ACME ARI Extension

draft-aaron-acme-ari-01

Aaron Gable, ISRG

Since IETF 112

- Updated URL construction
- Added “renewal complete” mechanism
- Various small edits

These will be published as version -02 shortly after IETF 113

Constructing an ARI URL

- Base path is contained in directory

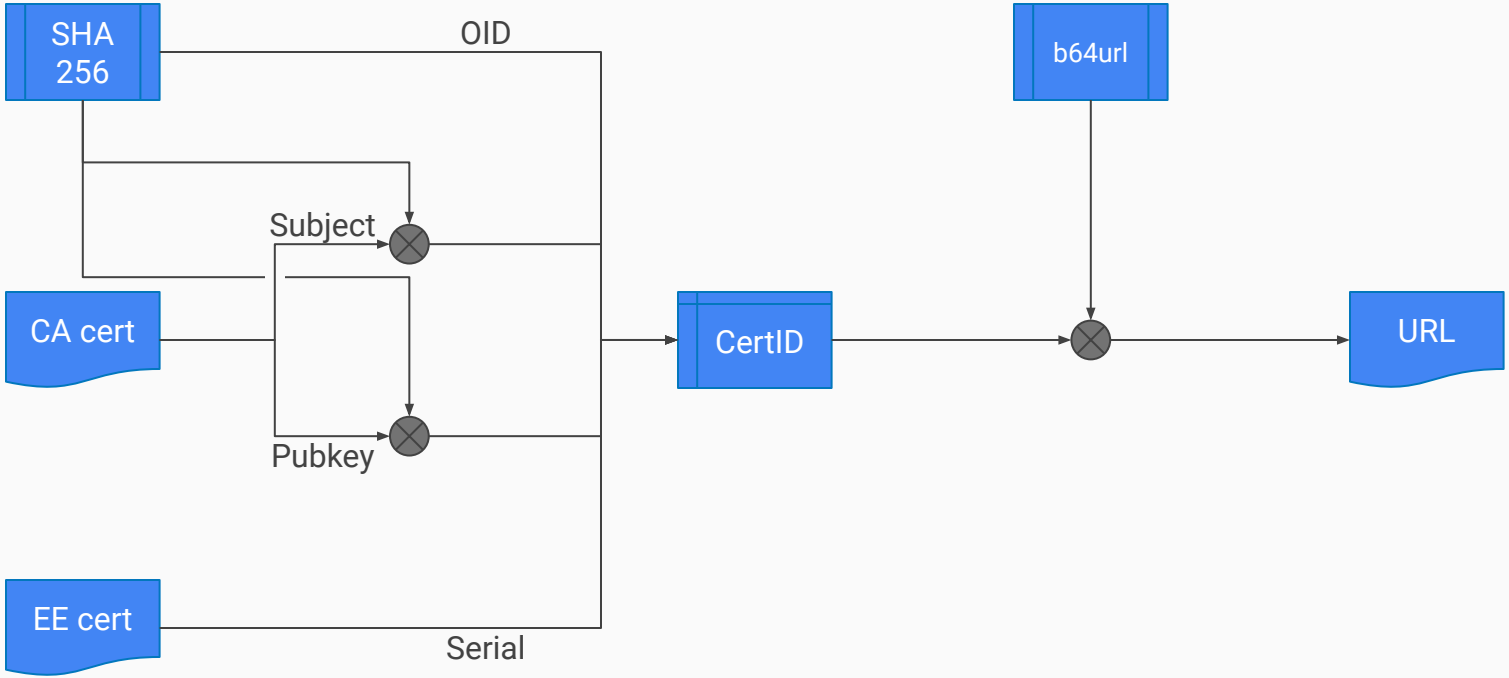
```
GET https://example.com/directory

HTTP/1.1 200 OK
Content-Type: application/json

{
  "newNonce":    "https://example.com/new-nonce",
  "newAccount":  "https://example.com/new-account",
  "newOrder":    "https://example.com/new-order",
  "newAuthz":    "https://example.com/new-authz",
  "revokeCert":  "https://example.com/revoke-cert",
  "keyChange":   "https://example.com/key-change",
  "renewalInfo": "https://example.com/renewal-info",
  "meta": {
    "website": "https://www.example.com/",
    "caaIdentities": ["example.com"],
    "externalAccountRequired": false
  }
}
```

Constructing an ARI URL

- Base path is contained in directory
- Remainder is the base64url-encoding of the DER-encoding of the CertID ASN.1 structure from RFC6960 (OCSP) with trailing “=” stripped

```
CertID          ::=     SEQUENCE {
    hashAlgorithm       AlgorithmIdentifier,
    issuerNameHash      OCTET STRING,
    issuerKeyHash       OCTET STRING,
    serialNumber        CertificateSerialNumber }
```

Constructing an ARI URL



Constructing an ARI URL

- Base path is contained in directory
- Remainder is the base64url-encoding of the DER-encoding of the CertID ASN.1 structure from RFC6960 (OCSP) with trailing “=” stripped

```
GET https://example.com/acme/renewal-info/
      MFswCwYJYIZIAWUDBAIBBCCeWLRusNLb--vmWOkx
      m34qDjTMWkc3utIhOMoMwKDqbgQg2iiKWySZrD-6
      c88HMZ6vhIHZPamChLlzGHeZ7pTS8jYCCD6jRWhl
      RB8c

HTTP/1.1 200 OK
Content-Type: application/json
Retry-After: "21600"

{
  "suggestedWindow": {
    "start": "2021-01-03T00:00:00Z",
    "end": "2021-01-07T00:00:00Z"
  }
}
```

Updating Renewal Information

- POST-as-GET to the renewalInfo base URL
- Payload contains the same base64url-encoded CertID
- Also contains metadata about the replacement

```
POST /acme/renewal-info HTTP/1.1
Host: example.com
Content-Type: application/jose+json

{
  "protected": base64url({
    "alg": "ES256",
    "kid": "...",
    "nonce": "...",
    "url": "https://example.com/acme/renewal-info"
  }),
  "payload": base64url({
    "certID": "MFswCwYJ...RWhlRB8c",
    "replaced": true
  }),
  "signature": "nuSD...awps"
}

HTTP/1.1 200 OK
```

Updating Renewal Information

- Request MUST be signed by the original Subscriber's key
- Server might use this info to:
  - Revoke replaced certs during a mass-revocation
  - Avoid sending renewal reminder notifications for replaced certs
  - Return errors for subsequent renewalInfo requests for replaced certs

```
POST /acme/renewal-info HTTP/1.1
Host: example.com
Content-Type: application/jose+json

{
  "protected": base64url({
    "alg": "ES256",
    "kid": "...",
    "nonce": "...",
    "url": "https://example.com/acme/renewal-info"
  }),
  "payload": base64url({
    "certID": "MFswCwYJ...RWhlRB8c",
    "replaced": true
  }),
  "signature": "nuSD...awps"
}

HTTP/1.1 200 OK
```

Open Questions

- Additional metadata in renewal info update?
  - e.g. Serial of replacement cert?
- ExplanationURI in renewalInfo response?
  - Might provide value for certificate status monitoring services