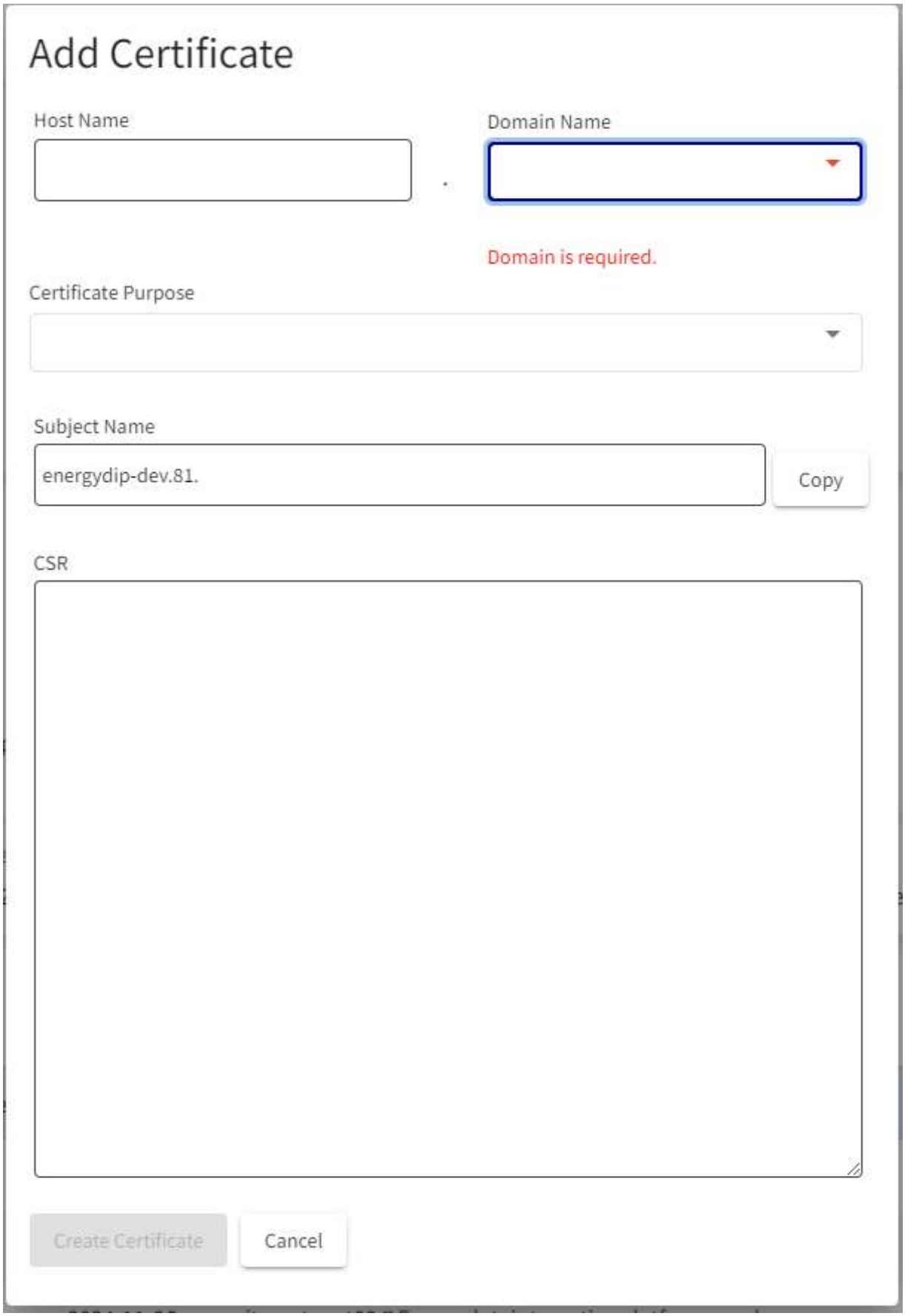
mTLS certificates and Market Participant Webhooks

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:

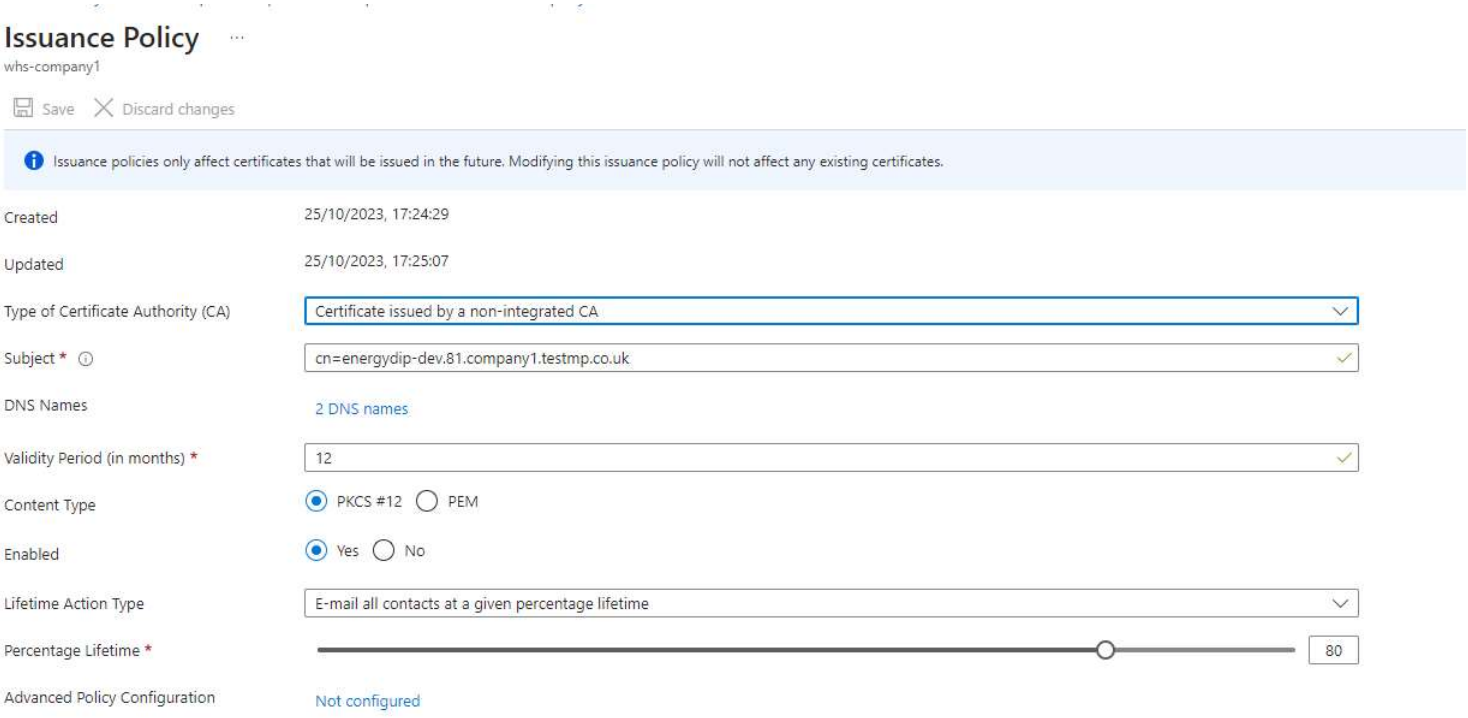


The table below details the fields, as per the screenshot above, and how they relate to the issued certificate and the associated recipient webhook:

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	Possible values are; • *mTLS (only)* - this is to be used by DCPs to establish a connection with the DIP. • *Signing (only)* - this is to be used by an MP to sign messages that will be sent by a DCP on their behalf. • *mTLS & Signing* - to be used by direct MPs and can be used for both mTLS and signing This is used to generate the subject name.	N/A	N/A
Subject name	Is a concatenation used to generate the required Common Name (cn): • Environment prefix • Certificate purpose (mTLS, Sig or <blank> • Org ID • Domain name This gives a combined value of {Environment prefix}.{Cert	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

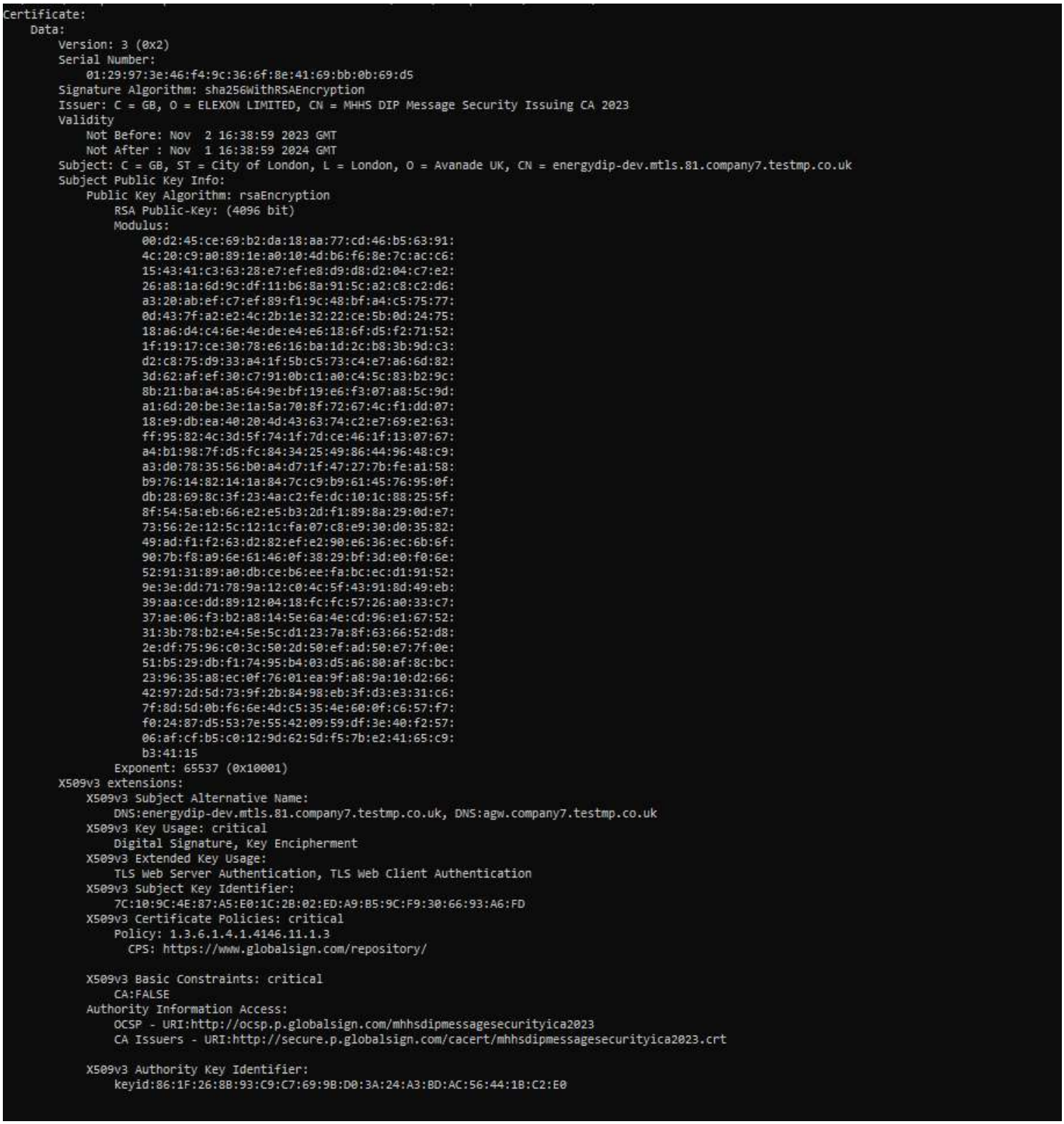


Attribute	Value
Type of Certificate Authority (CA)	Certificate issued by a non-integrated CA
Subject	Needs to specify the CN (Common name), whereby the value is equal to the subject name generated in the DIP portal.
DNS name	Requires two entries: • The subject name specified in the DIP portal (matches the common name) • Hostname.Domain name (webhook URL) If either entry is not present, the certificate will not merge
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:



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: *C = GB, O = ELEXON LIMITED, CN = MHHS DIP Message Security Issuing CA 2023*	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.