**Electronic Logging Devices and Hours of Service - Provider Updates**

**Why does an ELD provider need to submit a public key?**

Provider certificates, which must include a public key, are vital to completing both the telematics and local transfer options for submitting ELD data. The following is excerpted from the ELD Interface Control Document and Web Services Development Handbook, which is now available in the ELD Provider Portal (you will need to log in with your user account).

## Provider Certificates

All providers will need a public/private key pair for their ELDs. The Public/Private Key pair must be compliant with the NIST SP800–32, Introduction to Public Key Technology and the Federal PKI Infrastructure. Key pairs do not have to be unique for individual devices—the same public/private key pair can be used by a provider for all ELD devices. However, each provider must have their own public/private key pair (they may not be shared by providers). Providers must register the public key portion of the public/private key pair registered with their ELD. This is done by submitting a vendor certificate containing the public key. Submitting this certificate is a required step in the ELD registration process (See section 5.2.2).

Providers may purchase a certificate from a certificate authority (CA), or may use a self-signed certificate. When requesting a certificate from a CA or generating a self-signed certificate, providers must make certain the certificate adheres to best practices as detailed in Section 2.2.1 of the ELD Interface Control Document and Web Services Development Handbook.

Providers will use their certificates when:

* Electronically signing emails when submitting ELD data to FMCSA using the email data transfer method (see Section 4.10.1.2).
* Connecting to FMCSA ELD web services to submit ELD data (see Section 4.10.1.1 and 4.10.1.4 (c)). Note: This is a requirement for both web services and Bluetooth data transfer methods.
* Calculating ELD Authentication Values when generating ELD files for all data transfer methods (see Section 5.2.2 and 7.14).

FMCSA will honor the expiration date listed in providers’ certificates. Should an ELD device submit data using an expired certificate, FMCSA will consider the device to be out of compliance with the ELD rule.

To provide your certificate containing your public key to FMCSA:

1. Log into your account.
2. From the left side navigation, select “My ELDs.”
3. Under “Actions,” select “Edit.”
4. Under “Certificate,” select “Choose File” to select and upload your certificate file or files that conform to the best practices as noted in Section 2.2.1 of the ELD Interface Control Document and Web Services Development Handbook.
5. Repeat for each ELD, if necessary.