Certificate Implementation/Renewal Process

This applies to:

- 3rd Party DMS Keys
- Pierce Keys
- Thurston Keys
- Jindex Keys

Certificate Requirements

1) The key exchange systems supported are the Rivest-Shamir-Adleman (RSA) algorithms and the Digital Signature Standard (DSS). The Advanced Encryption Standard (AES) exchange system for signature keys, is not supported (ie, CNG).
2) Signed by Externally "trusted CA" (ie: GoDaddy; commodo; etc)
3) Validation Periods should be 1 year minimum. Replacement with AOC should not be necessary prior to that validation's expiry.
4) Provide the Public Key to AOC in DER encoded binary X.509 format (if at all possible, please attach it to the eService Incident).

When a new key is needed to be provided to the AOC, the site should work with their local court contact and submit an eService request. Please cut and paste the below information into the eService incident with the appropriate information provided.

The AOC requests a ***two week advance notice*** for certificate replacement. Expired Certificate will cause the service to HALT.

Todays Date:

Court Impacted:

IT Contact Name:

IT Contact Phone:

IT Contact e-mail:

Reason for the Change:

Date/Time Requested for Swap:

Provide Public Key in X.509 format (attach to ticket).

A copy of the above instructions are available below in PDF format, if you need to share this information with IT staff.