- Updates made in Amazon Resource Manager (RAM) are reflected in policies. For more information, see Attach a Policy for Cross-Account Access.

Request Syntax

```
{
   "ResourceArn": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

ResourceArn

The Amazon Resource Number (ARN) of the private CA that will have its policy deleted. You can find the CA's ARN by calling the ListCertificateAuthorities action. The ARN value must have the form `arn:aws:acm-pca:region:account:certificate-authority/01234567-89ab-cdef-0123-0123456789ab`.

Type: String

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

Pattern: `arn:[\w+=/,.@-]+:acm-pca:[\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.

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 state of the private CA does not allow this action to occur.

HTTP Status Code: 400

LockoutPreventedException

The current action was prevented because it would lock the caller out from performing subsequent actions. Verify that the specified parameters would not result in the caller being denied access to the resource.

HTTP Status Code: 400

RequestFailedException

The request has failed for an unspecified reason.

HTTP Status Code: 400

ResourceNotFoundException

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

HTTP Status Code: 400

See Also

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

- Amazon Command Line Interface
- Amazon SDK for .NET
- Amazon SDK for C++
- Amazon SDK for Go v2
- Amazon SDK for Java V2
- Amazon SDK for JavaScript V3
- Amazon SDK for Kotlin
- Amazon SDK for PHP V3
- Amazon SDK for Python
- Amazon SDK for Ruby V3

DescribeCertificateAuthority

Lists information about your private certificate authority (CA) or one that has been shared with you. 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` - Amazon Private CA is creating your private certificate authority.
- `PENDING_CERTIFICATE` - The certificate is pending. You must use your Amazon Private CA-hosted or on-premises root or subordinate CA to sign your private CA CSR and then import it into Amazon Private CA.
- `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 back-end Amazon 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 action's output.

Request Syntax

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

Request Parameters

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

The request accepts the following data in JSON format.

CertificateAuthorityArn

The Amazon Resource Name (ARN) that was returned when you called CreateCertificateAuthority. 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+=/,.@-]+:acm-pca:[\w+=/,.@-]*:[0-9]*:[\w+=,.@-]+(/[\w+=,.@-]+)*`

Required: Yes

Response Syntax

```
{
   "CertificateAuthority": {
      "Arn": "string",
      "CertificateAuthorityConfiguration": {
         "CsrExtensions": {
            "KeyUsage": {
               "CRLSign": boolean,
               "DataEncipherment": boolean,
               "DecipherOnly": boolean,
               "DigitalSignature": boolean,
               "EncipherOnly": boolean,
               "KeyAgreement": boolean,
               "KeyCertSign": boolean,
               "KeyEncipherment": boolean,
               "NonRepudiation": boolean
            },
            "SubjectInformationAccess": [
               {
                  "AccessLocation": {
                     "DirectoryName": {
                        "CommonName": "string",
                        "Country": "string",
                        "CustomAttributes": [
                           {
                              "ObjectIdentifier": "string",
                              "Value": "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"
                     },
                     "DnsName": "string",
                     "EdiPartyName": {
                        "NameAssigner": "string",
                        "PartyName": "string"
                     },
                     "IpAddress": "string",
                     "OtherName": {
                        "TypeId": "string",
                        "Value": "string"
                     },
                     "RegisteredId": "string",
                     "Rfc822Name": "string",
                     "UniformResourceIdentifier": "string"
                  },
                  "AccessMethod": {
                     "AccessMethodType": "string",
                     "CustomObjectIdentifier": "string"
                  }
               }
            ]
         },
         "KeyAlgorithm": "string",
         "SigningAlgorithm": "string",
         "Subject": {
            "CommonName": "string",
            "Country": "string",
            "CustomAttributes": [
               {
                  "ObjectIdentifier": "string",
                  "Value": "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",
      "KeyStorageSecurityStandard": "string",
      "LastStateChangeAt": number,
      "NotAfter": number,
      "NotBefore": number,
      "OwnerAccount": "string",
      "RestorableUntil": number,
      "RevocationConfiguration": {
         "CrlConfiguration": {
            "CrlDistributionPointExtensionConfiguration": {
               "OmitExtension": boolean
            },
            "CrlType": "string",
            "CustomCname": "string",
            "CustomPath": "string",
            "Enabled": boolean,
            "ExpirationInDays": number,
            "S3BucketName": "string",
            "S3ObjectAcl": "string"
         },
         "OcspConfiguration": {
            "Enabled": boolean,
            "OcspCustomCname": "string"
         }
      },
      "Serial": "string",
      "Status": "string",
      "Type": "string",
      "UsageMode": "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

A CertificateAuthority structure that contains information about your private CA.

Type: CertificateAuthority object

Errors

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

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, audit report, or policy cannot be found.

HTTP Status Code: 400

Examples

Example

This example illustrates one usage of DescribeCertificateAuthority.

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

This example illustrates one usage of DescribeCertificateAuthority.

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 Amazon SDKs, see the following:

- Amazon Command Line Interface
- Amazon SDK for .NET
- Amazon SDK for C++
- Amazon SDK for Go v2
- Amazon SDK for Java V2
- Amazon SDK for JavaScript V3
- Amazon SDK for Kotlin
- Amazon SDK for PHP V3
- Amazon SDK for Python
- Amazon SDK for Ruby V3

DescribeCertificateAuthorityAuditReport

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

Request Syntax

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

Request Parameters

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

The request accepts the following data in JSON format.

AuditReportId

The report ID returned by calling the CreateCertificateAuthorityAuditReport action.

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

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+=/,.@-]+:acm-pca:[\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

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

Type: String

Valid Values: `CREATING | SUCCESS | FAILED`

CreatedAt

The date and time at which the report was created.

Type: Timestamp

S3BucketName

Name of the S3 bucket that contains the report.

Type: String

Length Constraints: Minimum length of 3. Maximum length of 63.

S3Key

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

Type: String

Length Constraints: Minimum length of 0. Maximum length of 1024.

Errors

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

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, audit report, or policy cannot be found.

HTTP Status Code: 400

Examples

Example

This example illustrates one usage of DescribeCertificateAuthorityAuditReport.

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

This example illustrates one usage of DescribeCertificateAuthorityAuditReport.

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 Amazon SDKs, see the following:

- Amazon Command Line Interface
- Amazon SDK for .NET

- Amazon SDK for C++
- Amazon SDK for Go v2
- Amazon SDK for Java V2
- Amazon SDK for JavaScript V3
- Amazon SDK for Kotlin
- Amazon SDK for PHP V3
- Amazon SDK for Python
- Amazon SDK for Ruby V3

GetCertificate

Retrieves a certificate from your private CA or one that has been shared with you. The ARN of the certificate is returned when you call the IssueCertificate action. You must specify both the ARN of your private CA and the ARN of the issued certificate when calling the **GetCertificate** action. You can retrieve the certificate if it is in the **ISSUED** state. You can call the CreateCertificateAuthorityAuditReport action 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.

The request accepts the following data in JSON format.

CertificateArn

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

Required: Yes

CertificateAuthorityArn

The Amazon Resource Name (ARN) that was returned when you called CreateCertificateAuthority. 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+=/,.@-]+:acm-pca:[\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

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

Type: String

CertificateChain

The base64 PEM-encoded certificate chain that chains up to the 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.

InvalidArnException

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

HTTP Status Code: 400

InvalidStateException

The state of the private CA does not allow this action to occur.

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, audit report, or policy cannot be found.

HTTP Status Code: 400

Examples

Example

This example illustrates one usage of GetCertificate.

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

This example illustrates one usage of GetCertificate.

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 Amazon SDKs, see the following:

- Amazon Command Line Interface
- Amazon SDK for .NET
- Amazon SDK for C++
- Amazon SDK for Go v2
- Amazon SDK for Java V2
- Amazon SDK for JavaScript V3
- Amazon SDK for Kotlin
- Amazon SDK for PHP V3
- Amazon SDK for Python
- Amazon SDK for Ruby V3

GetCertificateAuthorityCertificate

Retrieves the certificate and certificate chain for your private certificate authority (CA) or one that has been shared with you. 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.

The request accepts the following data in JSON format.

CertificateAuthorityArn

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+=/,.@-]+:acm-pca:[\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

Base64-encoded certificate authority (CA) certificate.

Type: String

CertificateChain

Base64-encoded certificate chain that includes any intermediate certificates and chains up to root certificate that you used to sign your private CA certificate. The chain does not include your private CA certificate. If this is a root CA, the value will be null.

Type: String

Errors

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

InvalidArnException

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

HTTP Status Code: 400

InvalidStateException

The state of the private CA does not allow this action to occur.

HTTP Status Code: 400

ResourceNotFoundException

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

HTTP Status Code: 400

Examples

Example

This example illustrates one usage of GetCertificateAuthorityCertificate.

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

This example illustrates one usage of GetCertificateAuthorityCertificate.

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 Amazon SDKs, see the following:

- Amazon Command Line Interface
- Amazon SDK for .NET
- Amazon SDK for C++
- Amazon SDK for Go v2
- Amazon SDK for Java V2
- Amazon SDK for JavaScript V3
- Amazon SDK for Kotlin
- Amazon SDK for PHP V3
- Amazon SDK for Python
- Amazon SDK for Ruby V3

GetCertificateAuthorityCsr

Retrieves the certificate signing request (CSR) for your private certificate authority (CA). The CSR is created when you call the CreateCertificateAuthority action. Sign the CSR with your Amazon Private CA-hosted or on-premises root or subordinate CA. Then import the signed certificate back into Amazon Private CA by calling the ImportCertificateAuthorityCertificate action. 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.

The request accepts the following data in JSON format.

CertificateAuthorityArn

The Amazon Resource Name (ARN) that was returned when you called the CreateCertificateAuthority action. 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+=/,.@-]+:acm-pca:[\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

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.

InvalidArnException

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

HTTP Status Code: 400

InvalidStateException

The state of the private CA does not allow this action to occur.

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, audit report, or policy cannot be found.

HTTP Status Code: 400

Examples

Example

This example illustrates one usage of GetCertificateAuthorityCsr.

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

This example illustrates one usage of GetCertificateAuthorityCsr.

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 Amazon SDKs, see the following:

- Amazon Command Line Interface
- Amazon SDK for .NET
- Amazon SDK for C++
- Amazon SDK for Go v2
- Amazon SDK for Java V2
- Amazon SDK for JavaScript V3
- Amazon SDK for Kotlin
- Amazon SDK for PHP V3
- Amazon SDK for Python
- Amazon SDK for Ruby V3

GetPolicy

Retrieves the resource-based policy attached to a private CA. If either the private CA resource or the policy cannot be found, this action returns a `ResourceNotFoundException`.

The policy can be attached or updated with PutPolicy and removed with DeletePolicy.

About Policies

- A policy grants access on a private CA to an Amazon customer account, to Amazon Organizations, or to an Amazon Organizations unit. Policies are under the control of a CA administrator. For more information, see Using a Resource Based Policy with Amazon Private CA.
- A policy permits a user of Amazon Certificate Manager (ACM) to issue ACM certificates signed by a CA in another account.
- For ACM to manage automatic renewal of these certificates, the ACM user must configure a Service Linked Role (SLR). The SLR allows the ACM service to assume the identity of the user, subject to confirmation against the Amazon Private CA policy. For more information, see Using a Service Linked Role with ACM.
- Updates made in Amazon Resource Manager (RAM) are reflected in policies. For more information, see Attach a Policy for Cross-Account Access.

Request Syntax

```
{
   "ResourceArn": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

ResourceArn

The Amazon Resource Number (ARN) of the private CA that will have its policy retrieved. You can find the CA's ARN by calling the ListCertificateAuthorities action.

Type: String

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

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

Required: Yes

Response Syntax

```
{
   "Policy": "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.

Policy

The policy attached to the private CA as a JSON document.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 81920.

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

Errors

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

InvalidArnException

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

HTTP Status Code: 400

InvalidStateException

The state of the private CA does not allow this action to occur.

HTTP Status Code: 400

RequestFailedException

The request has failed for an unspecified reason.

HTTP Status Code: 400

ResourceNotFoundException

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

HTTP Status Code: 400

See Also

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

- Amazon Command Line Interface
- Amazon SDK for .NET
- Amazon SDK for C++
- Amazon SDK for Go v2
- Amazon SDK for Java V2
- Amazon SDK for JavaScript V3
- Amazon SDK for Kotlin
- Amazon SDK for PHP V3
- Amazon SDK for Python
- Amazon SDK for Ruby V3

ImportCertificateAuthorityCertificate

Imports a signed private CA certificate into Amazon Private CA. This action is used when you are using a chain of trust whose root is located outside Amazon Private CA. Before you can call this action, the following preparations must in place:

1. In Amazon Private CA, call the CreateCertificateAuthority action to create the private CA that you plan to back with the imported certificate.
2. Call the GetCertificateAuthorityCsr action to generate a certificate signing request (CSR).
3. Sign the CSR using a root or intermediate CA hosted by either an on-premises PKI hierarchy or by a commercial CA.
4. Create a certificate chain and copy the signed certificate and the certificate chain to your working directory.

Amazon Private CA supports three scenarios for installing a CA certificate:

- Installing a certificate for a root CA hosted by Amazon Private CA.
- Installing a subordinate CA certificate whose parent authority is hosted by Amazon Private CA.
- Installing a subordinate CA certificate whose parent authority is externally hosted.

The following additional requirements apply when you import a CA certificate.

- Only a self-signed certificate can be imported as a root CA.
- A self-signed certificate cannot be imported as a subordinate CA.
- Your certificate chain must not include the private CA certificate that you are importing.
- Your root CA 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.
- The chain must be PEM-encoded.
- The maximum allowed size of a certificate is 32 KB.
- The maximum allowed size of a certificate chain is 2 MB.

Enforcement of Critical Constraints

Amazon Private CA allows the following extensions to be marked critical in the imported CA certificate or chain.

- Authority key identifier
- Basic constraints (*must* be marked critical)
- Certificate policies
- Extended key usage
- Inhibit anyPolicy
- Issuer alternative name
- Key usage
- Name constraints
- Policy mappings
- Subject alternative name
- Subject directory attributes
- Subject key identifier
- Subject information access

Amazon Private CA rejects the following extensions when they are marked critical in an imported CA certificate or chain.

- Authority information access
- CRL distribution points
- Freshest CRL
- Policy constraints

Amazon Private Certificate Authority will also reject any other extension marked as critical not contained on the preceding list of allowed extensions.

Request Syntax

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

```
}
```

Request Parameters

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

The request accepts the following data in JSON format.

Certificate

The PEM-encoded certificate for a private CA. This may be a self-signed certificate in the case of a root CA, or it may be signed by another CA that you control.

Type: Base64-encoded binary data object

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

Required: Yes

CertificateAuthorityArn

The Amazon Resource Name (ARN) that was returned when you called CreateCertificateAuthority. 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+=/,.@-]+:acm-pca:[\w+=/,.@-]*:[0-9]*:[\w+=,.@-]+(/[\w+=,.@-]+)*`

Required: Yes

CertificateChain

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

This parameter must be supplied when you import a subordinate CA. When you import a root CA, there is no chain.

Type: Base64-encoded binary data object

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

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.

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

InvalidRequestException

The request action cannot be performed or is prohibited.

HTTP Status Code: 400

InvalidStateException

The state of the private CA does not allow this action to occur.

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, audit report, or policy cannot be found.

HTTP Status Code: 400

Examples

Example

This example illustrates one usage of ImportCertificateAuthorityCertificate.

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

This example illustrates one usage of ImportCertificateAuthorityCertificate.

Sample Response

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

See Also

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

- Amazon Command Line Interface
- Amazon SDK for .NET
- Amazon SDK for C++
- Amazon SDK for Go v2
- Amazon SDK for Java V2
- Amazon SDK for JavaScript V3
- Amazon SDK for Kotlin
- Amazon SDK for PHP V3
- Amazon SDK for Python
- Amazon SDK for Ruby V3

IssueCertificate

Uses your private certificate authority (CA), or one that has been shared with you, to issue a client certificate. This action returns the Amazon Resource Name (ARN) of the certificate. You can retrieve the certificate by calling the GetCertificate action and specifying the ARN.

> **Note**
>
> You cannot use the ACM **ListCertificateAuthorities** action to retrieve the ARNs of the certificates that you issue by using Amazon Private CA.

Request Syntax

```
{
   "ApiPassthrough": {
      "Extensions": {
         "CertificatePolicies": [
            {
               "CertPolicyId": "string",
               "PolicyQualifiers": [
                  {
                     "PolicyQualifierId": "string",
                     "Qualifier": {
                        "CpsUri": "string"
                     }
                  }
               ]
            }
         ],
         "CustomExtensions": [
            {
               "Critical": boolean,
               "ObjectIdentifier": "string",
               "Value": "string"
            }
         ],
         "ExtendedKeyUsage": [
            {
               "ExtendedKeyUsageObjectIdentifier": "string",
               "ExtendedKeyUsageType": "string"
```

```
            }
         ],
         "KeyUsage": {
            "CRLSign": boolean,
            "DataEncipherment": boolean,
            "DecipherOnly": boolean,
            "DigitalSignature": boolean,
            "EncipherOnly": boolean,
            "KeyAgreement": boolean,
            "KeyCertSign": boolean,
            "KeyEncipherment": boolean,
            "NonRepudiation": boolean
         },
         "SubjectAlternativeNames": [
            {
               "DirectoryName": {
                  "CommonName": "string",
                  "Country": "string",
                  "CustomAttributes": [
                     {
                        "ObjectIdentifier": "string",
                        "Value": "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"
               },
               "DnsName": "string",
               "EdiPartyName": {
                  "NameAssigner": "string",
                  "PartyName": "string"
               },
               "IpAddress": "string",
               "OtherName": {
```

```
                "TypeId": "string",
                "Value": "string"
            },
            "RegisteredId": "string",
            "Rfc822Name": "string",
            "UniformResourceIdentifier": "string"
         }
      ]
   },
   "Subject": {
      "CommonName": "string",
      "Country": "string",
      "CustomAttributes": [
         {
            "ObjectIdentifier": "string",
            "Value": "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"
   }
},
"CertificateAuthorityArn": "string",
"Csr": blob,
"IdempotencyToken": "string",
"SigningAlgorithm": "string",
"TemplateArn": "string",
"Validity": {
   "Type": "string",
   "Value": number
},
"ValidityNotBefore": {
   "Type": "string",
   "Value": number
```

```
    }
}
```

Request Parameters

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

The request accepts the following data in JSON format.

ApiPassthrough

Specifies X.509 certificate information to be included in the issued certificate. An `APIPassthrough` or `APICSRPassthrough` template variant must be selected, or else this parameter is ignored. For more information about using these templates, see Understanding Certificate Templates.

If conflicting or duplicate certificate information is supplied during certificate issuance, Amazon Private CA applies order of operation rules to determine what information is used.

Type: ApiPassthrough object

Required: No

CertificateAuthorityArn

The Amazon Resource Name (ARN) that was returned when you called CreateCertificateAuthority. 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+=/,.@-]+:acm-pca:[\w+=/,.@-]*:[0-9]*:[\w+=,.@-]+(/[\w+=,.@-]+)*`

Required: Yes

Csr

The certificate signing request (CSR) for the certificate you want to issue. As an example, 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 then 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
```

Note: A CSR must provide either a *subject name* or a *subject alternative name* or the request will be rejected.

Type: Base64-encoded binary data object

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

Required: Yes

IdempotencyToken

Alphanumeric string that can be used to distinguish between calls to the **IssueCertificate** action. Idempotency tokens for **IssueCertificate** time out after five minutes. Therefore, if you call **IssueCertificate** multiple times with the same idempotency token within five minutes, Amazon Private CA recognizes that you are requesting only one certificate and will issue only one. If you change the idempotency token for each call, Amazon Private CA 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

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

This parameter should not be confused with the `SigningAlgorithm` parameter used to sign a CSR in the `CreateCertificateAuthority` action.

> **Note**
>
> The specified signing algorithm family (RSA or ECDSA) must match the algorithm family of the CA's secret key.

Type: String

Valid Values: `SHA256WITHECDSA | SHA384WITHECDSA | SHA512WITHECDSA | SHA256WITHRSA | SHA384WITHRSA | SHA512WITHRSA | SM3WITHSM2`

Required: Yes

TemplateArn

Specifies a custom configuration template to use when issuing a certificate. If this parameter is not provided, Amazon Private CA defaults to the `EndEntityCertificate/V1` template. For CA certificates, you should choose the shortest path length that meets your needs. The path length is indicated by the PathLen*N* portion of the ARN, where *N* is the CA depth.

Note: The CA depth configured on a subordinate CA certificate must not exceed the limit set by its parents in the CA hierarchy.

For a list of `TemplateArn` values supported by Amazon Private CA, see Understanding Certificate Templates.

Type: String

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

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

Required: No

Validity

Information describing the end of the validity period of the certificate. This parameter sets the “Not After” date for the certificate.

Certificate validity is the period of time during which a certificate is valid. Validity can be expressed as an explicit date and time when the certificate expires, or as a span of time after issuance, stated in days, months, or years. For more information, see Validity in RFC 5280.

This value is unaffected when `ValidityNotBefore` is also specified. For example, if `Validity` is set to 20 days in the future, the certificate will expire 20 days from issuance time regardless of the `ValidityNotBefore` value.

The end of the validity period configured on a certificate must not exceed the limit set on its parents in the CA hierarchy.

Type: Validity object

Required: Yes

ValidityNotBefore

Information describing the start of the validity period of the certificate. This parameter sets the “Not Before" date for the certificate.

By default, when issuing a certificate, Amazon Private CA sets the "Not Before" date to the issuance time minus 60 minutes. This compensates for clock inconsistencies across computer systems. The `ValidityNotBefore` parameter can be used to customize the “Not Before” value.

Unlike the `Validity` parameter, the `ValidityNotBefore` parameter is optional.

The `ValidityNotBefore` value is expressed as an explicit date and time, using the `Validity` type value ABSOLUTE. For more information, see Validity in this API reference and Validity in RFC 5280.

Type: Validity object

Required: No

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

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

Errors

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

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 state of the private CA does not allow this action to occur.

HTTP Status Code: 400

LimitExceededException

An Amazon Private CA quota has been exceeded. See the exception message returned to determine the quota 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, audit report, or policy cannot be found.

HTTP Status Code: 400

Examples

Example

This example illustrates one usage of IssueCertificate.

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

This example illustrates one usage of IssueCertificate.

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 Amazon SDKs, see the following:

- Amazon Command Line Interface
- Amazon SDK for .NET
- Amazon SDK for C++
- Amazon SDK for Go v2
- Amazon SDK for Java V2
- Amazon SDK for JavaScript V3
- Amazon SDK for Kotlin
- Amazon SDK for PHP V3
- Amazon SDK for Python
- Amazon SDK for Ruby V3

ListCertificateAuthorities

Lists the private certificate authorities that you created by using the CreateCertificateAuthority action.

Request Syntax

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

Request Parameters

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

The request accepts the following data in JSON format.

MaxResults

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.

Although the maximum value is 1000, the action only returns a maximum of 100 items.

Type: Integer

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

Required: No

NextToken

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 43739.

Required: No

ResourceOwner

Use this parameter to filter the returned set of certificate authorities based on their owner. The default is SELF.

Type: String

Valid Values: `SELF | OTHER_ACCOUNTS`

Required: No

Response Syntax

```
{
   "CertificateAuthorities": [
      {
         "Arn": "string",
         "CertificateAuthorityConfiguration": {
            "CsrExtensions": {
               "KeyUsage": {
                  "CRLSign": boolean,
                  "DataEncipherment": boolean,
                  "DecipherOnly": boolean,
                  "DigitalSignature": boolean,
                  "EncipherOnly": boolean,
                  "KeyAgreement": boolean,
                  "KeyCertSign": boolean,
                  "KeyEncipherment": boolean,
                  "NonRepudiation": boolean
               },
               "SubjectInformationAccess": [
                  {
                     "AccessLocation": {
                        "DirectoryName": {
                           "CommonName": "string",
                           "Country": "string",
                           "CustomAttributes": [
                              {
                                 "ObjectIdentifier": "string",
                                 "Value": "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"
                     },
                     "DnsName": "string",
                     "EdiPartyName": {
                        "NameAssigner": "string",
                        "PartyName": "string"
                     },
                     "IpAddress": "string",
                     "OtherName": {
                        "TypeId": "string",
                        "Value": "string"
                     },
                     "RegisteredId": "string",
                     "Rfc822Name": "string",
                     "UniformResourceIdentifier": "string"
                  },
                  "AccessMethod": {
                     "AccessMethodType": "string",
                     "CustomObjectIdentifier": "string"
                  }
               }
            ]
         },
         "KeyAlgorithm": "string",
         "SigningAlgorithm": "string",
         "Subject": {
            "CommonName": "string",
            "Country": "string",
            "CustomAttributes": [
               {
                  "ObjectIdentifier": "string",
                  "Value": "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",
   "KeyStorageSecurityStandard": "string",
   "LastStateChangeAt": number,
   "NotAfter": number,
   "NotBefore": number,
   "OwnerAccount": "string",
   "RestorableUntil": number,
   "RevocationConfiguration": {
      "CrlConfiguration": {
         "CrlDistributionPointExtensionConfiguration": {
            "OmitExtension": boolean
         },
         "CrlType": "string",
         "CustomCname": "string",
         "CustomPath": "string",
         "Enabled": boolean,
         "ExpirationInDays": number,
         "S3BucketName": "string",
         "S3ObjectAcl": "string"
      },
      "OcspConfiguration": {
         "Enabled": boolean,
         "OcspCustomCname": "string"
      }
   },
   "Serial": "string",
   "Status": "string",
```

```
            "Type": "string",
            "UsageMode": "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

Summary information about each certificate authority you have created.

Type: Array of CertificateAuthority objects

NextToken

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 43739.

Errors

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

InvalidNextTokenException

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

HTTP Status Code: 400

Examples

Example

This example illustrates one usage of ListCertificateAuthorities.

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

This example illustrates one usage of ListCertificateAuthorities.

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 Amazon SDKs, see the following:

- Amazon Command Line Interface
- Amazon SDK for .NET
- Amazon SDK for C++
- Amazon SDK for Go v2
- Amazon SDK for Java V2
- Amazon SDK for JavaScript V3
- Amazon SDK for Kotlin
- Amazon SDK for PHP V3
- Amazon SDK for Python
- Amazon SDK for Ruby V3

ListPermissions

List all permissions on a private CA, if any, granted to the Amazon Certificate Manager (ACM) service principal (acm.amazonaws.com).

These permissions allow ACM to issue and renew ACM certificates that reside in the same Amazon account as the CA.

Permissions can be granted with the CreatePermission action and revoked with the DeletePermission action.

About Permissions

- If the private CA and the certificates it issues reside in the same account, you can use `CreatePermission` to grant permissions for ACM to carry out automatic certificate renewals.
- For automatic certificate renewal to succeed, the ACM service principal needs permissions to create, retrieve, and list certificates.
- If the private CA and the ACM certificates reside in different accounts, then permissions cannot be used to enable automatic renewals. Instead, the ACM certificate owner must set up a resource-based policy to enable cross-account issuance and renewals. For more information, see Using a Resource Based Policy with Amazon Private CA.

Request Syntax

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

Request Parameters

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

The request accepts the following data in JSON format.

CertificateAuthorityArn

The Amazon Resource Number (ARN) of the private CA to inspect. You can find the ARN by calling the ListCertificateAuthorities action. This must be of the form: `arn:aws:acm-pca:region:account:certificate-authority/12345678-1234-1234-1234-123456789012` You can get a private CA's ARN by running the ListCertificateAuthorities action.

Type: String

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

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

Required: Yes

MaxResults

When paginating results, use this parameter 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

When paginating results, use this parameter 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 43739.

Required: No

Response Syntax

```
{
   "NextToken": "string",
   "Permissions": [
      {
         "Actions": [ "string" ],
         "CertificateAuthorityArn": "string",
         "CreatedAt": number,
         "Policy": "string",
         "Principal": "string",
         "SourceAccount": "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

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 43739.

Permissions

Summary information about each permission assigned by the specified private CA, including the action enabled, the policy provided, and the time of creation.

Type: Array of Permission objects

Array Members: Minimum number of 0 items.

Errors

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

InvalidArnException

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

HTTP Status Code: 400

InvalidNextTokenException

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

HTTP Status Code: 400

InvalidStateException

The state of the private CA does not allow this action to occur.

HTTP Status Code: 400

RequestFailedException

The request has failed for an unspecified reason.

HTTP Status Code: 400

ResourceNotFoundException

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

HTTP Status Code: 400

Examples

Example

This example illustrates one usage of ListPermissions.

Sample Request

```
POST / HTTP/1.1
Host: acm.us-east-1.privateca/latest/APIReference/
X-Amz-Target: CertificateManager.ListPermissions
X-Amz-Date: 20190113T171333Z
User-Agent: aws-cli/1.10.20 Python/2.7.3 Linux/3.13.0-83-generic botocore/1.4.11
Content-Type: application/x-amz-json-1.1
```

```
Authorization: AUTHPARAMS,
SignedHeaders=content-type;host;user-agent;x-amz-date;x-amz-target,
Signature=3c9429306c5a99b9b4be5b35f55c26cc1da32a215d8055a5ed0bdda57bcc881cc

{
  "CertificateArn":"arn:aws:acm:us-east-1:111122223333:certificate-
authority/01234567-89ab-cdef-0123-0123456789ab",
  "MaxResults": 10
}
```

Example

This example illustrates one usage of ListPermissions.

Sample Response

```
HTTP/1.1 200 OK
x-amzn-RequestId: 3c8d676d-025e-11e6-8823-93164b47113c
Content-Type: application/x-amz-json-1.1
Content-Length: 579
Date: Thu, Feb 13 2019 17:13:36 GMT

{
  "Permissions": [
    {
      "Actions": {
        "IssueCertificate",
        "GetCertificate",
        "ListPermissions"
      },
      "CertificateAuthorityArn": "arn:aws:acm:us-
east-1:111122223333:certificate/01234567-89ab-cdef-0123-0123456789ab",
      "CreatedAt": 1.516130652887E9,
      "Principal": "acm.amazonaws.com",
      "SourceAccount": "012345678901"
    },
    {
      "Actions": {
        "LIST_PERMISSIONS"
      },
      "CertificateAuthorityArn": "arn:aws:acm:us-
east-1:111122223333:certificate/12345678-1234-1234-1234-123456789012",
      "CreatedAt": 1.517830652887E9,
```

```
      "Principal": "acm.amazonaws.com",
      "SourceAccount": "012345678901"
    }
  ]
}
```

See Also

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

- Amazon Command Line Interface
- Amazon SDK for .NET
- Amazon SDK for C++
- Amazon SDK for Go v2
- Amazon SDK for Java V2
- Amazon SDK for JavaScript V3
- Amazon SDK for Kotlin
- Amazon SDK for PHP V3
- Amazon SDK for Python
- Amazon SDK for Ruby V3

ListTags

Lists the tags, if any, that are associated with your private CA or one that has been shared with you. 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 action to add one or more tags to your CA. Call the UntagCertificateAuthority action 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.

The request accepts the following data in JSON format.

CertificateAuthorityArn

The Amazon Resource Name (ARN) that was returned when you called the CreateCertificateAuthority action. 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+=/,.@-]+:acm-pca:[\w+=/,.@-]*:[0-9]*:[\w+=,.@-]+(/[\w+=,.@-]+)*`

Required: Yes

MaxResults

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

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 43739.

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

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 43739.

Tags

The tags associated with your private CA.

Type: Array of Tag 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.

InvalidArnException

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

HTTP Status Code: 400

InvalidStateException

The state of the private CA does not allow this action to occur.

HTTP Status Code: 400

RequestFailedException

The request has failed for an unspecified reason.

HTTP Status Code: 400

ResourceNotFoundException

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

HTTP Status Code: 400

Examples

Example

This example illustrates one usage of ListTags.

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

This example illustrates one usage of ListTags.

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 Amazon SDKs, see the following:

- Amazon Command Line Interface
- Amazon SDK for .NET
- Amazon SDK for C++
- Amazon SDK for Go v2
- Amazon SDK for Java V2
- Amazon SDK for JavaScript V3
- Amazon SDK for Kotlin
- Amazon SDK for PHP V3
- Amazon SDK for Python
- Amazon SDK for Ruby V3

PutPolicy

Attaches a resource-based policy to a private CA.

A policy can also be applied by sharing a private CA through Amazon Resource Access Manager (RAM). For more information, see Attach a Policy for Cross-Account Access.

The policy can be displayed with GetPolicy and removed with DeletePolicy.

About Policies

- A policy grants access on a private CA to an Amazon customer account, to Amazon Organizations, or to an Amazon Organizations unit. Policies are under the control of a CA administrator. For more information, see Using a Resource Based Policy with Amazon Private CA.
- A policy permits a user of Amazon Certificate Manager (ACM) to issue ACM certificates signed by a CA in another account.
- For ACM to manage automatic renewal of these certificates, the ACM user must configure a Service Linked Role (SLR). The SLR allows the ACM service to assume the identity of the user, subject to confirmation against the Amazon Private CA policy. For more information, see Using a Service Linked Role with ACM.
- Updates made in Amazon Resource Manager (RAM) are reflected in policies. For more information, see Attach a Policy for Cross-Account Access.

Request Syntax

```
{
   "Policy": "string",
   "ResourceArn": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

Policy

The path and file name of a JSON-formatted IAM policy to attach to the specified private CA resource. If this policy does not contain all required statements or if it includes any statement that is not allowed, the `PutPolicy` action returns an `InvalidPolicyException`. For information about IAM policy and statement structure, see Overview of JSON Policies.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 81920.

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

Required: Yes

ResourceArn

The Amazon Resource Number (ARN) of the private CA to associate with the policy. The ARN of the CA can be found by calling the ListCertificateAuthorities action.

Type: String

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

Pattern: `arn:[\w+=/,.@-]+:acm-pca:[\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.

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

InvalidPolicyException

The resource policy is invalid or is missing a required statement. For general information about IAM policy and statement structure, see Overview of JSON Policies.

HTTP Status Code: 400

InvalidStateException

The state of the private CA does not allow this action to occur.

HTTP Status Code: 400

LockoutPreventedException

The current action was prevented because it would lock the caller out from performing subsequent actions. Verify that the specified parameters would not result in the caller being denied access to the resource.

HTTP Status Code: 400

RequestFailedException

The request has failed for an unspecified reason.

HTTP Status Code: 400

ResourceNotFoundException

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

HTTP Status Code: 400

Examples

Example Policy

The following JSON code grants permissions to allow the designated principal to issue certificates and perform read-only actions using a private CA.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"1",
         "Effect":"Allow",
         "Principal":{
            "AWS":"012345678901"
         },
         "Action":[
            "acm-pca:DescribeCertificateAuthority",
            "acm-pca:GetCertificate",
            "acm-pca:GetCertificateAuthorityCertificate",
            "acm-pca:ListPermissions",
            "acm-pca:ListTags"
         ],
         "Resource":"arn:aws:acm-pca:us-east-1:098765432109:certificate-
authority/01234567-89ab-cdef-0123-456789abcdef"
      },
      {
         "Sid":"2",
         "Effect":"Allow",
         "Principal":{
            "AWS":"012345678901"
         },
         "Action":[
            "acm-pca:IssueCertificate"
         ],
         "Resource":"arn:aws:acm-pca:us-east-1:098765432109:certificate-
authority/01234567-89ab-cdef-0123-456789abcdef",
         "Condition":{
            "StringEquals":{
               "acm-pca:TemplateArn":"arn:aws:acm-pca:::template/EndEntityCertificate/
V1"
            }
         }
      }
   ]
}
```

See Also

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

- Amazon Command Line Interface
- Amazon SDK for .NET
- Amazon SDK for C++
- Amazon SDK for Go v2
- Amazon SDK for Java V2
- Amazon SDK for JavaScript V3
- Amazon SDK for Kotlin
- Amazon SDK for PHP V3
- Amazon SDK for Python
- Amazon SDK for Ruby V3

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 action. 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 or ListCertificateAuthorities actions. The status of a restored CA is set to its pre-deletion status when the **RestoreCertificateAuthority** action returns. To change its status to ACTIVE, call the UpdateCertificateAuthority action. If the private CA was in the PENDING_CERTIFICATE state at deletion, you must use the ImportCertificateAuthorityCertificate action 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.

The request accepts the following data in JSON format.

CertificateAuthorityArn

The Amazon Resource Name (ARN) that was returned when you called the CreateCertificateAuthority action. 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+=/,.@-]+:acm-pca:[\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.

InvalidArnException

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

HTTP Status Code: 400

InvalidStateException

The state of the private CA does not allow this action to occur.

HTTP Status Code: 400

ResourceNotFoundException

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

HTTP Status Code: 400

Examples

Example

This example illustrates one usage of RestoreCertificateAuthority.

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

This example illustrates one usage of RestoreCertificateAuthority.

Sample Response

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

See Also

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

- Amazon Command Line Interface
- Amazon SDK for .NET
- Amazon SDK for C++
- Amazon SDK for Go v2
- Amazon SDK for Java V2
- Amazon SDK for JavaScript V3
- Amazon SDK for Kotlin
- Amazon SDK for PHP V3
- Amazon SDK for Python
- Amazon SDK for Ruby V3

RevokeCertificate

Revokes a certificate that was issued inside Amazon Private CA. 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. Amazon Private CA writes the CRL to an S3 bucket that you specify. A CRL is typically updated approximately 30 minutes after a certificate is revoked. If for any reason the CRL update fails, Amazon Private CA attempts makes further attempts every 15 minutes. With Amazon CloudWatch, you can create alarms for the metrics `CRLGenerated` and `MisconfiguredCRLBucket`. For more information, see Supported CloudWatch Metrics.

> **Note**
>
> Both Amazon Private CA and the IAM principal must have permission to write to the S3 bucket that you specify. If the IAM principal making the call does not have permission to write to the bucket, then an exception is thrown. For more information, see Access policies for CRLs in Amazon S3.

Amazon Private CA also writes revocation information to the audit report. For more information, see CreateCertificateAuthorityAuditReport.

> **Note**
>
> You cannot revoke a root CA self-signed certificate.

Request Syntax

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

Request Parameters

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

The request accepts the following data in JSON format.

CertificateAuthorityArn

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

Required: Yes

CertificateSerial

Serial number of the certificate to be revoked. This must be in hexadecimal format. You can retrieve the serial number by calling GetCertificate with the Amazon Resource Name (ARN) of the certificate you want and the ARN of your private CA. The **GetCertificate** action 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 action in the *Amazon Certificate Manager API Reference*.

Type: String

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

Required: Yes

RevocationReason

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.

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

InvalidRequestException

The request action cannot be performed or is prohibited.

HTTP Status Code: 400

InvalidStateException

The state of the private CA does not allow this action to occur.

HTTP Status Code: 400

LimitExceededException

An Amazon Private CA quota has been exceeded. See the exception message returned to determine the quota that was exceeded.

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, audit report, or policy cannot be found.

HTTP Status Code: 400

Examples

Example

This example illustrates one usage of RevokeCertificate.

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

This example illustrates one usage of RevokeCertificate.

Sample Response

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

See Also

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

- Amazon Command Line Interface
- Amazon SDK for .NET
- Amazon SDK for C++
- Amazon SDK for Go v2
- Amazon SDK for Java V2
- Amazon SDK for JavaScript V3
- Amazon SDK for Kotlin
- Amazon SDK for PHP V3
- Amazon SDK for Python
- Amazon SDK for Ruby V3

TagCertificateAuthority

Adds one or more tags to your private CA. Tags are labels that you can use to identify and organize your Amazon 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 action. Call the ListTags action to see what tags are associated with your CA.

> **Note**
>
> To attach tags to a private CA during the creation procedure, a CA administrator must first associate an inline IAM policy with the `CreateCertificateAuthority` action and explicitly allow tagging. For more information, see Attaching tags to a CA at the time of creation.

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.

The request accepts the following data in JSON format.

CertificateAuthorityArn

The Amazon Resource Name (ARN) that was returned when you called CreateCertificateAuthority. 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+=/,.@-]+:acm-pca:[\w+=/,.@-]*:[0-9]*:[\w+=,.@-]+(/[\w+=,.@-]+)*`

Required: Yes

Tags

List of tags to be associated with the CA.

Type: Array of Tag 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.

InvalidArnException

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

HTTP Status Code: 400

InvalidStateException

The state of the private CA does not allow this action to occur.

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, audit report, or policy 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

This example illustrates one usage of TagCertificateAuthority.

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

This example illustrates one usage of TagCertificateAuthority.

Sample Response

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

See Also

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

- Amazon Command Line Interface
- Amazon SDK for .NET
- Amazon SDK for C++
- Amazon SDK for Go v2
- Amazon SDK for Java V2
- Amazon SDK for JavaScript V3
- Amazon SDK for Kotlin
- Amazon SDK for PHP V3
- Amazon SDK for Python
- Amazon SDK for Ruby V3

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 action, 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. Call the ListTags action 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.

The request accepts the following data in JSON format.

CertificateAuthorityArn

The Amazon Resource Name (ARN) that was returned when you called CreateCertificateAuthority. 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+=/,.@-]+:acm-pca:[\w+=/,.@-]*:[0-9]*:[\w+=,.@-]+(/[\w+=,.@-]+)*`

Required: Yes

Tags

List of tags to be removed from the CA.

Type: Array of Tag 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.

InvalidArnException

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

HTTP Status Code: 400

InvalidStateException

The state of the private CA does not allow this action to occur.

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, audit report, or policy cannot be found.

HTTP Status Code: 400

Examples

Example

This example illustrates one usage of UntagCertificateAuthority.

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

This example illustrates one usage of UntagCertificateAuthority.

Sample Response

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

See Also

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

- Amazon Command Line Interface
- Amazon SDK for .NET
- Amazon SDK for C++
- Amazon SDK for Go v2
- Amazon SDK for Java V2
- Amazon SDK for JavaScript V3
- Amazon SDK for Kotlin
- Amazon SDK for PHP V3
- Amazon SDK for Python
- Amazon SDK for Ruby V3

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.

> **Note**
>
> Both Amazon Private CA and the IAM principal must have permission to write to the S3 bucket that you specify. If the IAM principal making the call does not have permission to write to the bucket, then an exception is thrown. For more information, see Access policies for CRLs in Amazon S3.

Request Syntax

```
{
   "CertificateAuthorityArn": "string",
   "RevocationConfiguration": {
      "CrlConfiguration": {
         "CrlDistributionPointExtensionConfiguration": {
            "OmitExtension": boolean
         },
         "CrlType": "string",
         "CustomCname": "string",
         "CustomPath": "string",
         "Enabled": boolean,
         "ExpirationInDays": number,
         "S3BucketName": "string",
         "S3ObjectAcl": "string"
      },
      "OcspConfiguration": {
         "Enabled": boolean,
         "OcspCustomCname": "string"
      }
   },
   "Status": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

CertificateAuthorityArn

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

Required: Yes

RevocationConfiguration

Contains information to enable support for Online Certificate Status Protocol (OCSP), certificate revocation list (CRL), both protocols, or neither. If you don't supply this parameter, existing capibilites remain unchanged. For more information, see the OcspConfiguration and CrlConfiguration types.

The following requirements apply to revocation configurations.

- A configuration disabling CRLs or OCSP must contain only the `Enabled=False` parameter, and will fail if other parameters such as `CustomCname` or `ExpirationInDays` are included.
- In a CRL configuration, the `S3BucketName` parameter must conform to Amazon S3 bucket naming rules.
- A configuration containing a custom Canonical Name (CNAME) parameter for CRLs or OCSP must conform to RFC2396 restrictions on the use of special characters in a CNAME.
- In a CRL or OCSP configuration, the value of a CNAME parameter must not include a protocol prefix such as "http://" or "https://".

> **Important**
>
> If you update the `S3BucketName` of CrlConfiguration, you can break revocation for existing certificates. In other words, if you call UpdateCertificateAuthority to update the CRL configuration's S3 bucket name, Amazon Private CA only writes CRLs to the new S3 bucket. Certificates issued prior to this point will have the old S3 bucket name in your CRL Distribution Point (CDP) extension, essentially breaking revocation. If you must update the S3 bucket, you'll need to reissue old certificates to keep the revocation working. Alternatively, you can use a CustomCname in your CRL configuration if you might need to change the S3 bucket name in the future.

Type: RevocationConfiguration object

Required: No

Status

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.

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 resource policy is invalid or is missing a required statement. For general information about IAM policy and statement structure, see Overview of JSON Policies.

HTTP Status Code: 400

InvalidStateException

The state of the private CA does not allow this action to occur.

HTTP Status Code: 400

ResourceNotFoundException

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

HTTP Status Code: 400

Examples

Example

This example illustrates one usage of UpdateCertificateAuthority.

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

This example illustrates one usage of UpdateCertificateAuthority.

Sample Response

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

See Also

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

- Amazon Command Line Interface
- Amazon SDK for .NET
- Amazon SDK for C++
- Amazon SDK for Go v2
- Amazon SDK for Java V2
- Amazon SDK for JavaScript V3

- Amazon SDK for Kotlin
- Amazon SDK for PHP V3
- Amazon SDK for Python
- Amazon SDK for Ruby V3

Data Types

The Amazon 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:

- AccessDescription
- AccessMethod
- ApiPassthrough
- ASN1Subject
- CertificateAuthority
- CertificateAuthorityConfiguration
- CrlConfiguration
- CrlDistributionPointExtensionConfiguration
- CsrExtensions
- CustomAttribute
- CustomExtension
- EdiPartyName
- ExtendedKeyUsage
- Extensions
- GeneralName
- KeyUsage
- OcspConfiguration
- OtherName
- Permission
- PolicyInformation

- PolicyQualifierInfo
- Qualifier
- RevocationConfiguration
- Tag
- Validity

AccessDescription

Provides access information used by the `authorityInfoAccess` and `subjectInfoAccess` extensions described in RFC 5280.

Contents

AccessLocation

The location of `AccessDescription` information.

Type: GeneralName object

Required: Yes

AccessMethod

The type and format of `AccessDescription` information.

Type: AccessMethod object

Required: Yes

See Also

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

- Amazon SDK for C++
- Amazon SDK for Java V2
- Amazon SDK for Ruby V3

AccessMethod

Describes the type and format of extension access. Only one of `CustomObjectIdentifier` or `AccessMethodType` may be provided. Providing both results in `InvalidArgsException`.

Contents

AccessMethodType

Specifies the `AccessMethod`.

Type: String

Valid Values: `CA_REPOSITORY | RESOURCE_PKI_MANIFEST | RESOURCE_PKI_NOTIFY`

Required: No

CustomObjectIdentifier

An object identifier (OID) specifying the `AccessMethod`. The OID must satisfy the regular expression shown below. For more information, see NIST's definition of Object Identifier (OID).

Type: String

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

Pattern: `([0-2])\.([0-9]|([0-3][0-9]))((\.([0-9]+)){0,126})`

Required: No

See Also

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

- Amazon SDK for C++
- Amazon SDK for Java V2
- Amazon SDK for Ruby V3

ApiPassthrough

Contains X.509 certificate information to be placed in an issued certificate. An `APIPassthrough` or `APICSRPassthrough` template variant must be selected, or else this parameter is ignored.

If conflicting or duplicate certificate information is supplied from other sources, Amazon Private CA applies order of operation rules to determine what information is used.

Contents

Extensions

Specifies X.509 extension information for a certificate.

Type: Extensions object

Required: No

Subject

Contains information about the certificate subject. 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.

Type: ASN1Subject object

Required: No

See Also

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

- Amazon SDK for C++
- Amazon SDK for Java V2
- Amazon SDK for Ruby V3

ASN1Subject

Contains information about the certificate subject. 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.

Contents

CommonName

For CA and end-entity certificates in a private PKI, the common name (CN) can be any string within the length limit.

Note: In publicly trusted certificates, the common name must be a 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

Length Constraints: Fixed length of 2.

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

Required: No

CustomAttributes

Contains a sequence of one or more X.500 relative distinguished names (RDNs), each of which consists of an object identifier (OID) and a value. For more information, see NIST's definition of Object Identifier (OID).

> **Note**
>
> Custom attributes cannot be used in combination with standard attributes.

Type: Array of CustomAttribute objects

Array Members: Minimum number of 1 item. Maximum number of 150 items.

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.

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

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 Amazon SDKs, see the following:

- Amazon SDK for C++
- Amazon SDK for Java V2
- Amazon SDK for Ruby V3

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 action to create your private CA. You must then call the GetCertificateAuthorityCertificate action to retrieve a private CA certificate signing request (CSR). Sign the CSR with your Amazon Private CA-hosted or on-premises root or subordinate CA certificate. Call the ImportCertificateAuthorityCertificate action to import the signed certificate into Amazon 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+=/,.@-]+:acm-pca:[\w+=/,.@-]*:[0-9]*:[\w+=,.@-]+(/[\w+=,.@-]+)*`

Required: No

CertificateAuthorityConfiguration

Your private CA configuration.

Type: CertificateAuthorityConfiguration 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

KeyStorageSecurityStandard

Defines a cryptographic key management compliance standard for handling and protecting CA keys.

Default: FIPS_140_2_LEVEL_3_OR_HIGHER

> **Note**
>
> Starting January 26, 2023, Amazon Private CA protects all CA private keys in non-China regions using hardware security modules (HSMs) that comply with FIPS PUB 140-2 Level 3.
> For information about security standard support in different Amazon Regions, see Storage and security compliance of Amazon Private CA private keys.

Type: String

Valid Values: `FIPS_140_2_LEVEL_2_OR_HIGHER | FIPS_140_2_LEVEL_3_OR_HIGHER | CCPC_LEVEL_1_OR_HIGHER`

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

OwnerAccount

The Amazon account ID that owns the certificate authority.

Type: String

Length Constraints: Fixed length of 12.

Pattern: `[0-9]+`

Required: No

RestorableUntil

The period during which a deleted CA can be restored. For more information, see the `PermanentDeletionTimeInDays` parameter of the DeleteCertificateAuthorityRequest action.

Type: Timestamp

Required: No

RevocationConfiguration

Information about the Online Certificate Status Protocol (OCSP) configuration or certificate revocation list (CRL) created and maintained by your private CA.

Type: RevocationConfiguration 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: `ROOT | SUBORDINATE`

Required: No

UsageMode

Specifies whether the CA issues general-purpose certificates that typically require a revocation mechanism, or short-lived certificates that may optionally omit revocation because they expire quickly. Short-lived certificate validity is limited to seven days.

The default value is GENERAL_PURPOSE.

Type: String

Valid Values: `GENERAL_PURPOSE | SHORT_LIVED_CERTIFICATE`

Required: No

See Also

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

- Amazon SDK for C++

- Amazon SDK for Java V2
- Amazon SDK for Ruby V3

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. It also includes the signature algorithm that it uses when issuing certificates, and its X.500 distinguished name. You must specify this information when you call the CreateCertificateAuthority action.

Contents

KeyAlgorithm

Type of the public key algorithm and size, in bits, of the key pair that your CA creates when it issues a certificate. When you create a subordinate CA, you must use a key algorithm supported by the parent CA.

Type: String

Valid Values: `RSA_2048 | RSA_3072 | RSA_4096 | EC_prime256v1 | EC_secp384r1 | EC_secp521r1 | SM2`

Required: Yes

SigningAlgorithm

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

This parameter should not be confused with the `SigningAlgorithm` parameter used to sign certificates when they are issued.

Type: String

Valid Values: `SHA256WITHECDSA | SHA384WITHECDSA | SHA512WITHECDSA | SHA256WITHRSA | SHA384WITHRSA | SHA512WITHRSA | SM3WITHSM2`

Required: Yes

Subject

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

Type: ASN1Subject object

Required: Yes

CsrExtensions

Specifies information to be added to the extension section of the certificate signing request (CSR).

Type: CsrExtensions object

Required: No

See Also

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

- Amazon SDK for C++
- Amazon SDK for Java V2
- Amazon SDK for Ruby V3

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 by default copies the CNAME or the S3 bucket name to the **CRL Distribution Points** extension of each certificate it issues. If you want to configure this default behavior to be something different, you can set the **CrlDistributionPointExtensionConfiguration** parameter. Your S3 bucket policy must give write permission to Amazon Private CA.

Amazon Private CA assets that are stored in Amazon S3 can be protected with encryption. For more information, see Encrypting Your CRLs.

Your private CA uses the value in the **ExpirationInDays** parameter to calculate the **nextUpdate** field in the CRL. The CRL is refreshed prior to a certificate's expiration date or when a certificate is revoked. When a certificate is revoked, it appears in the CRL until the certificate expires, and then in one additional CRL after expiration, and it always appears in the audit report.

A CRL is typically updated approximately 30 minutes after a certificate is revoked. If for any reason a CRL update fails, Amazon Private CA makes further attempts every 15 minutes.

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 Amazon Private CA are DER-encoded. You can use the following OpenSSL command to list a CRL.

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

For more information, see Planning a certificate revocation list (CRL) in the *Amazon Private Certificate Authority User Guide*

Contents

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 action or for an existing CA when you call the UpdateCertificateAuthority action.

Type: Boolean

Required: Yes

CrlDistributionPointExtensionConfiguration

Configures the behavior of the CRL Distribution Point extension for certificates issued by your certificate authority. If this field is not provided, then the CRl Distribution Point Extension will be present and contain the default CRL URL.

Type: CrlDistributionPointExtensionConfiguration object

Required: No

CrlType

Specifies whether to create a complete or partitioned CRL. This setting determines the maximum number of certificates that the certificate authority can issue and revoke. For more information, see Amazon Private CA quotas.

- `COMPLETE` - The default setting. Amazon Private CA maintains a single CRL file for all unexpired certificates issued by a CA that have been revoked for any reason. Each certificate that Amazon Private CA issues is bound to a specific CRL through its CRL distribution point (CDP) extension, defined in RFC 5280.
- `PARTITIONED` - Compared to complete CRLs, partitioned CRLs dramatically increase the number of certificates your private CA can issue.

> **Important**
>
> When using partitioned CRLs, you must validate that the CRL's associated issuing distribution point (IDP) URI matches the certificate's CDP URI to ensure the right CRL has been fetched. Amazon Private CA marks the IDP extension as critical, which your client must be able to process.

Type: String

Valid Values: `COMPLETE | PARTITIONED`

Required: No

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.

> **Note**
>
> The content of a Canonical Name (CNAME) record must conform to RFC2396 restrictions on the use of special characters in URIs. Additionally, the value of the CNAME must not include a protocol prefix such as "http://" or "https://".

Type: String

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

Pattern: `[-a-zA-Z0-9;/?:@&=+$,%_.!~*()']*`

Required: No

CustomPath

Designates a custom file path in S3 for CRL(s). For example, `http://<CustomName>/<CustomPath>/<CrlPartition_GUID>.crl`.

Type: String

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

Pattern: `[-a-zA-Z0-9;?:@&=+$,%_.!~*()']+(/[-a-zA-Z0-9;?:@&=+$,%_.!~*()']+)*`

Required: No

ExpirationInDays

Validity period of the CRL in days.

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 operation. You must specify a bucket policy that allows Amazon Private CA to write the CRL to your bucket.

> **Note**
>
> The `S3BucketName` parameter must conform to the S3 bucket naming rules.

Type: String

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

Pattern: `[-a-zA-Z0-9._/]+`

Required: No

S3ObjectAcl

Determines whether the CRL will be publicly readable or privately held in the CRL Amazon S3 bucket. If you choose PUBLIC_READ, the CRL will be accessible over the public internet. If you choose BUCKET_OWNER_FULL_CONTROL, only the owner of the CRL S3 bucket can access the CRL, and your PKI clients may need an alternative method of access.

If no value is specified, the default is `PUBLIC_READ`.

Note: This default can cause CA creation to fail in some circumstances. If you have have enabled the Block Public Access (BPA) feature in your S3 account, then you must specify the value of this parameter as `BUCKET_OWNER_FULL_CONTROL`, and not doing so results in an error. If you have disabled BPA in S3, then you can specify either `BUCKET_OWNER_FULL_CONTROL` or `PUBLIC_READ` as the value.

For more information, see Blocking public access to the S3 bucket.

Type: String

Valid Values: `PUBLIC_READ | BUCKET_OWNER_FULL_CONTROL`

Required: No

See Also

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

- Amazon SDK for C++
- Amazon SDK for Java V2
- Amazon SDK for Ruby V3

CrlDistributionPointExtensionConfiguration

Contains configuration information for the default behavior of the CRL Distribution Point (CDP) extension in certificates issued by your CA. This extension contains a link to download the CRL, so you can check whether a certificate has been revoked. To choose whether you want this extension omitted or not in certificates issued by your CA, you can set the **OmitExtension** parameter.

Contents

OmitExtension

Configures whether the CRL Distribution Point extension should be populated with the default URL to the CRL. If set to `true`, then the CDP extension will not be present in any certificates issued by that CA unless otherwise specified through CSR or API passthrough.

> **Note**
>
> Only set this if you have another way to distribute the CRL Distribution Points ffor certificates issued by your CA, such as the Matter Distributed Compliance Ledger This configuration cannot be enabled with a custom CNAME set.

Type: Boolean

Required: Yes

See Also

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

- Amazon SDK for C++
- Amazon SDK for Java V2
- Amazon SDK for Ruby V3

CsrExtensions

Describes the certificate extensions to be added to the certificate signing request (CSR).

Contents

KeyUsage

Indicates the purpose of the certificate and of the key contained in the certificate.

Type: KeyUsage object

Required: No

SubjectInformationAccess

For CA certificates, provides a path to additional information pertaining to the CA, such as revocation and policy. For more information, see Subject Information Access in RFC 5280.

Type: Array of AccessDescription objects

Required: No

See Also

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

- Amazon SDK for C++
- Amazon SDK for Java V2
- Amazon SDK for Ruby V3

CustomAttribute

Defines the X.500 relative distinguished name (RDN).

Contents

ObjectIdentifier

Specifies the object identifier (OID) of the attribute type of the relative distinguished name (RDN).

Type: String

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

Pattern: `([0-2])\.([0-9]|([0-3][0-9]))((\.([0-9]+)){0,126})`

Required: Yes

Value

Specifies the attribute value of relative distinguished name (RDN).

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Required: Yes

See Also

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

- Amazon SDK for C++
- Amazon SDK for Java V2
- Amazon SDK for Ruby V3

CustomExtension

Specifies the X.509 extension information for a certificate.

Extensions present in `CustomExtensions` follow the `ApiPassthrough` template rules.

Contents

ObjectIdentifier

Specifies the object identifier (OID) of the X.509 extension. For more information, see the Global OID reference database.

Type: String

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

Pattern: `([0-2])\.([0-9]|([0-3][0-9]))((\.([0-9]+)){0,126})`

Required: Yes

Value

Specifies the base64-encoded value of the X.509 extension.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 4096.

Pattern: `(?:[A-Za-z0-9+/]{4})*(?:[A-Za-z0-9+/]{2}==|[A-Za-z0-9+/]{3}=)?`

Required: Yes

Critical

Specifies the critical flag of the X.509 extension.

Type: Boolean

Required: No

See Also

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

- Amazon SDK for C++
- Amazon SDK for Java V2
- Amazon SDK for Ruby V3

EdiPartyName

Describes an Electronic Data Interchange (EDI) entity as described in as defined in Subject Alternative Name in RFC 5280.

Contents

PartyName

Specifies the party name.

Type: String

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

Required: Yes

NameAssigner

Specifies the name assigner.

Type: String

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

Required: No

See Also

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

- Amazon SDK for C++
- Amazon SDK for Java V2
- Amazon SDK for Ruby V3

ExtendedKeyUsage

Specifies additional purposes for which the certified public key may be used other than basic purposes indicated in the `KeyUsage` extension.

Contents

ExtendedKeyUsageObjectIdentifier

Specifies a custom `ExtendedKeyUsage` with an object identifier (OID).

Type: String

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

Pattern: `([0-2])\.([0-9]|([0-3][0-9]))((\.([0-9]+)){0,126})`

Required: No

ExtendedKeyUsageType

Specifies a standard `ExtendedKeyUsage` as defined as in RFC 5280.

Type: String

Valid Values: `SERVER_AUTH | CLIENT_AUTH | CODE_SIGNING | EMAIL_PROTECTION | TIME_STAMPING | OCSP_SIGNING | SMART_CARD_LOGIN | DOCUMENT_SIGNING | CERTIFICATE_TRANSPARENCY`

Required: No

See Also

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

- Amazon SDK for C++
- Amazon SDK for Java V2
- Amazon SDK for Ruby V3

Extensions

Contains X.509 extension information for a certificate.

Contents

CertificatePolicies

Contains a sequence of one or more policy information terms, each of which consists of an object identifier (OID) and optional qualifiers. For more information, see NIST's definition of Object Identifier (OID).

In an end-entity certificate, these terms indicate the policy under which the certificate was issued and the purposes for which it may be used. In a CA certificate, these terms limit the set of policies for certification paths that include this certificate.

Type: Array of PolicyInformation objects

Array Members: Minimum number of 1 item. Maximum number of 20 items.

Required: No

CustomExtensions

Contains a sequence of one or more X.509 extensions, each of which consists of an object identifier (OID), a base64-encoded value, and the critical flag. For more information, see the Global OID reference database.

Type: Array of CustomExtension objects

Array Members: Minimum number of 1 item. Maximum number of 150 items.

Required: No

ExtendedKeyUsage

Specifies additional purposes for which the certified public key may be used other than basic purposes indicated in the `KeyUsage` extension.

Type: Array of ExtendedKeyUsage objects

Array Members: Minimum number of 1 item. Maximum number of 20 items.

Required: No

KeyUsage

Defines one or more purposes for which the key contained in the certificate can be used. Default value for each option is false.

Type: KeyUsage object

Required: No

SubjectAlternativeNames

The subject alternative name extension allows identities to be bound to the subject of the certificate. These identities may be included in addition to or in place of the identity in the subject field of the certificate.

Type: Array of GeneralName objects

Array Members: Minimum number of 1 item. Maximum number of 150 items.

Required: No

See Also

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

- Amazon SDK for C++
- Amazon SDK for Java V2
- Amazon SDK for Ruby V3

GeneralName

Describes an ASN.1 X.400 `GeneralName` as defined in RFC 5280. Only one of the following naming options should be provided. Providing more than one option results in an `InvalidArgsException` error.

Contents

DirectoryName

Contains information about the certificate subject. 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.

Type: ASN1Subject object

Required: No

DnsName

Represents `GeneralName` as a DNS name.

Type: String

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

Required: No

EdiPartyName

Represents `GeneralName` as an `EdiPartyName` object.

Type: EdiPartyName object

Required: No

IpAddress

Represents `GeneralName` as an IPv4 or IPv6 address.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 39.

Required: No

OtherName

Represents `GeneralName` using an `OtherName` object.

Type: OtherName object

Required: No

RegisteredId

Represents `GeneralName` as an object identifier (OID).

Type: String

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

Pattern: `([0-2])\.([0-9]|([0-3][0-9]))((\.([0-9]+)){0,126})`

Required: No

Rfc822Name

Represents `GeneralName` as an RFC 822 email address.

Type: String

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

Required: No

UniformResourceIdentifier

Represents `GeneralName` as a URI.

Type: String

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

Required: No

See Also

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

- Amazon SDK for C++
- Amazon SDK for Java V2
- Amazon SDK for Ruby V3

KeyUsage

Defines one or more purposes for which the key contained in the certificate can be used. Default value for each option is false.

Contents

CRLSign

Key can be used to sign CRLs.

Type: Boolean

Required: No

DataEncipherment

Key can be used to decipher data.

Type: Boolean

Required: No

DecipherOnly

Key can be used only to decipher data.

Type: Boolean

Required: No

DigitalSignature

Key can be used for digital signing.

Type: Boolean

Required: No

EncipherOnly

Key can be used only to encipher data.

Type: Boolean

Required: No

KeyAgreement

Key can be used in a key-agreement protocol.

Type: Boolean

Required: No

KeyCertSign

Key can be used to sign certificates.

Type: Boolean

Required: No

KeyEncipherment

Key can be used to encipher data.

Type: Boolean

Required: No

NonRepudiation

Key can be used for non-repudiation.

Type: Boolean

Required: No

See Also

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

- Amazon SDK for C++
- Amazon SDK for Java V2
- Amazon SDK for Ruby V3

OcspConfiguration

Contains information to enable and configure Online Certificate Status Protocol (OCSP) for validating certificate revocation status.

When you revoke a certificate, OCSP responses may take up to 60 minutes to reflect the new status.

Contents

Enabled

Flag enabling use of the Online Certificate Status Protocol (OCSP) for validating certificate revocation status.

Type: Boolean

Required: Yes

OcspCustomCname

By default, Amazon Private CA injects an Amazon domain into certificates being validated by the Online Certificate Status Protocol (OCSP). A customer can alternatively use this object to define a CNAME specifying a customized OCSP domain.

> **Note**
>
> The content of a Canonical Name (CNAME) record must conform to RFC2396 restrictions on the use of special characters in URIs. Additionally, the value of the CNAME must not include a protocol prefix such as "http://" or "https://".

For more information, see Customizing Online Certificate Status Protocol (OCSP) in the *Amazon Private Certificate Authority User Guide*.

Type: String

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

Pattern: `[-a-zA-Z0-9;/?:@&=+$,%_.!~*()']*`

Required: No

See Also

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

- Amazon SDK for C++
- Amazon SDK for Java V2
- Amazon SDK for Ruby V3

OtherName

Defines a custom ASN.1 X.400 `GeneralName` using an object identifier (OID) and value. The OID must satisfy the regular expression shown below. For more information, see NIST's definition of Object Identifier (OID).

Contents

TypeId

Specifies an OID.

Type: String

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

Pattern: `([0-2])\.([0-9]|([0-3][0-9]))((\.([0-9]+)){0,126})`

Required: Yes

Value

Specifies an OID value.

Type: String

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

Required: Yes

See Also

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

- Amazon SDK for C++
- Amazon SDK for Java V2
- Amazon SDK for Ruby V3

Permission

Permissions designate which private CA actions can be performed by an Amazon service or entity. In order for ACM to automatically renew private certificates, you must give the ACM service principal all available permissions (`IssueCertificate`, `GetCertificate`, and `ListPermissions`). Permissions can be assigned with the CreatePermission action, removed with the DeletePermission action, and listed with the ListPermissions action.

Contents

Actions

The private CA actions that can be performed by the designated Amazon service.

Type: Array of strings

Array Members: Minimum number of 1 item. Maximum number of 3 items.

Valid Values: `IssueCertificate | GetCertificate | ListPermissions`

Required: No

CertificateAuthorityArn

The Amazon Resource Number (ARN) of the private CA from which the permission was issued.

Type: String

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

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

Required: No

CreatedAt

The time at which the permission was created.

Type: Timestamp

Required: No

Policy

The name of the policy that is associated with the permission.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 81920.

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

Required: No

Principal

The Amazon service or entity that holds the permission. At this time, the only valid principal is `acm.amazonaws.com`.

Type: String

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

Pattern: `[^*]+`

Required: No

SourceAccount

The ID of the account that assigned the permission.

Type: String

Length Constraints: Fixed length of 12.

Pattern: `[0-9]+`

Required: No

See Also

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

- Amazon SDK for C++

- Amazon SDK for Java V2
- Amazon SDK for Ruby V3

PolicyInformation

Defines the X.509 `CertificatePolicies` extension.

Contents

CertPolicyId

Specifies the object identifier (OID) of the certificate policy under which the certificate was issued. For more information, see NIST's definition of Object Identifier (OID).

Type: String

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

Pattern: `([0-2])\.([0-9]|([0-3][0-9]))((\.([0-9]+)){0,126})`

Required: Yes

PolicyQualifiers

Modifies the given `CertPolicyId` with a qualifier. Amazon Private CA supports the certification practice statement (CPS) qualifier.

Type: Array of PolicyQualifierInfo objects

Array Members: Minimum number of 1 item. Maximum number of 20 items.

Required: No

See Also

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

- Amazon SDK for C++
- Amazon SDK for Java V2
- Amazon SDK for Ruby V3

PolicyQualifierInfo

Modifies the `CertPolicyId` of a `PolicyInformation` object with a qualifier. Amazon Private CA supports the certification practice statement (CPS) qualifier.

Contents

PolicyQualifierId

Identifies the qualifier modifying a `CertPolicyId`.

Type: String

Valid Values: CPS

Required: Yes

Qualifier

Defines the qualifier type. Amazon Private CA supports the use of a URI for a CPS qualifier in this field.

Type: Qualifier object

Required: Yes

See Also

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

- Amazon SDK for C++
- Amazon SDK for Java V2
- Amazon SDK for Ruby V3

Qualifier

Defines a `PolicyInformation` qualifier. Amazon Private CA supports the certification practice statement (CPS) qualifier defined in RFC 5280.

Contents

CpsUri

Contains a pointer to a certification practice statement (CPS) published by the CA.

Type: String

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

Required: Yes

See Also

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

- Amazon SDK for C++
- Amazon SDK for Java V2
- Amazon SDK for Ruby V3

RevocationConfiguration

Certificate revocation information used by the CreateCertificateAuthority and UpdateCertificateAuthority actions. Your private certificate authority (CA) can configure Online Certificate Status Protocol (OCSP) support and/or maintain a certificate revocation list (CRL). OCSP returns validation information about certificates as requested by clients, and a CRL contains an updated list of certificates revoked by your CA. For more information, see RevokeCertificate and Setting up a certificate revocation method in the *Amazon Private Certificate Authority User Guide*.

Contents

CrlConfiguration

Configuration of the certificate revocation list (CRL), if any, maintained by your private CA. A CRL is typically updated approximately 30 minutes after a certificate is revoked. If for any reason a CRL update fails, Amazon Private CA makes further attempts every 15 minutes.

Type: CrlConfiguration object

Required: No

OcspConfiguration

Configuration of Online Certificate Status Protocol (OCSP) support, if any, maintained by your private CA. When you revoke a certificate, OCSP responses may take up to 60 minutes to reflect the new status.

Type: OcspConfiguration object

Required: No

See Also

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

- Amazon SDK for C++
- Amazon SDK for Java V2
- Amazon SDK for Ruby V3

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 action. To remove a tag, call the UntagCertificateAuthority action.

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 Amazon SDKs, see the following:

- Amazon SDK for C++
- Amazon SDK for Java V2
- Amazon SDK for Ruby V3

Validity

Validity specifies the period of time during which a certificate is valid. Validity can be expressed as an explicit date and time when the validity of a certificate starts or expires, or as a span of time after issuance, stated in days, months, or years. For more information, see Validity in RFC 5280.

Amazon Private CA API consumes the `Validity` data type differently in two distinct parameters of the `IssueCertificate` action. The required parameter `IssueCertificate:Validity` specifies the end of a certificate's validity period. The optional parameter `IssueCertificate:ValidityNotBefore` specifies a customized starting time for the validity period.

Contents

Type

Determines how *Amazon Private CA* interprets the `Value` parameter, an integer. Supported validity types include those listed below. Type definitions with values include a sample input value and the resulting output.

`END_DATE`: The specific date and time when the certificate will expire, expressed using UTCTime (YYMMDDHHMMSS) or GeneralizedTime (YYYYMMDDHHMMSS) format. When UTCTime is used, if the year field (YY) is greater than or equal to 50, the year is interpreted as 19YY. If the year field is less than 50, the year is interpreted as 20YY.

- Sample input value: 491231235959 (UTCTime format)
- Output expiration date/time: 12/31/2049 23:59:59

`ABSOLUTE`: The specific date and time when the validity of a certificate will start or expire, expressed in seconds since the Unix Epoch.

- Sample input value: 2524608000
- Output expiration date/time: 01/01/2050 00:00:00

`DAYS`, `MONTHS`, `YEARS`: The relative time from the moment of issuance until the certificate will expire, expressed in days, months, or years.

Example if `DAYS`, issued on 10/12/2020 at 12:34:54 UTC:

- Sample input value: 90
- Output expiration date: 01/10/2020 12:34:54 UTC

The minimum validity duration for a certificate using relative time (DAYS) is one day. The minimum validity for a certificate using absolute time (ABSOLUTE or END_DATE) is one second.

Type: String

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

Required: Yes

Value

A long integer interpreted according to the value of Type, below.

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 Amazon SDKs, see the following:

- Amazon SDK for C++
- Amazon SDK for Java V2
- Amazon SDK for Ruby V3

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 Signing Amazon API requests in the *IAM User Guide*.

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 Create a signed Amazon API request in the *IAM User Guide*.

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 Elements of an Amazon API request signature in the *IAM User Guide*.

Type: string

Required: Conditional

X-Amz-Security-Token

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

Condition: If you're using temporary security credentials from Amazon STS, 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 Create a signed Amazon API request in the *IAM User Guide*.

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 Amazon 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 Amazon 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 Amazon access key ID provided does not exist in our records.

HTTP Status Code: 403

NotAuthorized

You do not have permission to perform this action.

HTTP Status Code: 400

OptInRequired

The Amazon 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 Amazon service.

HTTP Status Code: 400