

mTLS certificates and Market Participant Webhooks

Last updated by | Alan Parsons | 4 Dec 2023 at 16:19 GMT

Issuing certificates

Certificates are issued through the DIP portal once the Market Participant has onboarded with GlobalSign and completed domain vetting processes.

When creating a certificate, the Certificate admin is presented with the following page:

Add Certificate

Host Name

Domain Name

Domain is required.

Certificate Purpose

Subject Name

Copy

CSR

Create Certificate

Cancel

The table below details the fields, as per the screenshot above, and how they relate to the issued certificate and the associated recipient webhook:

| Field name | Description | Attribute within certificate | Implication on webhook |
|---------------------|---|--|--|
| Hostname | Combined with the domain name, this forms the URL of the desired webhook | DNS Entry (max 2) within the Subject Alternative Name (SAN) | The MP will need to ensure that they create a corresponding DNS entry in their corporate DNS that matches a SAN entry configured within the certificate. |
| Domain name | List of the vetted domains. The a combination of the hostname and the domain name fields constitutes a valid SAN entry | N/A | N/A |
| Certificate purpose | <p>Possible values are;</p> <ul style="list-style-type: none"> • <i>mTLS (only)</i> - this is to be used by DCPs to establish a connection with the DIP. • <i>Signing (only)</i> - this is to be used by an MP to sign messages that will be sent by a DCP on their behalf. • <i>mTLS & Signing</i> - to be used by direct MPs and can be used for both mTLS and signing <p>This is used to generate the subject name.</p> | N/A | N/A |
| Subject name | <p>Is a concatenation used to generate the required Common Name (cn):</p> <ul style="list-style-type: none"> • Environment prefix • Certificate purpose (mTLS, Sig or <blank> • Org ID • Domain name <p>This gives a combined value of {Environment prefix}.{Cert</p> | Is the common name part of the certificate subject attribute, and is configured as an additional DNS entry in the SAN. | This can be used as the URL for the webhook as it is an entry in the SAN. |

| Field name | Description | Attribute within certificate | Implication on webhook |
|------------|---|------------------------------|------------------------|
| | purpose}.{Org ID}.{Domain name}} | | |
| CSR | The Market Participant generates and pastes the CSR (see below) | N/A | N/A |

Generating the CSR

Issuance Policy

whs-company1

 Save  Discard changes

 Issuance policies only affect certificates that will be issued in the future. Modifying this issuance policy will not affect any existing certificates.

| | |
|------------------------------------|---|
| Created | 25/10/2023, 17:24:29 |
| Updated | 25/10/2023, 17:25:07 |
| Type of Certificate Authority (CA) | <input type="text" value="Certificate issued by a non-integrated CA"/> |
| Subject * | <input type="text" value="cn=energydip-dev.81.company1.testmp.co.uk"/> |
| DNS Names | 2 DNS names |
| Validity Period (in months) * | <input type="text" value="12"/> |
| Content Type | <input checked="" type="radio"/> PKCS #12 <input type="radio"/> PEM |
| Enabled | <input checked="" type="radio"/> Yes <input type="radio"/> No |
| Lifetime Action Type | <input type="text" value="E-mail all contacts at a given percentage lifetime"/> |
| Percentage Lifetime * | <input type="range" value="80"/> 80 |
| Advanced Policy Configuration | Not configured |

| Attribute | Value |
|------------------------------------|---|
| Type of Certificate Authority (CA) | Certificate issued by a non-integrated CA |
| Subject | Needs to specify the CN (Common name), whereby the value is equal to the subject name generated in the DIP portal. |
| DNS name | <p>Requires two entries:</p> <ul style="list-style-type: none"> • The subject name specified in the DIP portal (matches the common name) • Hostname.Domain name (webhook URL) <p>If either entry is not present, the certificate will not merge</p> |
| Advanced Policy Configuration | Key Size: 4096 |

Once submitted, GlobalSign will sign the CSR and generate the certificate. The certificate is then available to download the certificate as a .cer file, which can then be merged with the CSR/Private Key to complete and form the key pair.

The certificate

With a .cer file, you can open it and view the attributes (found in the certificate details tab in Windows), or use the following OpenSSL command to view the attributes: `openssl x509 -noout -text -in 'cerfile.cer';` . This produces output, as per the example below:

```

Certificate:
Data:
  Version: 3 (0x2)
  Serial Number:
    01:29:97:3e:46:f4:9c:36:6f:8e:41:69:bb:0b:69:d5
  Signature Algorithm: sha256WithRSAEncryption
  Issuer: C = GB, O = ELEXON LIMITED, CN = MHHS DIP Message Security Issuing CA 2023
  Validity
    Not Before: Nov  2 16:38:59 2023 GMT
    Not After : Nov  1 16:38:59 2024 GMT
  Subject: C = GB, ST = City of London, L = London, O = Avanade UK, CN = energydip-dev.mtls.81.company7.testmp.co.uk
  Subject Public Key Info:
    Public Key Algorithm: rsaEncryption
    RSA Public-Key: (4096 bit)
    Modulus:
      00:d2:45:ce:69:b2:da:18:aa:77:cd:46:b5:63:91:
      4c:20:c9:a0:89:1e:a0:10:4d:b6:f6:8e:7c:ac:c6:
      15:43:41:c3:63:28:e7:ef:e8:d9:d8:d2:04:c7:e2:
      26:a8:1a:6d:9c:df:11:b6:8a:91:5c:a2:c8:c2:d6:
      a3:20:ab:ef:c7:ef:89:f1:9c:48:bf:a4:c5:75:77:
      0d:43:7f:a2:e2:4c:2b:1e:32:22:ce:5b:0d:24:75:
      18:a6:d4:c4:6e:4e:de:e4:e6:18:6f:d5:f2:71:52:
      1f:19:17:ce:30:78:e6:16:ba:1d:2c:b8:3b:9d:c3:
      d2:c8:75:d9:33:a4:1f:5b:c5:73:c4:e7:a6:6d:82:
      3d:62:af:ef:30:c7:91:0b:c1:a0:c4:5c:83:b2:9c:
      8b:21:ba:a4:a5:64:9e:bf:19:e6:f3:07:a8:5c:9d:
      a1:6d:20:be:3e:1a:5a:70:8f:72:67:4c:f1:dd:07:
      18:e9:db:ea:40:20:4d:43:63:74:c2:e7:69:e2:63:
      ff:95:82:4c:3d:5f:74:1f:7d:ce:46:1f:13:07:67:
      a4:b1:98:7f:d5:fc:84:34:25:49:86:44:96:48:c9:
      a3:d0:78:35:56:b0:a4:d7:1f:47:27:7b:fe:a1:58:
      b9:76:14:82:14:1a:84:7c:c9:b9:61:45:76:95:0f:
      db:28:69:8c:3f:23:4a:c2:fe:dc:10:1c:88:25:5f:
      8f:54:5a:eb:66:e2:e5:b3:2d:f1:89:8a:29:0d:e7:
      73:56:2e:12:5c:12:1c:fa:07:c8:e9:30:d0:35:82:
      49:ad:f1:f2:63:d2:82:ef:e2:90:e6:36:ec:6b:6f:
      90:7b:f8:a9:6e:61:46:0f:38:29:bf:3d:e0:f0:6e:
      52:91:31:89:a0:db:ce:b6:ee:fa:bc:ec:d1:91:52:
      9e:3e:dd:71:78:9a:12:c0:4c:5f:43:91:8d:49:eb:
      39:aa:ce:dd:89:12:04:18:fc:fc:57:26:a0:33:c7:
      37:ae:06:f3:b2:a8:14:5e:6a:4e:cd:96:e1:67:52:
      31:3b:78:b2:e4:5e:5c:d1:23:7a:8f:63:66:52:d8:
      2e:df:75:96:c0:3c:50:2d:50:ef:ad:50:e7:7f:0e:
      51:b5:29:db:f1:74:95:b4:03:d5:a6:80:af:8c:bc:
      23:96:35:a8:ec:0f:76:01:ea:9f:a8:9a:10:d2:66:
      42:97:2d:5d:73:9f:2b:84:98:eb:3f:d3:e3:31:c6:
      7f:8d:5d:0b:f6:6e:4d:c5:35:4e:60:0f:c6:57:f7:
      f0:24:87:d5:53:7e:55:42:09:59:df:3e:40:f2:57:
      06:af:cf:b5:c0:12:9d:62:5d:f5:7b:e2:41:65:c9:
      b3:41:15
    Exponent: 65537 (0x10001)
  X509v3 extensions:
    X509v3 Subject Alternative Name:
      DNS:energydip-dev.mtls.81.company7.testmp.co.uk, DNS:agw.company7.testmp.co.uk
    X509v3 Key Usage: critical
      Digital Signature, Key Encipherment
    X509v3 Extended Key Usage:
      TLS Web Server Authentication, TLS Web Client Authentication
    X509v3 Subject Key Identifier:
      7C:10:9C:4E:87:A5:E0:1C:2B:02:ED:A9:B5:9C:F9:30:66:93:A6:FD
    X509v3 Certificate Policies: critical
      Policy: 1.3.6.1.4.1.4146.11.1.3
      CPS: https://www.globalsign.com/repository/

    X509v3 Basic Constraints: critical
      CA:FALSE
  Authority Information Access:
    OCSP - URI:http://ocsp.p.globalsign.com/mhhsdipmessagesecurityica2023
    CA Issuers - URI:http://secure.p.globalsign.com/cacert/mhhsdipmessagesecurityica2023.crt

  X509v3 Authority Key Identifier:
    keyid:86:1F:26:8B:93:C9:C7:69:9B:D0:3A:24:A3:BD:AC:56:44:1B:C2:E0

```

The following table describes the attributes, as per the screenshot above:

| Name | Value | Notes |
|---------------------------------|--|--|
| Subject | The Common Name (CN) as value specified in the portal. The other attributes are derived from the Identity Profile (company details) as inputted and vetted during the GlobalSign registration process. | The Common Name is used in checks with the DIP, for example when confirming that the environment prefix is correct. |
| Issuer | Is our dedicated CA. This will always be: <i>C = GB, O = ELEXON LIMITED, CN = MHHS DIP Message Security Issuing CA 2023</i> | This is non-longer used as text in any checks, but App Gateway and API-Management does test the chain of the incoming client certificate, ensuring that the client certificate is issued by this Issuer. |
| Validity | Not before is the time the certificate was signed. Not after will be 397 days from signing (A year + 32 days leaway) | Normal certificates issued from public trust CAs will expire in 3 months |
| Authority Information Access | Details the OCSP (Online Certificate Status Protocol) URL for the certificate | OCSP is used by App Gateway to check the revocation status of a cert (during mTLS checks). |
| X509v3 CRL Distribution Points | The Certificate Revocation List (CRL) URL | This URL needs to be allowed through the firewall. |
| X509v3 Subject Alternative Name | The DNS names/URLs that this certificate can be bound too | This will consist of a DNS entry based on the Subject Name, and an entry based on hostname+domain name. |