(1) Send GET foo.com request to proxy using TLS connection
(2) DNS lookup from proxy for foo.com
(3) CDN DNS lookup for a19.akamai.net (some Akamai ID that represents foo.com)
(4) Proxy sends DNS request to origin's authoritative server, and the origin publishes $\{k\}_{PK(proxy)}$ in the SRV record. Then the proxy decrypts the shared key with his own private key
(5) Proxy generates GET $HMAC_k$(URL) request
(6) Proxy sends request to cache node
(7) Cache node returns $\{content\}_k$, $\{cert\}_k$ to proxy. Proxy decrypts and validates the cert. Once the cert is validated, proxy decrypts the content with origin server's shared key
(8) Proxy returns decrypted content to client (using TLS)