

Digital Certificate Requirements for the State of Nevada

Platform: IBM z9 BC (Business Class mainframe)

Operating System: z/OS v1.8

Security Package: RACF v1.8

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.
4. One or more X.509 certificates contained within a PKCS #7 DER encoding package.
5. One or more X.509 certificates and private keys contained within a PKCS #12 DER encoding package. If the input is in this format, all certificates are processed but only the first user private key is used. PKCS #12 is also known as Private Information Exchange (PFX). The obsolete PFX V0.02 standard is not supported.

Details regarding all certificates

The following are additional details regarding RACDCERT's certificate processing:

1. All fields as defined for X.509 version 1 certificates 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:
 - o keyUsage - { 2 5 29 15 }
 - o basicConstraints - { 2 5 29 19 }
 - o subjectAltname - { 2 5 29 17 }
 - o issuerAltName - { 2 5 29 18 }
 - o certificatePolicies - { 2 5 29 32 }
 - o policyMappings - { 2 5 29 33 }
 - o policyConstraints - { 2 5 29 36 }
 - o nameConstraints - { 2 5 29 30 }
 - o extKeyUsage - { 2 5 29 37 }
 - o hostIdMapping - { 1 3 18 0 2 18 1 }
 - o subjectKeyIdentifier - { 2 5 29 14 }
 - o authorityKeyIdentifier - { 2 5 29 35 }
4. Subject and issuer names can contain only the following string types:
 - o UTF8 - TAG 12 (7-bit ASCII only)
 - o PRINTABLESTRING - TAG 19
 - o T61STRING - TAG 20
 - o IA5STRING - TAG 22
 - o VISIBLESTRING - TAG 26
 - o GENERALSTRING - TAG 27
 - o BMPString - TAG 30 (ASCII Unicode only)