Digital Certificate Requirements DMV, State of Nevada

Platform: Microsoft Windows

Operating System: Windows 2003/2008

Supported certificate package formats:
The certificate package must be in one of the following formats:

1. A single BER encoded X.509 certificate.
2. A single Base64 encoded X.509 certificate.
3. A Privacy Enhanced Mail (PEM) encoded X.509 certificate. If the input is in this format, only the Originator Certificate is used.

Details regarding all certificates
The following are additional details regarding certificate processing:

1. All fields as defined for X.509 version 1 certificate must be present and must have a length greater than zero (non-null).
2. X.509 certificates with version numbers greater than 3 are not supported.
3. Noncritical extensions are ignored. Critical extensions that are supported include:
    - keyUsage - { 2 5 29 15 }
    - basicConstraints - { 2 5 29 19 }
    - subjectAltname - { 2 5 29 17 }
    - issuerAltName - { 2 5 29 18 }
    - certificatePolicies - { 2 5 29 32 }
    - policyMappings - { 2 5 29 33 }
    - policyConstraints - { 2 5 29 36 }
    - nameConstraints - { 2 5 29 30 }
    - extKeyUsage - { 2 5 29 37 }
    - hostIdMapping - { 1 3 18 0 2 18 1 }
    - subjectKeyIdentifier - { 2 5 29 14 }
    - authorityKeyIdentifier - { 2 5 29 35 }