**ACRONYMS / TERMINOLOGY**

TLS – Transport Layer Security:  Cryptographic protocol that provides secure online communication

SSL – Secure Socket Layer:  Cryptographic protocol that provides secure online communication

RSA – Rivest, Shamir, Adleman:  Algorithm for public-key cryptography

SHA – Secure Hash Algorithm:  Cryptographic hash function

CRL – Certificate Revocation List:  A list of certificates that have been revoked

OCSP – Online Certificate Status Protocol:  Internet protocol used for obtaining the revocation status of x.509 digital certificate

x.509 – Specifies, amongst other things, standard formats for public key certificates, certificate revocation lists, attribute certificates, and a certification path validation algorithm

CN – Common Name:  The primary domain to be secured on a certificate

SAN – Subject Alternative Name:   Different name on certificate other than common name

FQDN – Fully Qualified Domain Name:  Complete domain name for specified host

PKI – Public Key Infrastructure:  Set of hardware, software, people, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates

CSR – Certificate Signing Request:  Encoded text that contains an organizations information (name, unit, location)

EV – Extended Validation:  Certificates that require a more stringent validation process (green bar certificates)

**INTERNAL ACRONYMS**

DCV – Domain Control Validation:  Email sent out to WHOIS contacts and admin contacts on base domain requesting confirmation of domain control and approval

OV – Ordinary Validation: Standard non-EV SSL certificates

MA – Master Agreement:  Agreement between certificate applicant and DigiCert

DAL – Domain Authorization Letter:  Letter of approval from domain owner for certificate applicant to get an SSL certificate for their domain

** Also see "Glossary of SSL, Server, and Validation Terms in DigiCert Wiki