Secure access in delegated streaming

YANA1123 – Nov 5 2023

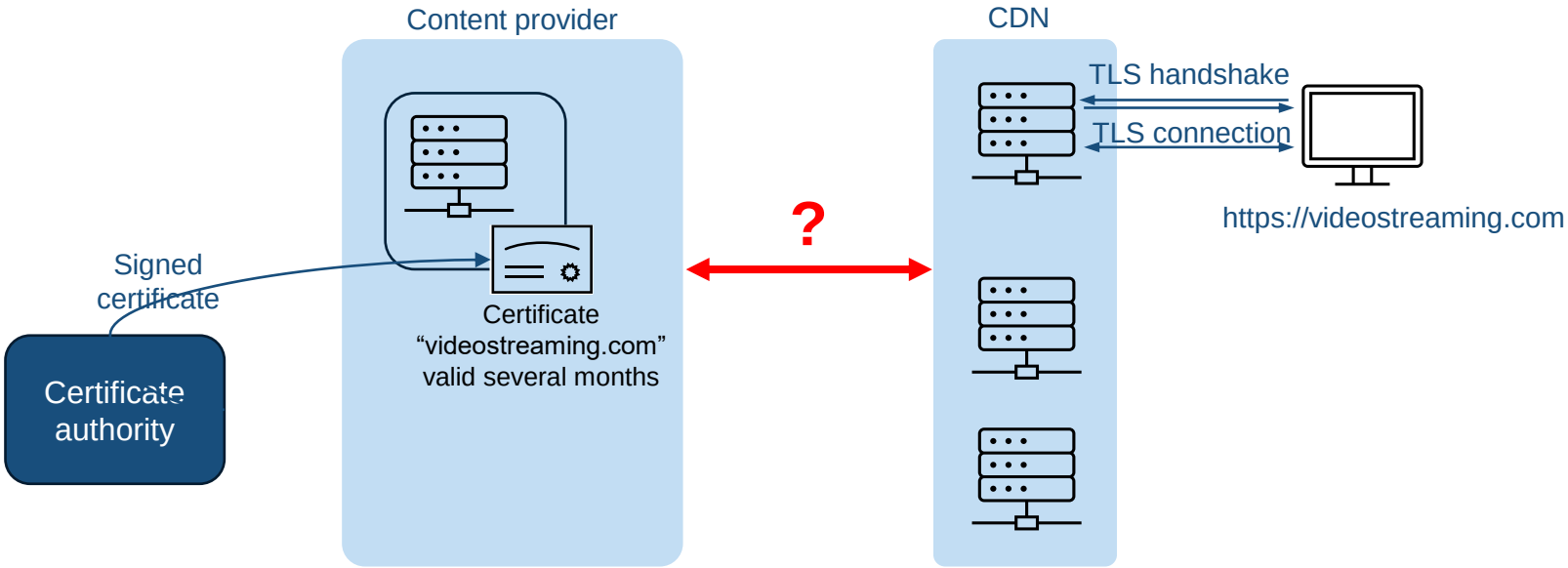
christoph.neumann@broadpeak.tv
guillaume.bichot@broadpeak.tv

broadpeak
This is streaming at its peak

Secure access in delegated streaming

Objective

- **Delegation of secure TLS termination using the FQDN of the content provider**



Example

- **The content provider owning the FQDN videostreaming.com delegates video streaming to some CDN**
- **The TLS connection is between the terminal and a CDN cache node**

Two proposals

ACME-based

- Use “full-fledged” certificates in CDN
- CA issues these certificates for the CDN upon enrollment of CDN by content provider
- Requires extension of the Automatic Certificate Management Environment (ACME) protocol in the context of CDNI

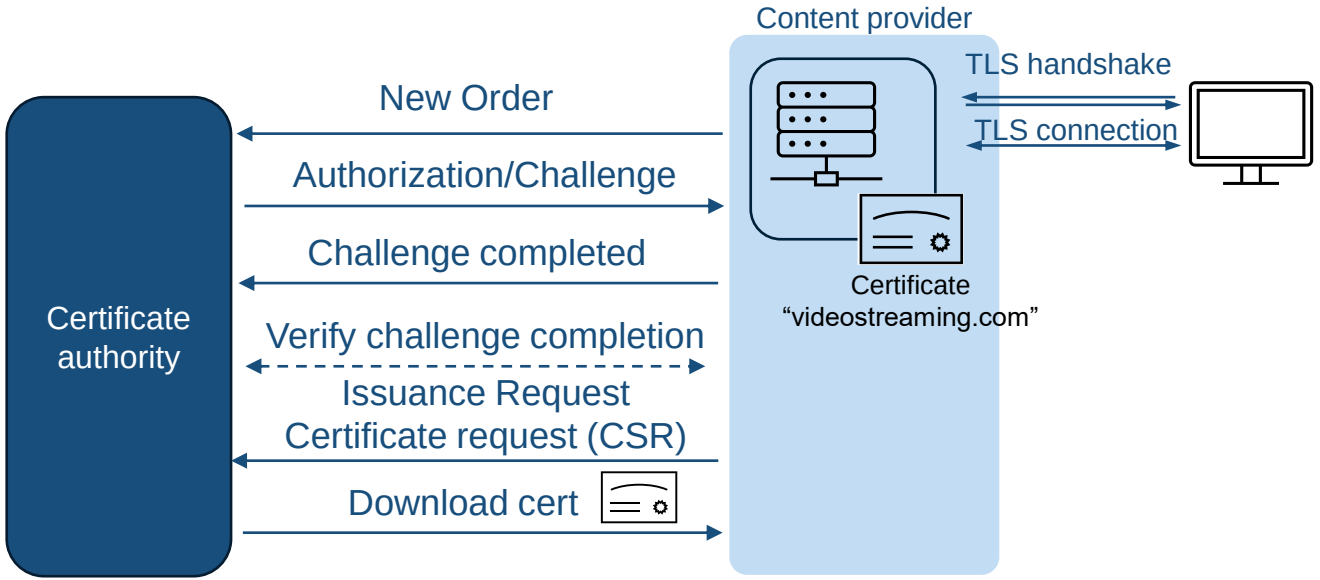
Delegated credentials

- Rely on delegated credential (DC) in CDN. DC is a new lightweight cryptographic structure
- Delegated credentials can be issued by content provider without involving CA
- Propose CDNI extension to request and support transport DCs

01

ACME-based

ACME



Principles

- **To issue a certificate signing requests (CSR) for a given FQDN to a certification authority**
- **The certification authority submits a challenge to the requester checking that he owns the FQDN**
- **Upon successful challenge verification the CA issues the certificate**
- **The requester can download it on a specified URL**

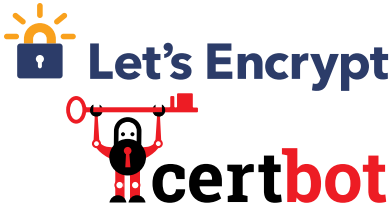
ACME

Most common ACME Challenge types

- HTTP challenge
  - CA provides a token used to build a key authorization to be placed on the requester's server responding to the FQDN http://<FQDN>/.well-known/acme-challenge/<TOKEN>
- DNS challenge
  - CA provides a token used to build a key authorization to be placed on the requester's DNS server (TXT record) under the FQDN

Adoption

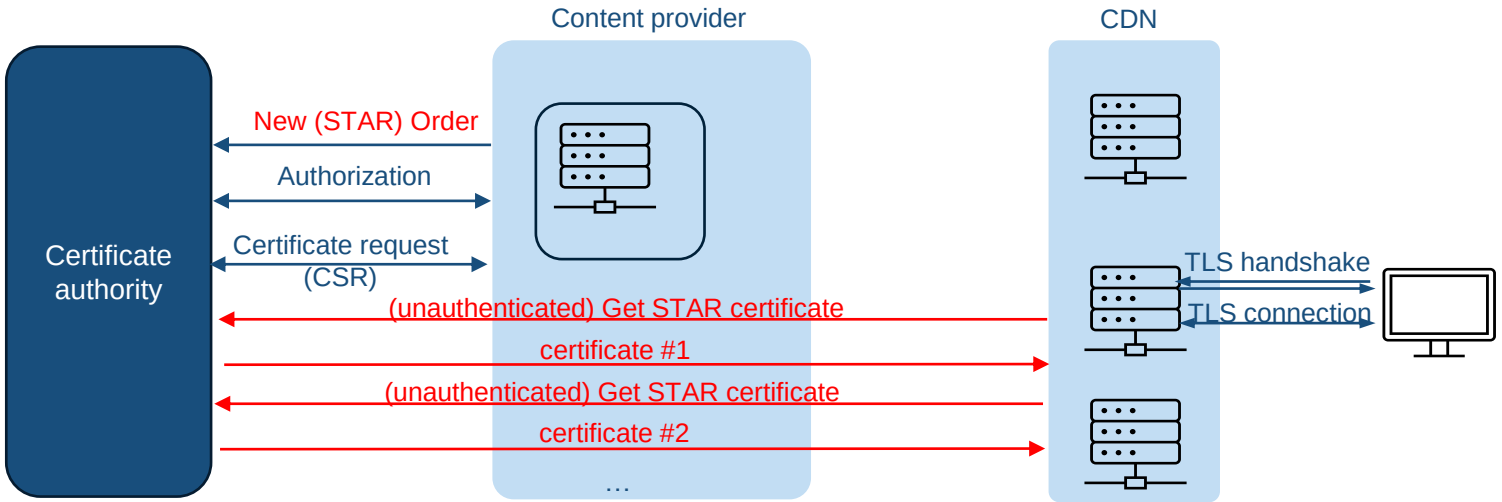
- Wide support by certification authorities: LetsEncrypt, Digicert, …
- Tools available: CertBot
- Standardized by IETF: RFC8555



ACME – STAR extension

STAR: Short-Term, Automatically Renewed Certificates (RFC8739)

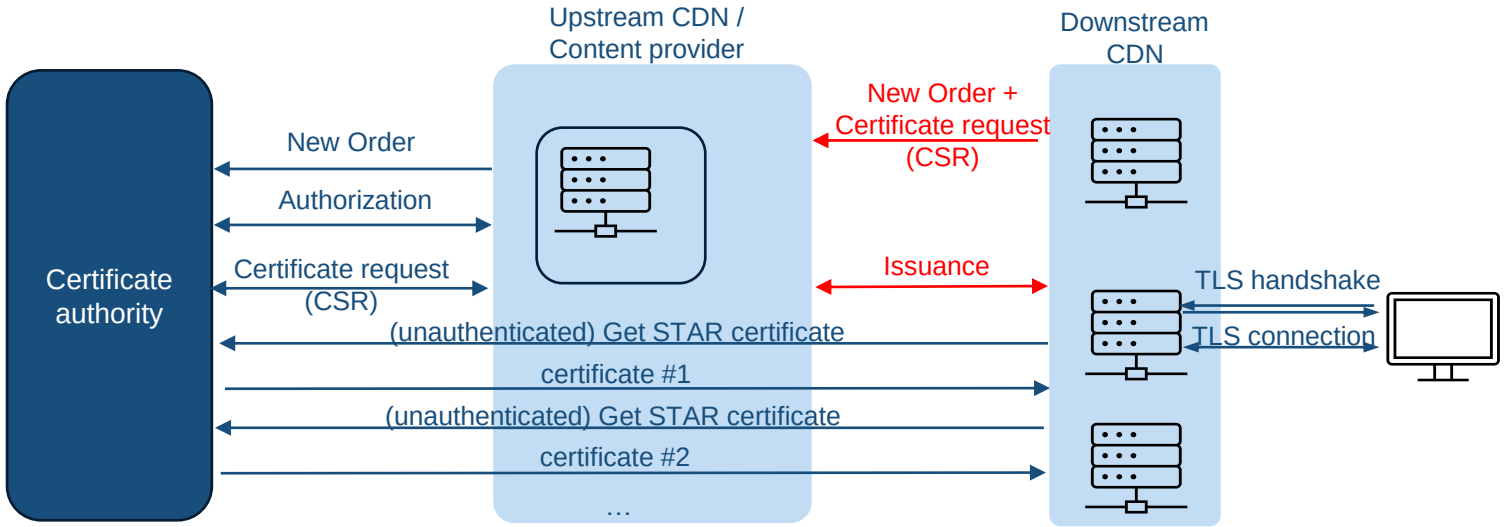
- **Short-lived certificates with few hours/days of validity**
- **All certificates of one certificate order rely on the same private key**
- **CA instructed to issue series of STAR certificates periodically according to validity period**
- **Each STAR certificate can be publicly retrieved**



Profile for Generating Delegated Certificates

STAR Profile for Generating Delegated Certificates (RFC9115)

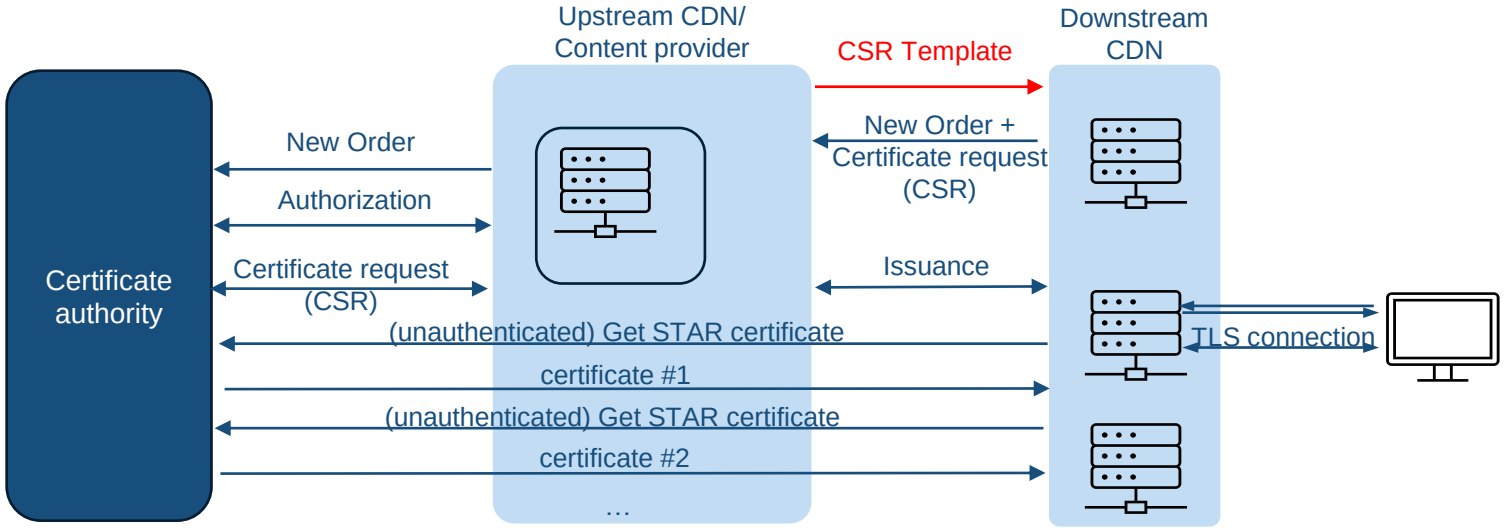
- **CP exposes ACME server interface**
- **CDN sends CSR to CP using a CSR template provided by CP**
- **CP sends CSR for CDN to CA and can cancel certificate generation any time**



ACME/STAR in CDNi

CDNi delegation using ACME environment

- **Working group draft: [draft-ietf-cdni-delegation-acme]**



MI.ACMEDelegationMethod

- **Points to an acme-delegation object, containing the CSR template**

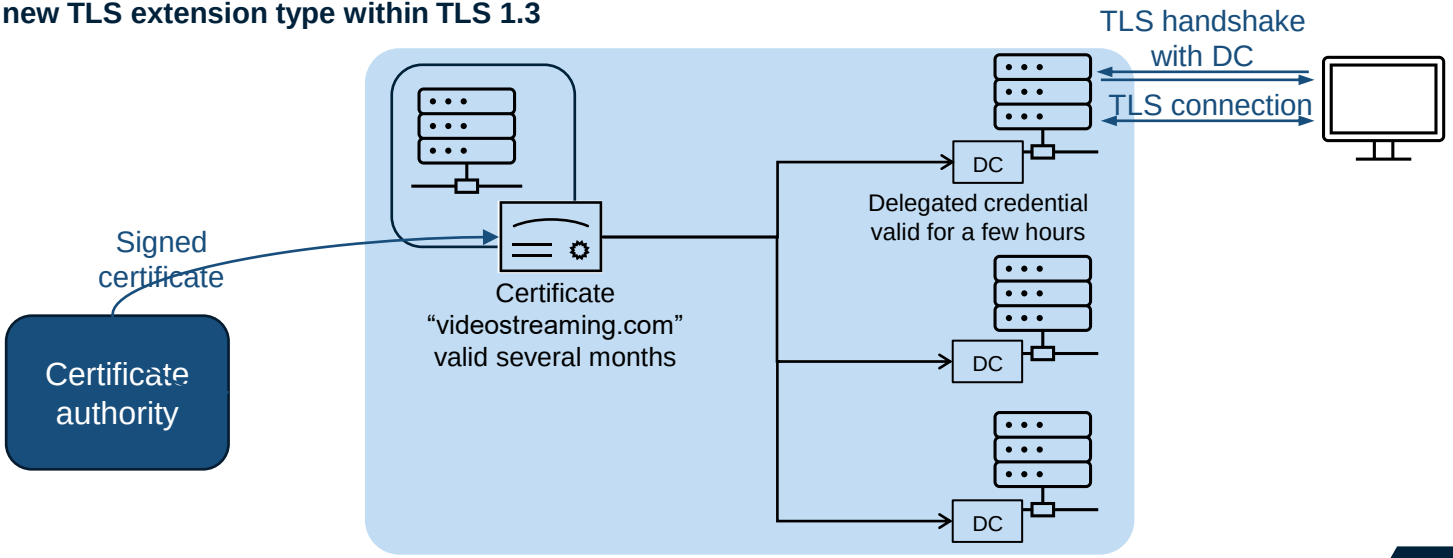
02

Delegated credentials

Delegated credentials

Principles

- **A delegated credential is not a “full-fledged” certificate**
  - **Cryptographic structure containing the public key information of the end-point**
  - **Signed by a “full-fledged” certificate having a DelegationUsage extension**
- **Issued by certificate owner**
  - **Small validity period: 7 days maximum**
- **Allows a peer to terminate TLS on behalf of the certificate owner**
  - **Requires a new TLS extension type within TLS 1.3**



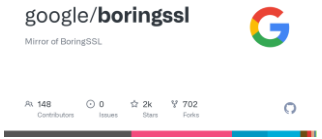
Delegated credentials

Advantages

- Lightweight mechanism for delegation of secure TLS termination
- Allows frequent renewal of short-lived delegated credentials
- No revocation needed
- No need to involve CA in the process (CA validation processes can be long)
- Private key of “full-fledged” certificates are not exposed on end-points
- Limited exposure due to loss or theft of a delegated credential’s private key

Adoption

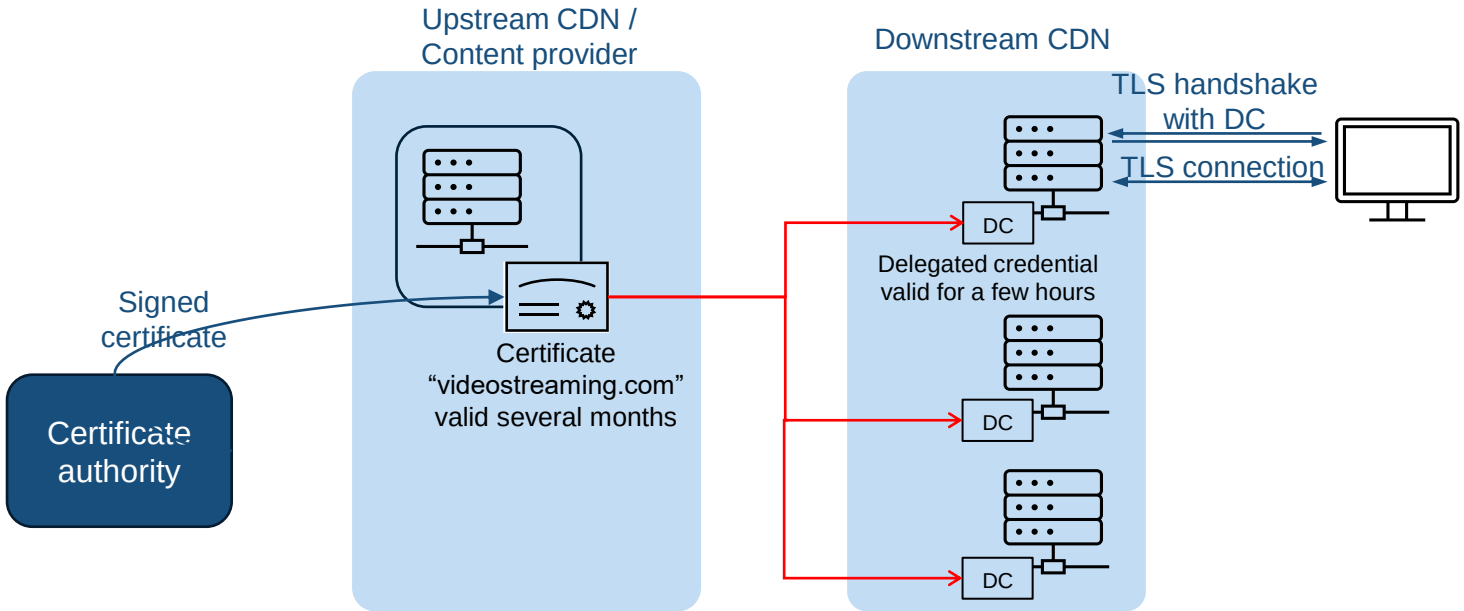
- Supported by some major CAs (e.g., DigiCert)
- Implemented in Facebook’s Fizz, Google’s BoringSSL
- Supported by Cloudflare CDN and Firefox browser
- Standardized by IETF: [RFC9345]
- Limitation: not supported everywhere (yet), legacy device support



Delegated credentials and CDNI

IETF standardization effort ongoing to support delegated credentials in CDNI

- **Working group draft: [draft-ietf-cdni-https-delegation-subcerts]**



Delegated credentials and CDNI – Objects defined

FCI.DelegatedCredentials

- **Allows the dCDN to announce the maximum number of delegated credentials supported; typically, but not necessarily linked with the number of servers**
- **Properties**
  - **number-delegated-certs-supported (mandatory)**
  - **PrivateKeyEncryptionKey (optional)**

```
{ "capabilities": [
        {
         "capability-type": "FCI.DelegatedCredentials",
         "capability-value": {
            "number-delegated-certs-supported": 3
          }
         "footprints": [
            <Footprint objects>
          ]
        }
    ]
}
```

MI.DelegatedCredentials

- **Contains an array of delegated credentials**
- **Allows the uCDN to push a set of delegated credentials to the dCDN**
- **Properties:**
  - **delegated-credentials [array] (mandatory)**
    - **delegated-credential (mandatory)**
    - **private-key (optional)**

```
{ "generic-metadata-type": "MI.DelegatedCredentials",
  "generic-metadata-value": {
    "delegated-credentials": [
            {"delegated-credential":
                "cBBfm8KK6pPz/tdgKyedwA...
                 iXCCIAmzMM0R8FLI3Ba0UQ=="},
        {"delegated-credential":
                "4pyIGtjFdys1+9y/4sS/Fg...
                 J+h9lnRY/xgmi65RLGKoRw=="},
         {"delegated-credential":
                "6PWFO0g2AXvUaULXLObcVA...
                HXoldT/qaYCCNEyCc8JM2A=="}]}
}
```

Delegated credentials and CDNI – Workflow example