**What sort of certificate do we need for this?**

Yes, we need a TLS (Transport Layer Security) certificate for mutual authentication and encrypted communication between our application and Citi's APIs. This is different from SMIME certificates, which are primarily used for securing email communications.

**What should the Common Name be?**

**Common Name (CN):** The Common Name should typically be a fully-qualified domain name (FQDN) that represents our application’s domain. For example, if our domain is www.ned.org, the CN should be www.ned.org. This ensures the certificate is tied to our specific domain.

## **Certificate Requirements**

The below is the minimum set of requirements for the certificates used for Citi APIs:

* Certificates must be issued by a Certificate Authority that is a member of the Certificate and Browser forum. You can find a list of recognized authorities at the [CAB Forum Members site](https://cabforum.org/members/)
* X509 certificates with file formats of \*.cer or \*.pem are accepted for sign-in and encryption. The base64-encoded certificate file must be embedded with all intermediate and root certificates.
* Certificates should use a Certificate Name (CN) value in the Subject field. It is recommended that production certificates be valid for at least a year from the date they are uploaded. Certificates for test environments can expire in as little as one day
* Certificates must be either Organization Validated (OV) or Extended Validation (EV). Domain Validated (DV) Certificates are not acceptable since issuing CA checks only the domain registry and not the legal entity/organizational unit.
* OV Certificates are verified for legitimate business information. As an example,
  + Certificate Name CN = www.domain.com
  + Organization O = Domain Services ltd.
  + Organizational Unit OU = Treasury IT
  + Location L = San Diego
  + State S = California
  + Country C = US
* EV Certificates provide more trust and security than the DV and OV Certificates

**Where is this certificate going to be installed and by whom?**

The private key, along with its associated certificates, will be installed on the environment where Business Central is running and making API calls to Citi.

**Should we plan to provide you with both the certificate and the private key?**

Yes, you should provide both the certificate and the private key to us if we’re handling the integration and installation.

**Should the certificate be encrypted or not?**

The certificate itself doesn't need to be encrypted. It depends on your organization's security policies. The communication channel (using TLS) will ensure the data is encrypted in transit.