

crt.sh id	not before	not after	lint
10022111	2015-10-06 05:36:13	2018-01-06 05:36:12	<p>cablintERRORBR certificates with organizationName must include either localityName or stateOrProvinceName</p> <p>cablintWARNINGCertificate does not include authorityInformationAccess. BRs require OCSP stapling for this certificate.</p> <p>cablintWARNINGDeprecated Netscape extension 2.16.840.1.113730.1.1 treated as opaque extension</p> <p>cablintWARNINGTLS Server auth certificates should not contain Netscape Server Gated Crypto usage</p> <p>cablintINFOTLS Server certificate identified</p> <p>x509lintERRORError parsing URL</p> <p>x509lintERRORno authorityInformationAccess extension</p> <p>x509lintERRORNo OCSP over HTTP</p> <p>x509lintERRORSubject with organizationName, givenName or surname but without stateOrProvince or localityName</p> <p>x509lintWARNINGexplicitText is not using a UTF8String</p> <p>x509lintWARNINGNo HTTP URL for issuing certificate</p> <p>x509lintWARNINGPolicy information has qualifier other than CPS URI</p> <p>x509lintWARNINGUnknown extended key usage</p> <p>x509lintINFOSubject has a deprecated CommonName</p> <p>x509lintINFOUnknown validation policy</p> <p>zlintERRORSubscriber Certificate: authorityInformationAccess MUST contain the HTTP URL of the Issuing CA's OSCP responder.</p> <p>zlintERRORSubscriber certificate cRLDistributionPoints extension must contain the HTTP URL of the CA's CRL service</p> <p>zlintERRORSubscriber Certificate: authorityInformationAccess MUST be present, with the exception of stapling.</p> <p>zlintWARNINGCompliant certificates should use the utf8string encoding for explicitText</p> <p>zlintWARNINGSubscriber Certificate: extKeyUsage either the value id-kp-serverAuth or id-kp-clientAuth or both values MUST be present.</p> <p>zlintWARNINGSubscriber certificates authorityInformationAccess extension should contain the HTTP URL of the issuing CA's certificate</p> <p>zlintNOTICESubscriber Certificate: commonName is deprecated.</p>

cablintERRORBR certificates with organizationName must include either localityName or stateOrProvinceName
cablintWARNINGCertificate does not include authorityInformationAccess. BRs require OCSP stapling for this certificate.
cablintWARNINGDeprecated Netscape extension 2.16.840.1.113730.1.1 treated as opaque extension
cablintWARNINGTLS Server auth certificates should not contain Netscape Server Gated Crypto usage
cablintINFOTLS Server certificate identified
x509lintERRORError parsing URL
x509lintERRORno authorityInformationAccess extension
x509lintERRORNo OCSP over HTTP
x509lintERRORSubject with organizationName, givenName or surname but without stateOrProvince or localityName
x509lintWARNINGexplicitText is not using a UTF8String
x509lintWARNINGNo HTTP URL for issuing certificate
x509lintWARNINGPolicy information has qualifier other than CPS URI
10176492 2015-10-12 04:15:33 2018-01-12 04:15:32 x509lintWARNINGUnknown extended key usage
x509lintINFOSubject has a deprecated CommonName
x509lintINFOUnknown validation policy
zlintERRORSubscriber Certificate: authorityInformationAccess MUST contain the HTTP URL of the Issuing CA's OSCP responder.
zlintERRORSubscriber certificate cRLDistributionPoints extension must contain the HTTP URL of the CA's CRL service
zlintERRORSubscriber Certificate: authorityInformationAccess MUST be present, with the exception of stapling.
zlintWARNINGCompliant certificates should use the utf8string encoding for explicitText
zlintWARNINGSubscriber Certificate: extKeyUsage either the value id-kp-serverAuth or id-kp-clientAuth or both values MUST be present.
zlintWARNINGSubscriber certificates authorityInformationAccess extension should contain the HTTP URL of the issuing CA's certificate
zlintNOTICESubscriber Certificate: commonName is deprecated.

cablintERRORBR certificates with organizationName must include either localityName or stateOrProvinceName
cablintWARNINGCertificate does not include authorityInformationAccess. BRs require OCSP stapling for this certificate.
cablintWARNINGDeprecated Netscape extension 2.16.840.1.113730.1.1 treated as opaque extension
cablintWARNINGTLS Server auth certificates should not contain Netscape Server Gated Crypto usage
cablintINFOTLS Server certificate identified
x509lintERRORError parsing URL
x509lintERRORno authorityInformationAccess extension
x509lintERRORNo OCSP over HTTP
x509lintERRORSubject with organizationName, givenName or surname but without stateOrProvince or localityName
x509lintWARNINGexplicitText is not using a UTF8String
x509lintWARNINGNo HTTP URL for issuing certificate
15455964 2015-11-18 00:39:57 2018-02-18 00:39:56 x509lintWARNINGPolicy information has qualifier other than CPS URI
x509lintWARNINGUnknown extended key usage
x509lintINFOSubject has a deprecated CommonName
x509lintINFOUnknown validation policy
zlintERRORSubscriber Certificate: authorityInformationAccess MUST contain the HTTP URL of the Issuing CA's OSCP responder.
zlintERRORSubscriber certificate cRLDistributionPoints extension must contain the HTTP URL of the CA's CRL service
zlintERRORSubscriber Certificate: authorityInformationAccess MUST be present, with the exception of stapling.
zlintWARNINGCompliant certificates should use the utf8string encoding for explicitText
zlintWARNINGSubscriber Certificate: extKeyUsage either the value id-kp-serverAuth or id-kp-clientAuth or both values MUST be present.
zlintWARNINGSubscriber certificates authorityInformationAccess extension should contain the HTTP URL of the issuing CA's certificate
zlintNOTICESubscriber Certificate: commonName is deprecated.

cablintERRORBR certificates with organizationName must include either localityName or stateOrProvinceName
cablintWARNINGCertificate does not include authorityInformationAccess. BRs require OCSP stapling for this certificate.
cablintWARNINGDeprecated Netscape extension 2.16.840.1.113730.1.1 treated as opaque extension
cablintWARNINGTLS Server auth certificates should not contain Netscape Server Gated Crypto usage
cablintINFOTLS Server certificate identified
x509lintERRORError parsing URL
x509lintERRORno authorityInformationAccess extension
x509lintERRORNo OCSP over HTTP
x509lintERRORSubject with organizationName, givenName or surname but without stateOrProvince or localityName
x509lintWARNINGexplicitText is not using a UTF8String
x509lintWARNINGNo HTTP URL for issuing certificate
10203472 2015-10-07 07:43:06 2018-01-07 07:43:05 x509lintWARNINGPolicy information has qualifier other than CPS URI
x509lintWARNINGUnknown extended key usage
x509lintINFOSubject has a deprecated CommonName
x509lintINFOUnknown validation policy
zlintERRORSubscriber Certificate: authorityInformationAccess MUST contain the HTTP URL of the Issuing CA's OSCP responder.
zlintERRORSubscriber certificate cRLDistributionPoints extension must contain the HTTP URL of the CA's CRL service
zlintERRORSubscriber Certificate: authorityInformationAccess MUST be present, with the exception of stapling.
zlintWARNINGCompliant certificates should use the utf8string encoding for explicitText
zlintWARNINGSubscriber Certificate: extKeyUsage either the value id-kp-serverAuth or id-kp-clientAuth or both values MUST be present.
zlintWARNINGSubscriber certificates authorityInformationAccess extension should contain the HTTP URL of the issuing CA's certificate
zlintNOTICESubscriber Certificate: commonName is deprecated.

cablintERRORBR certificates with organizationName must include either localityName or stateOrProvinceName
cablintWARNINGCertificate does not include authorityInformationAccess. BRs require OCSP stapling for this certificate.
cablintWARNINGDeprecated Netscape extension 2.16.840.1.113730.1.1 treated as opaque extension
cablintWARNINGTLS Server auth certificates should not contain Netscape Server Gated Crypto usage
cablintINFOTLS Server certificate identified
x509lintERRORError parsing URL
x509lintERRORno authorityInformationAccess extension
x509lintERRORNo OCSP over HTTP
x509lintERRORSubject with organizationName, givenName or surname but without stateOrProvince or localityName
x509lintWARNINGexplicitText is not using a UTF8String
x509lintWARNINGNo HTTP URL for issuing certificate
10805402 2015-11-12 09:19:40 2018-02-12 09:19:39 x509lintWARNINGPolicy information has qualifier other than CPS URI
x509lintWARNINGUnknown extended key usage
x509lintINFOSubject has a deprecated CommonName
x509lintINFOUnknown validation policy
zlintERRORSubscriber Certificate: authorityInformationAccess MUST contain the HTTP URL of the Issuing CA's OSCP responder.
zlintERRORSubscriber certificate cRLDistributionPoints extension must contain the HTTP URL of the CA's CRL service
zlintERRORSubscriber Certificate: authorityInformationAccess MUST be present, with the exception of stapling.
zlintWARNINGCompliant certificates should use the utf8string encoding for explicitText
zlintWARNINGSubscriber Certificate: extKeyUsage either the value id-kp-serverAuth or id-kp-clientAuth or both values MUST be present.
zlintWARNINGSubscriber certificates authorityInformationAccess extension should contain the HTTP URL of the issuing CA's certificate
zlintNOTICESubscriber Certificate: commonName is deprecated.

cablintERRORBR certificates with organizationName must include either localityName or stateOrProvinceName
cablintWARNINGCertificate does not include authorityInformationAccess. BRs require OCSP stapling for this certificate.
cablintWARNINGDeprecated Netscape extension 2.16.840.1.113730.1.1 treated as opaque extension
cablintWARNINGTLS Server auth certificates should not contain Netscape Server Gated Crypto usage
cablintINFOTLS Server certificate identified
x509lintERRORError parsing URL
x509lintERRORno authorityInformationAccess extension
x509lintERRORNo OCSP over HTTP
x509lintERRORSubject with organizationName, givenName or surname but without stateOrProvince or localityName
x509lintWARNINGexplicitText is not using a UTF8String
x509lintWARNINGNo HTTP URL for issuing certificate
10312197 2015-10-16 06:27:43 2018-01-16 06:27:42 x509lintWARNINGPolicy information has qualifier other than CPS URI
x509lintWARNINGUnknown extended key usage
x509lintINFOSubject has a deprecated CommonName
x509lintINFOUnknown validation policy
zlintERRORSubscriber Certificate: authorityInformationAccess MUST contain the HTTP URL of the Issuing CA's OSCP responder.
zlintERRORSubscriber certificate cRLDistributionPoints extension must contain the HTTP URL of the CA's CRL service
zlintERRORSubscriber Certificate: authorityInformationAccess MUST be present, with the exception of stapling.
zlintWARNINGCompliant certificates should use the utf8string encoding for explicitText
zlintWARNINGSubscriber Certificate: extKeyUsage either the value id-kp-serverAuth or id-kp-clientAuth or both values MUST be present.
zlintWARNINGSubscriber certificates authorityInformationAccess extension should contain the HTTP URL of the issuing CA's certificate
zlintNOTICESubscriber Certificate: commonName is deprecated.

cablintERRORBR certificates with organizationName must include either localityName or stateOrProvinceName
cablintWARNINGCertificate does not include authorityInformationAccess. BRs require OCSP stapling for this certificate.
cablintWARNINGDeprecated Netscape extension 2.16.840.1.113730.1.1 treated as opaque extension
cablintWARNINGTLS Server auth certificates should not contain Netscape Server Gated Crypto usage
cablintINFOTLS Server certificate identified
x509lintERRORError parsing URL
x509lintERRORno authorityInformationAccess extension
x509lintERRORNo OCSP over HTTP
x509lintERRORSubject with organizationName, givenName or surname but without stateOrProvince or localityName
x509lintWARNINGexplicitText is not using a UTF8String
x509lintWARNINGNo HTTP URL for issuing certificate
11103995 2015-09-25 04:12:09 2017-12-25 04:12:08 x509lintWARNINGPolicy information has qualifier other than CPS URI
x509lintWARNINGUnknown extended key usage
x509lintINFOSubject has a deprecated CommonName
x509lintINFOUnknown validation policy
zlintERRORSubscriber Certificate: authorityInformationAccess MUST contain the HTTP URL of the Issuing CA's OSCP responder.
zlintERRORSubscriber certificate cRLDistributionPoints extension must contain the HTTP URL of the CA's CRL service
zlintERRORSubscriber Certificate: authorityInformationAccess MUST be present, with the exception of stapling.
zlintWARNINGCompliant certificates should use the utf8string encoding for explicitText
zlintWARNINGSubscriber Certificate: extKeyUsage either the value id-kp-serverAuth or id-kp-clientAuth or both values MUST be present.
zlintWARNINGSubscriber certificates authorityInformationAccess extension should contain the HTTP URL of the issuing CA's certificate
zlintNOTICESubscriber Certificate: commonName is deprecated.

cablintERRORBR certificates with organizationName must include either localityName or stateOrProvinceName
cablintWARNINGCertificate does not include authorityInformationAccess. BRs require OCSP stapling for this certificate.
cablintWARNINGDeprecated Netscape extension 2.16.840.1.113730.1.1 treated as opaque extension
cablintWARNINGTLS Server auth certificates should not contain Netscape Server Gated Crypto usage
cablintINFOTLS Server certificate identified
x509lintERRORError parsing URL
x509lintERRORno authorityInformationAccess extension
x509lintERRORNo OCSP over HTTP
x509lintERRORSubject with organizationName, givenName or surname but without stateOrProvince or localityName
x509lintWARNINGexplicitText is not using a UTF8String
x509lintWARNINGNo HTTP URL for issuing certificate
10832428 2015-11-17 03:51:59 2018-02-17 03:51:58 x509lintWARNINGPolicy information has qualifier other than CPS URI
x509lintWARNINGUnknown extended key usage
x509lintINFOSubject has a deprecated CommonName
x509lintINFOUnknown validation policy
zlintERRORSubscriber Certificate: authorityInformationAccess MUST contain the HTTP URL of the Issuing CA's OSCP responder.
zlintERRORSubscriber certificate cRLDistributionPoints extension must contain the HTTP URL of the CA's CRL service
zlintERRORSubscriber Certificate: authorityInformationAccess MUST be present, with the exception of stapling.
zlintWARNINGCompliant certificates should use the utf8string encoding for explicitText
zlintWARNINGSubscriber Certificate: extKeyUsage either the value id-kp-serverAuth or id-kp-clientAuth or both values MUST be present.
zlintWARNINGSubscriber certificates authorityInformationAccess extension should contain the HTTP URL of the issuing CA's certificate
zlintNOTICESubscriber Certificate: commonName is deprecated.

cablintERRORBR certificates with organizationName must include either localityName or stateOrProvinceName
cablintWARNINGCertificate does not include authorityInformationAccess. BRs require OCSP stapling for this certificate.
cablintWARNINGDeprecated Netscape extension 2.16.840.1.113730.1.1 treated as opaque extension
cablintWARNINGTLS Server auth certificates should not contain Netscape Server Gated Crypto usage
cablintINFOTLS Server certificate identified
x509lintERRORError parsing URL
x509lintERRORno authorityInformationAccess extension
x509lintERRORNo OCSP over HTTP
x509lintERRORSubject with organizationName, givenName or surname but without stateOrProvince or localityName
x509lintWARNINGexplicitText is not using a UTF8String
x509lintWARNINGNo HTTP URL for issuing certificate
9981096 2015-09-22 07:03:35 2017-12-22 07:03:34 x509lintWARNINGPolicy information has qualifier other than CPS URI
x509lintWARNINGUnknown extended key usage
x509lintINFOSubject has a deprecated CommonName
x509lintINFOUnknown validation policy
zlintERRORSubscriber Certificate: authorityInformationAccess MUST contain the HTTP URL of the Issuing CA's OSCP responder.
zlintERRORSubscriber certificate cRLDistributionPoints extension must contain the HTTP URL of the CA's CRL service
zlintERRORSubscriber Certificate: authorityInformationAccess MUST be present, with the exception of stapling.
zlintWARNINGCompliant certificates should use the utf8string encoding for explicitText
zlintWARNINGSubscriber Certificate: extKeyUsage either the value id-kp-serverAuth or id-kp-clientAuth or both values MUST be present.
zlintWARNINGSubscriber certificates authorityInformationAccess extension should contain the HTTP URL of the issuing CA's certificate
zlintNOTICESubscriber Certificate: commonName is deprecated.

cablintERRORBR certificates with organizationName must include either localityName or stateOrProvinceName
cablintWARNINGCertificate does not include authorityInformationAccess. BRs require OCSP stapling for this certificate.
cablintWARNINGDeprecated Netscape extension 2.16.840.1.113730.1.1 treated as opaque extension
cablintWARNINGTLS Server auth certificates should not contain Netscape Server Gated Crypto usage
cablintINFOTLS Server certificate identified
x509lintERRORError parsing URL
x509lintERRORno authorityInformationAccess extension
x509lintERRORNo OCSP over HTTP
x509lintERRORSubject with organizationName, givenName or surname but without stateOrProvince or localityName
x509lintWARNINGexplicitText is not using a UTF8String
x509lintWARNINGNo HTTP URL for issuing certificate
10383573 2015-10-15 23:52:09 2018-01-15 23:52:08 x509lintWARNINGPolicy information has qualifier other than CPS URI
x509lintWARNINGUnknown extended key usage
x509lintINFOSubject has a deprecated CommonName
x509lintINFOUnknown validation policy
zlintERRORSubscriber Certificate: authorityInformationAccess MUST contain the HTTP URL of the Issuing CA's OSCP responder.
zlintERRORSubscriber certificate cRLDistributionPoints extension must contain the HTTP URL of the CA's CRL service
zlintERRORSubscriber Certificate: authorityInformationAccess MUST be present, with the exception of stapling.
zlintWARNINGCompliant certificates should use the utf8string encoding for explicitText
zlintWARNINGSubscriber Certificate: extKeyUsage either the value id-kp-serverAuth or id-kp-clientAuth or both values MUST be present.
zlintWARNINGSubscriber certificates authorityInformationAccess extension should contain the HTTP URL of the issuing CA's certificate
zlintNOTICESubscriber Certificate: commonName is deprecated.

cablintERRORBR certificates with organizationName must include either localityName or stateOrProvinceName
cablintWARNINGCertificate does not include authorityInformationAccess. BRs require OCSP stapling for this certificate.
cablintWARNINGDeprecated Netscape extension 2.16.840.1.113730.1.1 treated as opaque extension
cablintWARNINGTLS Server auth certificates should not contain Netscape Server Gated Crypto usage
cablintINFOTLS Server certificate identified
x509lintERRORError parsing URL
x509lintERRORno authorityInformationAccess extension
x509lintERRORNo OCSP over HTTP
x509lintERRORSubject with organizationName, givenName or surname but without stateOrProvince or localityName
x509lintWARNINGexplicitText is not using a UTF8String
x509lintWARNINGNo HTTP URL for issuing certificate
287860086 2015-10-06 06:24:02 2018-01-06 06:24:01 x509lintWARNINGPolicy information has qualifier other than CPS URI
x509lintWARNINGUnknown extended key usage
x509lintINFOSubject has a deprecated CommonName
x509lintINFOUnknown validation policy
zlintERRORSubscriber Certificate: authorityInformationAccess MUST contain the HTTP URL of the Issuing CA's OSCP responder.
zlintERRORSubscriber certificate cRLDistributionPoints extension must contain the HTTP URL of the CA's CRL service
zlintERRORSubscriber Certificate: authorityInformationAccess MUST be present, with the exception of stapling.
zlintWARNINGCompliant certificates should use the utf8string encoding for explicitText
zlintWARNINGSubscriber Certificate: extKeyUsage either the value id-kp-serverAuth or id-kp-clientAuth or both values MUST be present.
zlintWARNINGSubscriber certificates authorityInformationAccess extension should contain the HTTP URL of the issuing CA's certificate
zlintNOTICESubscriber Certificate: commonName is deprecated.

cablintERRORBR certificates with organizationName must include either localityName or stateOrProvinceName
cablintWARNINGCertificate does not include authorityInformationAccess. BRs require OCSP stapling for this certificate.
cablintWARNINGDeprecated Netscape extension 2.16.840.1.113730.1.1 treated as opaque extension
cablintWARNINGTLS Server auth certificates should not contain Netscape Server Gated Crypto usage
cablintINFOTLS Server certificate identified
x509lintERRORError parsing URL
x509lintERRORno authorityInformationAccess extension
x509lintERRORNo OCSP over HTTP
x509lintERRORSubject with organizationName, givenName or surname but without stateOrProvince or localityName
x509lintWARNINGexplicitText is not using a UTF8String
x509lintWARNINGNo HTTP URL for issuing certificate
287865131 2015-10-01 04:31:07 2018-01-01 04:31:06 x509lintWARNINGPolicy information has qualifier other than CPS URI
x509lintWARNINGUnknown extended key usage
x509lintINFOSubject has a deprecated CommonName
x509lintINFOUnknown validation policy
zlintERRORSubscriber Certificate: authorityInformationAccess MUST contain the HTTP URL of the Issuing CA's OSCP responder.
zlintERRORSubscriber certificate cRLDistributionPoints extension must contain the HTTP URL of the CA's CRL service
zlintERRORSubscriber Certificate: authorityInformationAccess MUST be present, with the exception of stapling.
zlintWARNINGCompliant certificates should use the utf8string encoding for explicitText
zlintWARNINGSubscriber Certificate: extKeyUsage either the value id-kp-serverAuth or id-kp-clientAuth or both values MUST be present.
zlintWARNINGSubscriber certificates authorityInformationAccess extension should contain the HTTP URL of the issuing CA's certificate
zlintNOTICESubscriber Certificate: commonName is deprecated.

cablintERRORBR certificates with organizationName must include either localityName or stateOrProvinceName
cablintWARNINGCertificate does not include authorityInformationAccess. BRs require OCSP stapling for this certificate.
cablintWARNINGDeprecated Netscape extension 2.16.840.1.113730.1.1 treated as opaque extension
cablintWARNINGTLS Server auth certificates should not contain Netscape Server Gated Crypto usage
cablintINFOTLS Server certificate identified
x509lintERRORError parsing URL
x509lintERRORno authorityInformationAccess extension
x509lintERRORNo OCSP over HTTP
x509lintERRORSubject with organizationName, givenName or surname but without stateOrProvince or localityName
x509lintWARNINGexplicitText is not using a UTF8String
x509lintWARNINGNo HTTP URL for issuing certificate
9342113 2015-09-14 06:41:27 2017-12-14 06:41:26 x509lintWARNINGPolicy information has qualifier other than CPS URI
x509lintWARNINGUnknown extended key usage
x509lintINFOSubject has a deprecated CommonName
x509lintINFOUnknown validation policy
zlintERRORSubscriber Certificate: authorityInformationAccess MUST contain the HTTP URL of the Issuing CA's OSCP responder.
zlintERRORSubscriber certificate cRLDistributionPoints extension must contain the HTTP URL of the CA's CRL service
zlintERRORSubscriber Certificate: authorityInformationAccess MUST be present, with the exception of stapling.
zlintWARNINGCompliant certificates should use the utf8string encoding for explicitText
zlintWARNINGSubscriber Certificate: extKeyUsage either the value id-kp-serverAuth or id-kp-clientAuth or both values MUST be present.
zlintWARNINGSubscriber certificates authorityInformationAccess extension should contain the HTTP URL of the issuing CA's certificate
zlintNOTICESubscriber Certificate: commonName is deprecated.

cablintERRORBR certificates with organizationName must include either localityName or stateOrProvinceName
cablintWARNINGCertificate does not include authorityInformationAccess. BRs require OCSP stapling for this certificate.
cablintWARNINGDeprecated Netscape extension 2.16.840.1.113730.1.1 treated as opaque extension
cablintWARNINGTLS Server auth certificates should not contain Netscape Server Gated Crypto usage
cablintINFOTLS Server certificate identified
x509lintERRORError parsing URL
x509lintERRORno authorityInformationAccess extension
x509lintERRORNo OCSP over HTTP
x509lintERRORSubject with organizationName, givenName or surname but without stateOrProvince or localityName
x509lintWARNINGexplicitText is not using a UTF8String
x509lintWARNINGNo HTTP URL for issuing certificate
22475941 2015-11-12 05:15:11 2018-02-12 05:15:10 x509lintWARNINGPolicy information has qualifier other than CPS URI
x509lintWARNINGUnknown extended key usage
x509lintINFOSubject has a deprecated CommonName
x509lintINFOUnknown validation policy
zlintERRORSubscriber Certificate: authorityInformationAccess MUST contain the HTTP URL of the Issuing CA's OSCP responder.
zlintERRORSubscriber certificate cRLDistributionPoints extension must contain the HTTP URL of the CA's CRL service
zlintERRORSubscriber Certificate: authorityInformationAccess MUST be present, with the exception of stapling.
zlintWARNINGCompliant certificates should use the utf8string encoding for explicitText
zlintWARNINGSubscriber Certificate: extKeyUsage either the value id-kp-serverAuth or id-kp-clientAuth or both values MUST be present.
zlintWARNINGSubscriber certificates authorityInformationAccess extension should contain the HTTP URL of the issuing CA's certificate
zlintNOTICESubscriber Certificate: commonName is deprecated.

cablintERRORBR certificates with organizationName must include either localityName or stateOrProvinceName
cablintWARNINGCertificate does not include authorityInformationAccess. BRs require OCSP stapling for this certificate.
cablintWARNINGDeprecated Netscape extension 2.16.840.1.113730.1.1 treated as opaque extension
cablintWARNINGTLS Server auth certificates should not contain Netscape Server Gated Crypto usage
cablintINFOTLS Server certificate identified
x509lintERRORError parsing URL
x509lintERRORno authorityInformationAccess extension
x509lintERRORNo OCSP over HTTP
x509lintERRORSubject with organizationName, givenName or surname but without stateOrProvince or localityName
x509lintWARNINGexplicitText is not using a UTF8String
x509lintWARNINGNo HTTP URL for issuing certificate
9265587 2015-09-09 02:05:54 2017-12-09 02:05:53 x509lintWARNINGPolicy information has qualifier other than CPS URI
x509lintWARNINGUnknown extended key usage
x509lintINFOSubject has a deprecated CommonName
x509lintINFOUnknown validation policy
zlintERRORSubscriber Certificate: authorityInformationAccess MUST contain the HTTP URL of the Issuing CA's OSCP responder.
zlintERRORSubscriber certificate cRLDistributionPoints extension must contain the HTTP URL of the CA's CRL service
zlintERRORSubscriber Certificate: authorityInformationAccess MUST be present, with the exception of stapling.
zlintWARNINGCompliant certificates should use the utf8string encoding for explicitText
zlintWARNINGSubscriber Certificate: extKeyUsage either the value id-kp-serverAuth or id-kp-clientAuth or both values MUST be present.
zlintWARNINGSubscriber certificates authorityInformationAccess extension should contain the HTTP URL of the issuing CA's CRL service
certificate
zlintNOTICESubscriber Certificate: commonName is deprecated.

cablintERRORBR certificates with organizationName must include either localityName or stateOrProvinceName
cablintWARNINGCertificate does not include authorityInformationAccess. BRs require OCSP stapling for this certificate.
cablintWARNINGDeprecated Netscape extension 2.16.840.1.113730.1.1 treated as opaque extension
cablintWARNINGTLS Server auth certificates should not contain Netscape Server Gated Crypto usage
cablintINFOTLS Server certificate identified
x509lintERRORError parsing URL
x509lintERRORno authorityInformationAccess extension
x509lintERRORNo OCSP over HTTP
x509lintERRORSubject with organizationName, givenName or surname but without stateOrProvince or localityName
x509lintWARNINGexplicitText is not using a UTF8String
x509lintWARNINGNo HTTP URL for issuing certificate
10794091 2015-10-27 07:30:30 2018-01-27 07:30:29 x509lintWARNINGPolicy information has qualifier other than CPS URI
x509lintWARNINGUnknown extended key usage
x509lintINFOSubject has a deprecated CommonName
x509lintINFOUnknown validation policy
zlintERRORSubscriber Certificate: authorityInformationAccess MUST contain the HTTP URL of the Issuing CA's OSCP responder.
zlintERRORSubscriber certificate cRLDistributionPoints extension must contain the HTTP URL of the CA's CRL service
zlintERRORSubscriber Certificate: authorityInformationAccess MUST be present, with the exception of stapling.
zlintWARNINGCompliant certificates should use the utf8string encoding for explicitText
zlintWARNINGSubscriber Certificate: extKeyUsage either the value id-kp-serverAuth or id-kp-clientAuth or both values MUST be present.
zlintWARNINGSubscriber certificates authorityInformationAccess extension should contain the HTTP URL of the issuing CA's certificate
zlintNOTICESubscriber Certificate: commonName is deprecated.

cablintERRORBR certificates with organizationName must include either localityName or stateOrProvinceName
cablintWARNINGCertificate does not include authorityInformationAccess. BRs require OCSP stapling for this certificate.
cablintWARNINGDeprecated Netscape extension 2.16.840.1.113730.1.1 treated as opaque extension
cablintWARNINGTLS Server auth certificates should not contain Netscape Server Gated Crypto usage
cablintINFOTLS Server certificate identified
x509lintERRORError parsing URL
x509lintERRORno authorityInformationAccess extension
x509lintERRORNo OCSP over HTTP
x509lintERRORSubject with organizationName, givenName or surname but without stateOrProvince or localityName
x509lintWARNINGexplicitText is not using a UTF8String
x509lintWARNINGNo HTTP URL for issuing certificate
10819102 2015-10-08 10:24:21 2018-01-08 10:24:20 x509lintWARNINGPolicy information has qualifier other than CPS URI
x509lintWARNINGUnknown extended key usage
x509lintINFOSubject has a deprecated CommonName
x509lintINFOUnknown validation policy
zlintERRORSubscriber Certificate: authorityInformationAccess MUST contain the HTTP URL of the Issuing CA's OSCP responder.
zlintERRORSubscriber certificate cRLDistributionPoints extension must contain the HTTP URL of the CA's CRL service
zlintERRORSubscriber Certificate: authorityInformationAccess MUST be present, with the exception of stapling.
zlintWARNINGCompliant certificates should use the utf8string encoding for explicitText
zlintWARNINGSubscriber Certificate: extKeyUsage either the value id-kp-serverAuth or id-kp-clientAuth or both values MUST be present.
zlintWARNINGSubscriber certificates authorityInformationAccess extension should contain the HTTP URL of the issuing CA's certificate
zlintNOTICESubscriber Certificate: commonName is deprecated.

cablintERRORBR certificates with organizationName must include either localityName or stateOrProvinceName
cablintWARNINGCertificate does not include authorityInformationAccess. BRs require OCSP stapling for this certificate.
cablintWARNINGDeprecated Netscape extension 2.16.840.1.113730.1.1 treated as opaque extension
cablintWARNINGTLS Server auth certificates should not contain Netscape Server Gated Crypto usage
cablintINFOTLS Server certificate identified
x509lintERRORError parsing URL
x509lintERRORno authorityInformationAccess extension
x509lintERRORNo OCSP over HTTP
x509lintERRORSubject with organizationName, givenName or surname but without stateOrProvince or localityName
x509lintWARNINGexplicitText is not using a UTF8String
x509lintWARNINGNo HTTP URL for issuing certificate
9163475 2015-09-01 03:33:35 2017-12-01 03:33:34 x509lintWARNINGPolicy information has qualifier other than CPS URI
x509lintWARNINGUnknown extended key usage
x509lintINFOSubject has a deprecated CommonName
x509lintINFOUnknown validation policy
zlintERRORSubscriber Certificate: authorityInformationAccess MUST contain the HTTP URL of the Issuing CA's OSCP responder.
zlintERRORSubscriber certificate cRLDistributionPoints extension must contain the HTTP URL of the CA's CRL service
zlintERRORSubscriber Certificate: authorityInformationAccess MUST be present, with the exception of stapling.
zlintWARNINGCompliant certificates should use the utf8string encoding for explicitText
zlintWARNINGSubscriber Certificate: extKeyUsage either the value id-kp-serverAuth or id-kp-clientAuth or both values MUST be present.
zlintWARNINGSubscriber certificates authorityInformationAccess extension should contain the HTTP URL of the issuing CA's certificate
zlintNOTICESubscriber Certificate: commonName is deprecated.

cablintERRORBR certificates with organizationName must include either localityName or stateOrProvinceName
cablintWARNINGCertificate does not include authorityInformationAccess. BRs require OCSP stapling for this certificate.
cablintWARNINGDeprecated Netscape extension 2.16.840.1.113730.1.1 treated as opaque extension
cablintWARNINGTLS Server auth certificates should not contain Netscape Server Gated Crypto usage
cablintINFOTLS Server certificate identified
x509lintERRORError parsing URL
x509lintERRORno authorityInformationAccess extension
x509lintERRORNo OCSP over HTTP
x509lintERRORSubject with organizationName, givenName or surname but without stateOrProvince or localityName
x509lintWARNINGexplicitText is not using a UTF8String
x509lintWARNINGNo HTTP URL for issuing certificate
10029294 2015-10-07 01:49:49 2018-01-07 01:49:48 x509lintWARNINGPolicy information has qualifier other than CPS URI
x509lintWARNINGUnknown extended key usage
x509lintINFOSubject has a deprecated CommonName
x509lintINFOUnknown validation policy
zlintERRORSubscriber Certificate: authorityInformationAccess MUST contain the HTTP URL of the Issuing CA's OSCP responder.
zlintERRORSubscriber certificate cRLDistributionPoints extension must contain the HTTP URL of the CA's CRL service
zlintERRORSubscriber Certificate: authorityInformationAccess MUST be present, with the exception of stapling.
zlintWARNINGCompliant certificates should use the utf8string encoding for explicitText
zlintWARNINGSubscriber Certificate: extKeyUsage either the value id-kp-serverAuth or id-kp-clientAuth or both values MUST be present.
zlintWARNINGSubscriber certificates authorityInformationAccess extension should contain the HTTP URL of the issuing CA's certificate
zlintNOTICESubscriber Certificate: commonName is deprecated.

cablintERRORBR certificates with organizationName must include either localityName or stateOrProvinceName
cablintWARNINGCertificate does not include authorityInformationAccess. BRs require OCSP stapling for this certificate.
cablintWARNINGDeprecated Netscape extension 2.16.840.1.113730.1.1 treated as opaque extension
cablintWARNINGTLS Server auth certificates should not contain Netscape Server Gated Crypto usage
cablintINFOTLS Server certificate identified
x509lintERRORError parsing URL
x509lintERRORno authorityInformationAccess extension
x509lintERRORNo OCSP over HTTP
x509lintERRORSubject with organizationName, givenName or surname but without stateOrProvince or localityName
x509lintWARNINGexplicitText is not using a UTF8String
x509lintWARNINGNo HTTP URL for issuing certificate
10192778 2015-10-14 01:04:19 2018-01-14 01:04:18 x509lintWARNINGPolicy information has qualifier other than CPS URI
x509lintWARNINGUnknown extended key usage
x509lintINFOSubject has a deprecated CommonName
x509lintINFOUnknown validation policy
zlintERRORSubscriber Certificate: authorityInformationAccess MUST contain the HTTP URL of the Issuing CA's OSCP responder.
zlintERRORSubscriber certificate cRLDistributionPoints extension must contain the HTTP URL of the CA's CRL service
zlintERRORSubscriber Certificate: authorityInformationAccess MUST be present, with the exception of stapling.
zlintWARNINGCompliant certificates should use the utf8string encoding for explicitText
zlintWARNINGSubscriber Certificate: extKeyUsage either the value id-kp-serverAuth or id-kp-clientAuth or both values MUST be present.
zlintWARNINGSubscriber certificates authorityInformationAccess extension should contain the HTTP URL of the issuing CA's certificate
zlintNOTICESubscriber Certificate: commonName is deprecated.

cablintERRORBR certificates with organizationName must include either localityName or stateOrProvinceName
cablintWARNINGCertificate does not include authorityInformationAccess. BRs require OCSP stapling for this certificate.
cablintWARNINGDeprecated Netscape extension 2.16.840.1.113730.1.1 treated as opaque extension
cablintWARNINGTLS Server auth certificates should not contain Netscape Server Gated Crypto usage
cablintINFOTLS Server certificate identified
x509lintERRORError parsing URL
x509lintERRORno authorityInformationAccess extension
x509lintERRORNo OCSP over HTTP
x509lintERRORSubject with organizationName, givenName or surname but without stateOrProvince or localityName
x509lintWARNINGexplicitText is not using a UTF8String
x509lintWARNINGNo HTTP URL for issuing certificate
10787275 2015-11-18 05:50:58 2018-02-18 05:50:57 x509lintWARNINGPolicy information has qualifier other than CPS URI
x509lintWARNINGUnknown extended key usage
x509lintINFOSubject has a deprecated CommonName
x509lintINFOUnknown validation policy
zlintERRORSubscriber Certificate: authorityInformationAccess MUST contain the HTTP URL of the Issuing CA's OSCP responder.
zlintERRORSubscriber certificate cRLDistributionPoints extension must contain the HTTP URL of the CA's CRL service
zlintERRORSubscriber Certificate: authorityInformationAccess MUST be present, with the exception of stapling.
zlintWARNINGCompliant certificates should use the utf8string encoding for explicitText
zlintWARNINGSubscriber Certificate: extKeyUsage either the value id-kp-serverAuth or id-kp-clientAuth or both values MUST be present.
zlintWARNINGSubscriber certificates authorityInformationAccess extension should contain the HTTP URL of the issuing CA's certificate
zlintNOTICESubscriber Certificate: commonName is deprecated.

cablintERRORBR certificates with organizationName must include either localityName or stateOrProvinceName
cablintWARNINGCertificate does not include authorityInformationAccess. BRs require OCSP stapling for this certificate.
cablintWARNINGDeprecated Netscape extension 2.16.840.1.113730.1.1 treated as opaque extension
cablintWARNINGTLS Server auth certificates should not contain Netscape Server Gated Crypto usage
cablintINFOTLS Server certificate identified
x509lintERRORError parsing URL
x509lintERRORno authorityInformationAccess extension
x509lintERRORNo OCSP over HTTP
x509lintERRORSubject with organizationName, givenName or surname but without stateOrProvince or localityName
x509lintWARNINGexplicitText is not using a UTF8String
x509lintWARNINGNo HTTP URL for issuing certificate
97713427 2015-10-06 14:18:00 2018-01-06 14:17:59 x509lintWARNINGPolicy information has qualifier other than CPS URI
x509lintWARNINGUnknown extended key usage
x509lintINFOSubject has a deprecated CommonName
x509lintINFOUnknown validation policy
zlintERRORSubscriber Certificate: authorityInformationAccess MUST contain the HTTP URL of the Issuing CA's OSCP responder.
zlintERRORSubscriber certificate cRLDistributionPoints extension must contain the HTTP URL of the CA's CRL service
zlintERRORSubscriber Certificate: authorityInformationAccess MUST be present, with the exception of stapling.
zlintWARNINGCompliant certificates should use the utf8string encoding for explicitText
zlintWARNINGSubscriber Certificate: extKeyUsage either the value id-kp-serverAuth or id-kp-clientAuth or both values MUST be present.
zlintWARNINGSubscriber certificates authorityInformationAccess extension should contain the HTTP URL of the issuing CA's certificate
zlintNOTICESubscriber Certificate: commonName is deprecated.

cablintERRORBR certificates with organizationName must include either localityName or stateOrProvinceName
cablintWARNINGCertificate does not include authorityInformationAccess. BRs require OCSP stapling for this certificate.
cablintWARNINGDeprecated Netscape extension 2.16.840.1.113730.1.1 treated as opaque extension
cablintWARNINGTLS Server auth certificates should not contain Netscape Server Gated Crypto usage
cablintINFOTLS Server certificate identified
x509lintERRORError parsing URL
x509lintERRORno authorityInformationAccess extension
x509lintERRORNo OCSP over HTTP
x509lintERRORSubject with organizationName, givenName or surname but without stateOrProvince or localityName
x509lintWARNINGexplicitText is not using a UTF8String
x509lintWARNINGNo HTTP URL for issuing certificate
11082372 2015-11-02 07:18:30 2018-02-02 07:18:29 x509lintWARNINGPolicy information has qualifier other than CPS URI
x509lintWARNINGUnknown extended key usage
x509lintINFOSubject has a deprecated CommonName
x509lintINFOUnknown validation policy
zlintERRORSubscriber Certificate: authorityInformationAccess MUST contain the HTTP URL of the Issuing CA's OSCP responder.
zlintERRORSubscriber certificate cRLDistributionPoints extension must contain the HTTP URL of the CA's CRL service
zlintERRORSubscriber Certificate: authorityInformationAccess MUST be present, with the exception of stapling.
zlintWARNINGCompliant certificates should use the utf8string encoding for explicitText
zlintWARNINGSubscriber Certificate: extKeyUsage either the value id-kp-serverAuth or id-kp-clientAuth or both values MUST be present.
zlintWARNINGSubscriber certificates authorityInformationAccess extension should contain the HTTP URL of the issuing CA's certificate
zlintNOTICESubscriber Certificate: commonName is deprecated.

cablintERRORBR certificates with organizationName must include either localityName or stateOrProvinceName
cablintWARNINGCertificate does not include authorityInformationAccess. BRs require OCSP stapling for this certificate.
cablintWARNINGDeprecated Netscape extension 2.16.840.1.113730.1.1 treated as opaque extension
cablintWARNINGTLS Server auth certificates should not contain Netscape Server Gated Crypto usage
cablintINFOTLS Server certificate identified
x509lintERRORError parsing URL
x509lintERRORno authorityInformationAccess extension
x509lintERRORNo OCSP over HTTP
x509lintERRORSubject with organizationName, givenName or surname but without stateOrProvince or localityName
x509lintWARNINGexplicitText is not using a UTF8String
x509lintWARNINGNo HTTP URL for issuing certificate
28517784 2015-09-30 00:29:15 2017-12-30 00:29:14 x509lintWARNINGPolicy information has qualifier other than CPS URI
x509lintWARNINGUnknown extended key usage
x509lintINFOSubject has a deprecated CommonName
x509lintINFOUnknown validation policy
zlintERRORSubscriber Certificate: authorityInformationAccess MUST contain the HTTP URL of the Issuing CA's OSCP responder.
zlintERRORSubscriber certificate cRLDistributionPoints extension must contain the HTTP URL of the CA's CRL service
zlintERRORSubscriber Certificate: authorityInformationAccess MUST be present, with the exception of stapling.
zlintWARNINGCompliant certificates should use the utf8string encoding for explicitText
zlintWARNINGSubscriber Certificate: extKeyUsage either the value id-kp-serverAuth or id-kp-clientAuth or both values MUST be present.
zlintWARNINGSubscriber certificates authorityInformationAccess extension should contain the HTTP URL of the issuing CA's CRL service
certificate
zlintNOTICESubscriber Certificate: commonName is deprecated.

cablintERRORBR certificates with organizationName must include either localityName or stateOrProvinceName
cablintWARNINGCertificate does not include authorityInformationAccess. BRs require OCSP stapling for this certificate.
cablintWARNINGDeprecated Netscape extension 2.16.840.1.113730.1.1 treated as opaque extension
cablintWARNINGTLS Server auth certificates should not contain Netscape Server Gated Crypto usage
cablintINFOTLS Server certificate identified
x509lintERRORError parsing URL
x509lintERRORno authorityInformationAccess extension
x509lintERRORNo OCSP over HTTP
x509lintERRORSubject with organizationName, givenName or surname but without stateOrProvince or localityName
x509lintWARNINGexplicitText is not using a UTF8String
x509lintWARNINGNo HTTP URL for issuing certificate
10218268 2015-10-15 05:03:51 2018-01-15 05:03:50 x509lintWARNINGPolicy information has qualifier other than CPS URI
x509lintWARNINGUnknown extended key usage
x509lintINFOSubject has a deprecated CommonName
x509lintINFOUnknown validation policy
zlintERRORSubscriber Certificate: authorityInformationAccess MUST contain the HTTP URL of the Issuing CA's OSCP responder.
zlintERRORSubscriber certificate cRLDistributionPoints extension must contain the HTTP URL of the CA's CRL service
zlintERRORSubscriber Certificate: authorityInformationAccess MUST be present, with the exception of stapling.
zlintWARNINGCompliant certificates should use the utf8string encoding for explicitText
zlintWARNINGSubscriber Certificate: extKeyUsage either the value id-kp-serverAuth or id-kp-clientAuth or both values MUST be present.
zlintWARNINGSubscriber certificates authorityInformationAccess extension should contain the HTTP URL of the issuing CA's certificate
zlintNOTICESubscriber Certificate: commonName is deprecated.

cablintERRORBR certificates with organizationName must include either localityName or stateOrProvinceName
cablintWARNINGCertificate does not include authorityInformationAccess. BRs require OCSP stapling for this certificate.
cablintWARNINGDeprecated Netscape extension 2.16.840.1.113730.1.1 treated as opaque extension
cablintWARNINGTLS Server auth certificates should not contain Netscape Server Gated Crypto usage
cablintINFOTLS Server certificate identified
x509lintERRORError parsing URL
x509lintERRORno authorityInformationAccess extension
x509lintERRORNo OCSP over HTTP
x509lintERRORSubject with organizationName, givenName or surname but without stateOrProvince or localityName
x509lintWARNINGexplicitText is not using a UTF8String
x509lintWARNINGNo HTTP URL for issuing certificate
9181150 2015-09-04 00:39:09 2017-12-04 00:39:08 x509lintWARNINGPolicy information has qualifier other than CPS URI
x509lintWARNINGUnknown extended key usage
x509lintINFOSubject has a deprecated CommonName
x509lintINFOUnknown validation policy
zlintERRORSubscriber Certificate: authorityInformationAccess MUST contain the HTTP URL of the Issuing CA's OSCP responder.
zlintERRORSubscriber certificate cRLDistributionPoints extension must contain the HTTP URL of the CA's CRL service
zlintERRORSubscriber Certificate: authorityInformationAccess MUST be present, with the exception of stapling.
zlintWARNINGCompliant certificates should use the utf8string encoding for explicitText
zlintWARNINGSubscriber Certificate: extKeyUsage either the value id-kp-serverAuth or id-kp-clientAuth or both values MUST be present.
zlintWARNINGSubscriber certificates authorityInformationAccess extension should contain the HTTP URL of the issuing CA's certificate
zlintNOTICESubscriber Certificate: commonName is deprecated.

cablintERRORBR certificates with organizationName must include either localityName or stateOrProvinceName
cablintWARNINGCertificate does not include authorityInformationAccess. BRs require OCSP stapling for this certificate.
cablintWARNINGDeprecated Netscape extension 2.16.840.1.113730.1.1 treated as opaque extension
cablintWARNINGTLS Server auth certificates should not contain Netscape Server Gated Crypto usage
cablintINFOTLS Server certificate identified
x509lintERRORError parsing URL
x509lintERRORno authorityInformationAccess extension
x509lintERRORNo OCSP over HTTP
x509lintERRORSubject with organizationName, givenName or surname but without stateOrProvince or localityName
x509lintWARNINGexplicitText is not using a UTF8String
x509lintWARNINGNo HTTP URL for issuing certificate
9364042 2015-09-15 10:17:56 2017-12-15 10:17:55 x509lintWARNINGPolicy information has qualifier other than CPS URI
x509lintWARNINGUnknown extended key usage
x509lintINFOSubject has a deprecated CommonName
x509lintINFOUnknown validation policy
zlintERRORSubscriber Certificate: authorityInformationAccess MUST contain the HTTP URL of the Issuing CA's OSCP responder.
zlintERRORSubscriber certificate cRLDistributionPoints extension must contain the HTTP URL of the CA's CRL service
zlintERRORSubscriber Certificate: authorityInformationAccess MUST be present, with the exception of stapling.
zlintWARNINGCompliant certificates should use the utf8string encoding for explicitText
zlintWARNINGSubscriber Certificate: extKeyUsage either the value id-kp-serverAuth or id-kp-clientAuth or both values MUST be present.
zlintWARNINGSubscriber certificates authorityInformationAccess extension should contain the HTTP URL of the issuing CA's certificate
zlintNOTICESubscriber Certificate: commonName is deprecated.

cablintERRORBR certificates with organizationName must include either localityName or stateOrProvinceName
cablintWARNINGCertificate does not include authorityInformationAccess. BRs require OCSP stapling for this certificate.
cablintWARNINGDeprecated Netscape extension 2.16.840.1.113730.1.1 treated as opaque extension
cablintWARNINGTLS Server auth certificates should not contain Netscape Server Gated Crypto usage
cablintINFOTLS Server certificate identified
x509lintERRORError parsing URL
x509lintERRORno authorityInformationAccess extension
x509lintERRORNo OCSP over HTTP
x509lintERRORSubject with organizationName, givenName or surname but without stateOrProvince or localityName
x509lintWARNINGexplicitText is not using a UTF8String
x509lintWARNINGNo HTTP URL for issuing certificate
9998246 2015-10-05 07:15:14 2018-01-05 07:15:13 x509lintWARNINGPolicy information has qualifier other than CPS URI
x509lintWARNINGUnknown extended key usage
x509lintINFOSubject has a deprecated CommonName
x509lintINFOUnknown validation policy
zlintERRORSubscriber Certificate: authorityInformationAccess MUST contain the HTTP URL of the Issuing CA's OSCP responder.
zlintERRORSubscriber certificate cRLDistributionPoints extension must contain the HTTP URL of the CA's CRL service
zlintERRORSubscriber Certificate: authorityInformationAccess MUST be present, with the exception of stapling.
zlintWARNINGCompliant certificates should use the utf8string encoding for explicitText
zlintWARNINGSubscriber Certificate: extKeyUsage either the value id-kp-serverAuth or id-kp-clientAuth or both values MUST be present.
zlintWARNINGSubscriber certificates authorityInformationAccess extension should contain the HTTP URL of the issuing CA's certificate
zlintNOTICESubscriber Certificate: commonName is deprecated.

cablintERRORBR certificates with organizationName must include either localityName or stateOrProvinceName
cablintWARNINGCertificate does not include authorityInformationAccess. BRs require OCSP stapling for this certificate.
cablintWARNINGDeprecated Netscape extension 2.16.840.1.113730.1.1 treated as opaque extension
cablintWARNINGTLS Server auth certificates should not contain Netscape Server Gated Crypto usage
cablintINFOTLS Server certificate identified
x509lintERRORError parsing URL
x509lintERRORno authorityInformationAccess extension
x509lintERRORNo OCSP over HTTP
x509lintERRORSubject with organizationName, givenName or surname but without stateOrProvince or localityName
x509lintWARNINGexplicitText is not using a UTF8String
x509lintWARNINGNo HTTP URL for issuing certificate
9351543 2015-09-15 05:17:34 2017-12-15 05:17:33 x509lintWARNINGPolicy information has qualifier other than CPS URI
x509lintWARNINGUnknown extended key usage
x509lintINFOSubject has a deprecated CommonName
x509lintINFOUnknown validation policy
zlintERRORSubscriber Certificate: authorityInformationAccess MUST contain the HTTP URL of the Issuing CA's OSCP responder.
zlintERRORSubscriber certificate cRLDistributionPoints extension must contain the HTTP URL of the CA's CRL service
zlintERRORSubscriber Certificate: authorityInformationAccess MUST be present, with the exception of stapling.
zlintWARNINGCompliant certificates should use the utf8string encoding for explicitText
zlintWARNINGSubscriber Certificate: extKeyUsage either the value id-kp-serverAuth or id-kp-clientAuth or both values MUST be present.
zlintWARNINGSubscriber certificates authorityInformationAccess extension should contain the HTTP URL of the issuing CA's certificate
zlintNOTICESubscriber Certificate: commonName is deprecated.

cablintERRORBR certificates with organizationName must include either localityName or stateOrProvinceName
cablintWARNINGCertificate does not include authorityInformationAccess. BRs require OCSP stapling for this certificate.
cablintWARNINGDeprecated Netscape extension 2.16.840.1.113730.1.1 treated as opaque extension
cablintWARNINGTLS Server auth certificates should not contain Netscape Server Gated Crypto usage
cablintINFOTLS Server certificate identified
x509lintERRORError parsing URL
x509lintERRORno authorityInformationAccess extension
x509lintERRORNo OCSP over HTTP
x509lintERRORSubject with organizationName, givenName or surname but without stateOrProvince or localityName
x509lintWARNINGexplicitText is not using a UTF8String
x509lintWARNINGNo HTTP URL for issuing certificate
10200172 2015-10-15 08:26:34 2018-01-15 08:26:33 x509lintWARNINGPolicy information has qualifier other than CPS URI
x509lintWARNINGUnknown extended key usage
x509lintINFOSubject has a deprecated CommonName
x509lintINFOUnknown validation policy
zlintERRORSubscriber Certificate: authorityInformationAccess MUST contain the HTTP URL of the Issuing CA's OSCP responder.
zlintERRORSubscriber certificate cRLDistributionPoints extension must contain the HTTP URL of the CA's CRL service
zlintERRORSubscriber Certificate: authorityInformationAccess MUST be present, with the exception of stapling.
zlintWARNINGCompliant certificates should use the utf8string encoding for explicitText
zlintWARNINGSubscriber Certificate: extKeyUsage either the value id-kp-serverAuth or id-kp-clientAuth or both values MUST be present.
zlintWARNINGSubscriber certificates authorityInformationAccess extension should contain the HTTP URL of the issuing CA's certificate
zlintNOTICESubscriber Certificate: commonName is deprecated.

cablintERRORBR certificates must have subject alternative names extension
cablintERRORBR certificates with CRL Distribution Point must include HTTP URL
cablintERRORBR certificates with organizationName must include either localityName or stateOrProvinceName
cablintERRORcommonNames in BR certificates must be from SAN entries
cablintWARNINGCertificate does not include authorityInformationAccess. BRs require OCSP stapling for this certificate.
cablintWARNINGDeprecated Netscape extension 2.16.840.1.113730.1.1 treated as opaque extension
cablintWARNINGTLS Server auth certificates should not contain Netscape Server Gated Crypto usage
cablintINFOTLS Server certificate identified

x509lintERRORError parsing URL

x509lintERRORno authorityInformationAccess extension

x509lintERRORNo OCSP over HTTP

x509lintERRORNo Subject alternative name extension

9709628 2015-09-02 06:37:54 2017-12-02 06:37:53 x509lintERRORSubject with organizationName, givenName or surname but without stateOrProvince or localityName

x509lintWARNINGexplicitText is not using a UTF8String

x509lintWARNINGNo HTTP URL for issuing certificate

x509lintWARNINGPolicy information has qualifier other than CPS URI

x509lintWARNINGUnknown extended key usage

x509lintINFOSubject has a deprecated CommonName

x509lintINFOUnknown validation policy

zlintERRORCharacters in labels of DNSNames MUST be alphanumeric, -, _ or *

zlintERRORSubscriber Certificate: authorityInformationAccess MUST contain the HTTP URL of the Issuing CA's OSCP responder.

zlintERRORSubscriber certificate cRLDistributionPoints extension must contain the HTTP URL of the CA's CRL service

zlintERRORSubscriber certificates MUST contain the Subject Alternate Name extension

zlintERRORSubscriber Certificate: authorityInformationAccess MUST be present, with the exception of stapling.

zlintERRORThe common name field in subscriber certificates must include only names from the SAN extension

cablintERRORBR certificates with organizationName must include either localityName or stateOrProvinceName
cablintWARNINGCertificate does not include authorityInformationAccess. BRs require OCSP stapling for this certificate.
cablintWARNINGDeprecated Netscape extension 2.16.840.1.113730.1.1 treated as opaque extension
cablintWARNINGTLS Server auth certificates should not contain Netscape Server Gated Crypto usage
cablintINFOTLS Server certificate identified
x509lintERRORError parsing URL
x509lintERRORno authorityInformationAccess extension
x509lintERRORNo OCSP over HTTP
x509lintERRORSubject with organizationName, givenName or surname but without stateOrProvince or localityName
x509lintWARNINGexplicitText is not using a UTF8String
x509lintWARNINGNo HTTP URL for issuing certificate
10318099 2015-10-22 10:32:38 2018-01-22 10:32:37 x509lintWARNINGPolicy information has qualifier other than CPS URI
x509lintWARNINGUnknown extended key usage
x509lintINFOSubject has a deprecated CommonName
x509lintINFOUnknown validation policy
zlintERRORSubscriber Certificate: authorityInformationAccess MUST contain the HTTP URL of the Issuing CA's OSCP responder.
zlintERRORSubscriber certificate cRLDistributionPoints extension must contain the HTTP URL of the CA's CRL service
zlintERRORSubscriber Certificate: authorityInformationAccess MUST be present, with the exception of stapling.
zlintWARNINGCompliant certificates should use the utf8string encoding for explicitText
zlintWARNINGSubscriber Certificate: extKeyUsage either the value id-kp-serverAuth or id-kp-clientAuth or both values MUST be present.
zlintWARNINGSubscriber certificates authorityInformationAccess extension should contain the HTTP URL of the issuing CA's certificate
zlintNOTICESubscriber Certificate: commonName is deprecated.

cablintERRORBR certificates with organizationName must include either localityName or stateOrProvinceName
cablintWARNINGCertificate does not include authorityInformationAccess. BRs require OCSP stapling for this certificate.
cablintWARNINGDeprecated Netscape extension 2.16.840.1.113730.1.1 treated as opaque extension
cablintWARNINGTLS Server auth certificates should not contain Netscape Server Gated Crypto usage
cablintINFOTLS Server certificate identified
x509lintERRORError parsing URL
x509lintERRORno authorityInformationAccess extension
x509lintERRORNo OCSP over HTTP
x509lintERRORSubject with organizationName, givenName or surname but without stateOrProvince or localityName
x509lintWARNINGexplicitText is not using a UTF8String
x509lintWARNINGNo HTTP URL for issuing certificate
289950315 2015-09-03 08:42:33 2017-12-03 08:42:32 x509lintWARNINGPolicy information has qualifier other than CPS URI
x509lintWARNINGUnknown extended key usage
x509lintINFOSubject has a deprecated CommonName
x509lintINFOUnknown validation policy
zlintERRORSubscriber Certificate: authorityInformationAccess MUST contain the HTTP URL of the Issuing CA's OSCP responder.
zlintERRORSubscriber certificate cRLDistributionPoints extension must contain the HTTP URL of the CA's CRL service
zlintERRORSubscriber Certificate: authorityInformationAccess MUST be present, with the exception of stapling.
zlintWARNINGCompliant certificates should use the utf8string encoding for explicitText
zlintWARNINGSubscriber Certificate: extKeyUsage either the value id-kp-serverAuth or id-kp-clientAuth or both values MUST be present.
zlintWARNINGSubscriber certificates authorityInformationAccess extension should contain the HTTP URL of the issuing CA's certificate
zlintNOTICESubscriber Certificate: commonName is deprecated.

cablintERRORBR certificates with organizationName must include either localityName or stateOrProvinceName
cablintWARNINGCertificate does not include authorityInformationAccess. BRs require OCSP stapling for this certificate.
cablintWARNINGDeprecated Netscape extension 2.16.840.1.113730.1.1 treated as opaque extension
cablintWARNINGTLS Server auth certificates should not contain Netscape Server Gated Crypto usage
cablintINFOTLS Server certificate identified
x509lintERRORError parsing URL
x509lintERRORno authorityInformationAccess extension
x509lintERRORNo OCSP over HTTP
x509lintERRORSubject with organizationName, givenName or surname but without stateOrProvince or localityName
x509lintWARNINGexplicitText is not using a UTF8String
x509lintWARNINGNo HTTP URL for issuing certificate
9872608 2015-09-15 02:01:00 2017-12-15 02:00:59 x509lintWARNINGPolicy information has qualifier other than CPS URI
x509lintWARNINGUnknown extended key usage
x509lintINFOSubject has a deprecated CommonName
x509lintINFOUnknown validation policy
zlintERRORSubscriber Certificate: authorityInformationAccess MUST contain the HTTP URL of the Issuing CA's OSCP responder.
zlintERRORSubscriber certificate cRLDistributionPoints extension must contain the HTTP URL of the CA's CRL service
zlintERRORSubscriber Certificate: authorityInformationAccess MUST be present, with the exception of stapling.
zlintWARNINGCompliant certificates should use the utf8string encoding for explicitText
zlintWARNINGSubscriber Certificate: extKeyUsage either the value id-kp-serverAuth or id-kp-clientAuth or both values MUST be present.
zlintWARNINGSubscriber certificates authorityInformationAccess extension should contain the HTTP URL of the issuing CA's certificate
zlintNOTICESubscriber Certificate: commonName is deprecated.

cablintERRORBR certificates with organizationName must include either localityName or stateOrProvinceName
cablintWARNINGCertificate does not include authorityInformationAccess. BRs require OCSP stapling for this certificate.
cablintWARNINGDeprecated Netscape extension 2.16.840.1.113730.1.1 treated as opaque extension
cablintWARNINGTLS Server auth certificates should not contain Netscape Server Gated Crypto usage
cablintINFOTLS Server certificate identified
x509lintERRORError parsing URL
x509lintERRORno authorityInformationAccess extension
x509lintERRORNo OCSP over HTTP
x509lintERRORSubject with organizationName, givenName or surname but without stateOrProvince or localityName
x509lintWARNINGexplicitText is not using a UTF8String
x509lintWARNINGNo HTTP URL for issuing certificate
287853733 2015-10-22 01:04:21 2018-01-22 01:04:20 x509lintWARNINGPolicy information has qualifier other than CPS URI
x509lintWARNINGUnknown extended key usage
x509lintINFOSubject has a deprecated CommonName
x509lintINFOUnknown validation policy
zlintERRORSubscriber Certificate: authorityInformationAccess MUST contain the HTTP URL of the Issuing CA's OSCP responder.
zlintERRORSubscriber certificate cRLDistributionPoints extension must contain the HTTP URL of the CA's CRL service
zlintERRORSubscriber Certificate: authorityInformationAccess MUST be present, with the exception of stapling.
zlintWARNINGCompliant certificates should use the utf8string encoding for explicitText
zlintWARNINGSubscriber Certificate: extKeyUsage either the value id-kp-serverAuth or id-kp-clientAuth or both values MUST be present.
zlintWARNINGSubscriber certificates authorityInformationAccess extension should contain the HTTP URL of the issuing CA's certificate
zlintNOTICESubscriber Certificate: commonName is deprecated.

cablintERRORBR certificates with organizationName must include either localityName or stateOrProvinceName
cablintWARNINGCertificate does not include authorityInformationAccess. BRs require OCSP stapling for this certificate.
cablintWARNINGDeprecated Netscape extension 2.16.840.1.113730.1.1 treated as opaque extension
cablintWARNINGTLS Server auth certificates should not contain Netscape Server Gated Crypto usage
cablintINFOTLS Server certificate identified
x509lintERRORError parsing URL
x509lintERRORno authorityInformationAccess extension
x509lintERRORNo OCSP over HTTP
x509lintERRORSubject with organizationName, givenName or surname but without stateOrProvince or localityName
x509lintWARNINGexplicitText is not using a UTF8String
x509lintWARNINGNo HTTP URL for issuing certificate
13615553 2015-10-28 00:54:42 2018-01-28 00:54:41 x509lintWARNINGPolicy information has qualifier other than CPS URI
x509lintWARNINGUnknown extended key usage
x509lintINFOSubject has a deprecated CommonName
x509lintINFOUnknown validation policy
zlintERRORSubscriber Certificate: authorityInformationAccess MUST contain the HTTP URL of the Issuing CA's OSCP responder.
zlintERRORSubscriber certificate cRLDistributionPoints extension must contain the HTTP URL of the CA's CRL service
zlintERRORSubscriber Certificate: authorityInformationAccess MUST be present, with the exception of stapling.
zlintWARNINGCompliant certificates should use the utf8string encoding for explicitText
zlintWARNINGSubscriber Certificate: extKeyUsage either the value id-kp-serverAuth or id-kp-clientAuth or both values MUST be present.
zlintWARNINGSubscriber certificates authorityInformationAccess extension should contain the HTTP URL of the issuing CA's certificate
zlintNOTICESubscriber Certificate: commonName is deprecated.

cablintERRORBR certificates with organizationName must include either localityName or stateOrProvinceName
cablintWARNINGCertificate does not include authorityInformationAccess. BRs require OCSP stapling for this certificate.
cablintWARNINGDeprecated Netscape extension 2.16.840.1.113730.1.1 treated as opaque extension
cablintWARNINGTLS Server auth certificates should not contain Netscape Server Gated Crypto usage
cablintINFOTLS Server certificate identified
x509lintERRORError parsing URL
x509lintERRORno authorityInformationAccess extension
x509lintERRORNo OCSP over HTTP
x509lintERRORSubject with organizationName, givenName or surname but without stateOrProvince or localityName
x509lintWARNINGexplicitText is not using a UTF8String
x509lintWARNINGNo HTTP URL for issuing certificate
11544549 2015-10-28 01:59:35 2018-01-28 01:59:34 x509lintWARNINGPolicy information has qualifier other than CPS URI
x509lintWARNINGUnknown extended key usage
x509lintINFOSubject has a deprecated CommonName
x509lintINFOUnknown validation policy
zlintERRORSubscriber Certificate: authorityInformationAccess MUST contain the HTTP URL of the Issuing CA's OSCP responder.
zlintERRORSubscriber certificate cRLDistributionPoints extension must contain the HTTP URL of the CA's CRL service
zlintERRORSubscriber Certificate: authorityInformationAccess MUST be present, with the exception of stapling.
zlintWARNINGCompliant certificates should use the utf8string encoding for explicitText
zlintWARNINGSubscriber Certificate: extKeyUsage either the value id-kp-serverAuth or id-kp-clientAuth or both values MUST be present.
zlintWARNINGSubscriber certificates authorityInformationAccess extension should contain the HTTP URL of the issuing CA's certificate
zlintNOTICESubscriber Certificate: commonName is deprecated.

cablintERRORBR certificates with organizationName must include either localityName or stateOrProvinceName
cablintWARNINGCertificate does not include authorityInformationAccess. BRs require OCSP stapling for this certificate.
cablintWARNINGDeprecated Netscape extension 2.16.840.1.113730.1.1 treated as opaque extension
cablintWARNINGTLS Server auth certificates should not contain Netscape Server Gated Crypto usage
cablintINFOTLS Server certificate identified
x509lintERRORError parsing URL
x509lintERRORno authorityInformationAccess extension
x509lintERRORNo OCSP over HTTP
x509lintERRORSubject with organizationName, givenName or surname but without stateOrProvince or localityName
x509lintWARNINGexplicitText is not using a UTF8String
x509lintWARNINGNo HTTP URL for issuing certificate
10061573 2015-10-06 05:14:27 2018-01-06 05:14:26 x509lintWARNINGPolicy information has qualifier other than CPS URI
x509lintWARNINGUnknown extended key usage
x509lintINFOSubject has a deprecated CommonName
x509lintINFOUnknown validation policy
zlintERRORSubscriber Certificate: authorityInformationAccess MUST contain the HTTP URL of the Issuing CA's OSCP responder.
zlintERRORSubscriber certificate cRLDistributionPoints extension must contain the HTTP URL of the CA's CRL service
zlintERRORSubscriber Certificate: authorityInformationAccess MUST be present, with the exception of stapling.
zlintWARNINGCompliant certificates should use the utf8string encoding for explicitText
zlintWARNINGSubscriber Certificate: extKeyUsage either the value id-kp-serverAuth or id-kp-clientAuth or both values MUST be present.
zlintWARNINGSubscriber certificates authorityInformationAccess extension should contain the HTTP URL of the issuing CA's certificate
zlintNOTICESubscriber Certificate: commonName is deprecated.

cablintERRORBR certificates with organizationName must include either localityName or stateOrProvinceName
cablintWARNINGCertificate does not include authorityInformationAccess. BRs require OCSP stapling for this certificate.
cablintWARNINGDeprecated Netscape extension 2.16.840.1.113730.1.1 treated as opaque extension
cablintWARNINGTLS Server auth certificates should not contain Netscape Server Gated Crypto usage
cablintINFOTLS Server certificate identified
x509lintERRORError parsing URL
x509lintERRORno authorityInformationAccess extension
x509lintERRORNo OCSP over HTTP
x509lintERRORSubject with organizationName, givenName or surname but without stateOrProvince or localityName
x509lintWARNINGexplicitText is not using a UTF8String
x509lintWARNINGNo HTTP URL for issuing certificate
9351675 2015-09-16 02:32:06 2017-12-16 02:32:05 x509lintWARNINGPolicy information has qualifier other than CPS URI
x509lintWARNINGUnknown extended key usage
x509lintINFOSubject has a deprecated CommonName
x509lintINFOUnknown validation policy
zlintERRORSubscriber Certificate: authorityInformationAccess MUST contain the HTTP URL of the Issuing CA's OSCP responder.
zlintERRORSubscriber certificate cRLDistributionPoints extension must contain the HTTP URL of the CA's CRL service
zlintERRORSubscriber Certificate: authorityInformationAccess MUST be present, with the exception of stapling.
zlintWARNINGCompliant certificates should use the utf8string encoding for explicitText
zlintWARNINGSubscriber Certificate: extKeyUsage either the value id-kp-serverAuth or id-kp-clientAuth or both values MUST be present.
zlintWARNINGSubscriber certificates authorityInformationAccess extension should contain the HTTP URL of the issuing CA's certificate
zlintNOTICESubscriber Certificate: commonName is deprecated.

cablintERRORBR certificates with organizationName must include either localityName or stateOrProvinceName
cablintWARNINGCertificate does not include authorityInformationAccess. BRs require OCSP stapling for this certificate.
cablintWARNINGDeprecated Netscape extension 2.16.840.1.113730.1.1 treated as opaque extension
cablintWARNINGTLS Server auth certificates should not contain Netscape Server Gated Crypto usage
cablintINFOTLS Server certificate identified
x509lintERRORError parsing URL
x509lintERRORno authorityInformationAccess extension
x509lintERRORNo OCSP over HTTP
x509lintERRORSubject with organizationName, givenName or surname but without stateOrProvince or localityName
x509lintWARNINGexplicitText is not using a UTF8String
x509lintWARNINGNo HTTP URL for issuing certificate
10833867 2015-10-30 01:37:26 2018-01-30 01:37:25 x509lintWARNINGPolicy information has qualifier other than CPS URI
x509lintWARNINGUnknown extended key usage
x509lintINFOSubject has a deprecated CommonName
x509lintINFOUnknown validation policy
zlintERRORSubscriber Certificate: authorityInformationAccess MUST contain the HTTP URL of the Issuing CA's OSCP responder.
zlintERRORSubscriber certificate cRLDistributionPoints extension must contain the HTTP URL of the CA's CRL service
zlintERRORSubscriber Certificate: authorityInformationAccess MUST be present, with the exception of stapling.
zlintWARNINGCompliant certificates should use the utf8string encoding for explicitText
zlintWARNINGSubscriber Certificate: extKeyUsage either the value id-kp-serverAuth or id-kp-clientAuth or both values MUST be present.
zlintWARNINGSubscriber certificates authorityInformationAccess extension should contain the HTTP URL of the issuing CA's certificate
zlintNOTICESubscriber Certificate: commonName is deprecated.

cablintERRORBR certificates with organizationName must include either localityName or stateOrProvinceName
cablintWARNINGCertificate does not include authorityInformationAccess. BRs require OCSP stapling for this certificate.
cablintWARNINGDeprecated Netscape extension 2.16.840.1.113730.1.1 treated as opaque extension
cablintWARNINGTLS Server auth certificates should not contain Netscape Server Gated Crypto usage
cablintINFOTLS Server certificate identified
x509lintERRORError parsing URL
x509lintERRORno authorityInformationAccess extension
x509lintERRORNo OCSP over HTTP
x509lintERRORSubject with organizationName, givenName or surname but without stateOrProvince or localityName
x509lintWARNINGexplicitText is not using a UTF8String
x509lintWARNINGNo HTTP URL for issuing certificate
10826452 2015-11-12 08:32:09 2018-02-12 08:32:08 x509lintWARNINGPolicy information has qualifier other than CPS URI
x509lintWARNINGUnknown extended key usage
x509lintINFOSubject has a deprecated CommonName
x509lintINFOUnknown validation policy
zlintERRORSubscriber Certificate: authorityInformationAccess MUST contain the HTTP URL of the Issuing CA's OSCP responder.
zlintERRORSubscriber certificate cRLDistributionPoints extension must contain the HTTP URL of the CA's CRL service
zlintERRORSubscriber Certificate: authorityInformationAccess MUST be present, with the exception of stapling.
zlintWARNINGCompliant certificates should use the utf8string encoding for explicitText
zlintWARNINGSubscriber Certificate: extKeyUsage either the value id-kp-serverAuth or id-kp-clientAuth or both values MUST be present.
zlintWARNINGSubscriber certificates authorityInformationAccess extension should contain the HTTP URL of the issuing CA's certificate
zlintNOTICESubscriber Certificate: commonName is deprecated.

cablintERRORBR certificates with organizationName must include either localityName or stateOrProvinceName
cablintWARNINGCertificate does not include authorityInformationAccess. BRs require OCSP stapling for this certificate.
cablintWARNINGDeprecated Netscape extension 2.16.840.1.113730.1.1 treated as opaque extension
cablintWARNINGTLS Server auth certificates should not contain Netscape Server Gated Crypto usage
cablintINFOTLS Server certificate identified
x509lintERRORError parsing URL
x509lintERRORno authorityInformationAccess extension
x509lintERRORNo OCSP over HTTP
x509lintERRORSubject with organizationName, givenName or surname but without stateOrProvince or localityName
x509lintWARNINGexplicitText is not using a UTF8String
x509lintWARNINGNo HTTP URL for issuing certificate
9356645 2015-09-11 09:40:05 2017-12-11 09:40:04 x509lintWARNINGPolicy information has qualifier other than CPS URI
x509lintWARNINGUnknown extended key usage
x509lintINFOSubject has a deprecated CommonName
x509lintINFOUnknown validation policy
zlintERRORSubscriber Certificate: authorityInformationAccess MUST contain the HTTP URL of the Issuing CA's OSCP responder.
zlintERRORSubscriber certificate cRLDistributionPoints extension must contain the HTTP URL of the CA's CRL service
zlintERRORSubscriber Certificate: authorityInformationAccess MUST be present, with the exception of stapling.
zlintWARNINGCompliant certificates should use the utf8string encoding for explicitText
zlintWARNINGSubscriber Certificate: extKeyUsage either the value id-kp-serverAuth or id-kp-clientAuth or both values MUST be present.
zlintWARNINGSubscriber certificates authorityInformationAccess extension should contain the HTTP URL of the issuing CA's CRL service
certificate
zlintNOTICESubscriber Certificate: commonName is deprecated.

cablintERRORBR certificates with organizationName must include either localityName or stateOrProvinceName
cablintWARNINGCertificate does not include authorityInformationAccess. BRs require OCSP stapling for this certificate.
cablintWARNINGDeprecated Netscape extension 2.16.840.1.113730.1.1 treated as opaque extension
cablintWARNINGTLS Server auth certificates should not contain Netscape Server Gated Crypto usage
cablintINFOTLS Server certificate identified
x509lintERRORError parsing URL
x509lintERRORno authorityInformationAccess extension
x509lintERRORNo OCSP over HTTP
x509lintERRORSubject with organizationName, givenName or surname but without stateOrProvince or localityName
x509lintWARNINGexplicitText is not using a UTF8String
x509lintWARNINGNo HTTP URL for issuing certificate
22695132 2015-10-15 10:31:19 2018-01-15 10:31:18 x509lintWARNINGPolicy information has qualifier other than CPS URI
x509lintWARNINGUnknown extended key usage
x509lintINFOSubject has a deprecated CommonName
x509lintINFOUnknown validation policy
zlintERRORSubscriber Certificate: authorityInformationAccess MUST contain the HTTP URL of the Issuing CA's OSCP responder.
zlintERRORSubscriber certificate cRLDistributionPoints extension must contain the HTTP URL of the CA's CRL service
zlintERRORSubscriber Certificate: authorityInformationAccess MUST be present, with the exception of stapling.
zlintWARNINGCompliant certificates should use the utf8string encoding for explicitText
zlintWARNINGSubscriber Certificate: extKeyUsage either the value id-kp-serverAuth or id-kp-clientAuth or both values MUST be present.
zlintWARNINGSubscriber certificates authorityInformationAccess extension should contain the HTTP URL of the issuing CA's certificate
zlintNOTICESubscriber Certificate: commonName is deprecated.

cablintERRORBR certificates with organizationName must include either localityName or stateOrProvinceName
cablintWARNINGCertificate does not include authorityInformationAccess. BRs require OCSP stapling for this certificate.
cablintWARNINGDeprecated Netscape extension 2.16.840.1.113730.1.1 treated as opaque extension
cablintWARNINGTLS Server auth certificates should not contain Netscape Server Gated Crypto usage
cablintINFOTLS Server certificate identified
x509lintERRORError parsing URL
x509lintERRORno authorityInformationAccess extension
x509lintERRORNo OCSP over HTTP
x509lintERRORSubject with organizationName, givenName or surname but without stateOrProvince or localityName
x509lintWARNINGexplicitText is not using a UTF8String
x509lintWARNINGNo HTTP URL for issuing certificate
10911101 2015-09-30 08:14:32 2017-12-30 08:14:31 x509lintWARNINGPolicy information has qualifier other than CPS URI
x509lintWARNINGUnknown extended key usage
x509lintINFOSubject has a deprecated CommonName
x509lintINFOUnknown validation policy
zlintERRORSubscriber Certificate: authorityInformationAccess MUST contain the HTTP URL of the Issuing CA's OSCP responder.
zlintERRORSubscriber certificate cRLDistributionPoints extension must contain the HTTP URL of the CA's CRL service
zlintERRORSubscriber Certificate: authorityInformationAccess MUST be present, with the exception of stapling.
zlintWARNINGCompliant certificates should use the utf8string encoding for explicitText
zlintWARNINGSubscriber Certificate: extKeyUsage either the value id-kp-serverAuth or id-kp-clientAuth or both values MUST be present.
zlintWARNINGSubscriber certificates authorityInformationAccess extension should contain the HTTP URL of the issuing CA's certificate
zlintNOTICESubscriber Certificate: commonName is deprecated.

cablintERRORBR certificates with organizationName must include either localityName or stateOrProvinceName
cablintWARNINGCertificate does not include authorityInformationAccess. BRs require OCSP stapling for this certificate.
cablintWARNINGDeprecated Netscape extension 2.16.840.1.113730.1.1 treated as opaque extension
cablintWARNINGTLS Server auth certificates should not contain Netscape Server Gated Crypto usage
cablintINFOTLS Server certificate identified
x509lintERRORError parsing URL
x509lintERRORno authorityInformationAccess extension
x509lintERRORNo OCSP over HTTP
x509lintERRORSubject with organizationName, givenName or surname but without stateOrProvince or localityName
x509lintWARNINGexplicitText is not using a UTF8String
x509lintWARNINGNo HTTP URL for issuing certificate
10592865 2015-11-05 07:46:52 2018-02-05 07:46:51 x509lintWARNINGPolicy information has qualifier other than CPS URI
x509lintWARNINGUnknown extended key usage
x509lintINFOSubject has a deprecated CommonName
x509lintINFOUnknown validation policy
zlintERRORSubscriber Certificate: authorityInformationAccess MUST contain the HTTP URL of the Issuing CA's OSCP responder.
zlintERRORSubscriber certificate cRLDistributionPoints extension must contain the HTTP URL of the CA's CRL service
zlintERRORSubscriber Certificate: authorityInformationAccess MUST be present, with the exception of stapling.
zlintWARNINGCompliant certificates should use the utf8string encoding for explicitText
zlintWARNINGSubscriber Certificate: extKeyUsage either the value id-kp-serverAuth or id-kp-clientAuth or both values MUST be present.
zlintWARNINGSubscriber certificates authorityInformationAccess extension should contain the HTTP URL of the issuing CA's certificate
zlintNOTICESubscriber Certificate: commonName is deprecated.

cablintERRORBR certificates with organizationName must include either localityName or stateOrProvinceName
cablintWARNINGCertificate does not include authorityInformationAccess. BRs require OCSP stapling for this certificate.
cablintWARNINGDeprecated Netscape extension 2.16.840.1.113730.1.1 treated as opaque extension
cablintWARNINGTLS Server auth certificates should not contain Netscape Server Gated Crypto usage
cablintINFOTLS Server certificate identified
x509lintERRORError parsing URL
x509lintERRORno authorityInformationAccess extension
x509lintERRORNo OCSP over HTTP
x509lintERRORSubject with organizationName, givenName or surname but without stateOrProvince or localityName
x509lintWARNINGexplicitText is not using a UTF8String
x509lintWARNINGNo HTTP URL for issuing certificate
9166482 2015-09-03 02:28:08 2017-12-03 02:28:07 x509lintWARNINGPolicy information has qualifier other than CPS URI
x509lintWARNINGUnknown extended key usage
x509lintINFOSubject has a deprecated CommonName
x509lintINFOUnknown validation policy
zlintERRORSubscriber Certificate: authorityInformationAccess MUST contain the HTTP URL of the Issuing CA's OSCP responder.
zlintERRORSubscriber certificate cRLDistributionPoints extension must contain the HTTP URL of the CA's CRL service
zlintERRORSubscriber Certificate: authorityInformationAccess MUST be present, with the exception of stapling.
zlintWARNINGCompliant certificates should use the utf8string encoding for explicitText
zlintWARNINGSubscriber Certificate: extKeyUsage either the value id-kp-serverAuth or id-kp-clientAuth or both values MUST be present.
zlintWARNINGSubscriber certificates authorityInformationAccess extension should contain the HTTP URL of the issuing CA's certificate
zlintNOTICESubscriber Certificate: commonName is deprecated.

cablintERRORBR certificates with CRL Distribution Point must include HTTP URL
cablintERRORBR certificates with organizationName must include either localityName or stateOrProvinceName
cablintERRORWildcard to immediate left of public suffix in SAN
cablintWARNINGCertificate does not include authorityInformationAccess. BRs require OCSP stapling for this certificate.
cablintWARNINGDeprecated Netscape extension 2.16.840.1.113730.1.1 treated as opaque extension
cablintWARNINGTLS Server auth certificates should not contain Netscape Server Gated Crypto usage
cablintINFOTLS Server certificate identified
x509lintERRORError parsing URL
x509lintERRORno authorityInformationAccess extension
x509lintERRORNo OCSP over HTTP
x509lintERRORSubject with organizationName, givenName or surname but without stateOrProvince or localityName
x509lintWARNINGexplicitText is not using a UTF8String
10598992 2015-11-05 08:15:26 2018-02-05 08:15:25 x509lintWARNINGNo HTTP URL for issuing certificate
x509lintWARNINGPolicy information has qualifier other than CPS URI
x509lintWARNINGUnknown extended key usage
x509lintINFOSubject has a deprecated CommonName
x509lintINFOUnknown validation policy
zlintERRORSubscriber Certificate: authorityInformationAccess MUST contain the HTTP URL of the Issuing CA's OSCP responder.
zlintERRORSubscriber certificate cRLDistributionPoints extension must contain the HTTP URL of the CA's CRL service
zlintERRORSubscriber Certificate: authorityInformationAccess MUST be present, with the exception of stapling.
zlintWARNINGCompliant certificates should use the utf8string encoding for explicitText
zlintWARNINGSubscriber Certificate: extKeyUsage either the value id-kp-serverAuth or id-kp-clientAuth or both values MUST be present.
zlintWARNINGSubscriber certificates authorityInformationAccess extension should contain the HTTP URL of the issuing CA's certificate

cablintERRORBR certificates with CRL Distribution Point must include HTTP URL
cablintERRORBR certificates with organizationName must include either localityName or stateOrProvinceName
cablintERRORUnknown TLD in SAN
cablintWARNINGCertificate does not include authorityInformationAccess. BRs require OCSP stapling for this certificate.
cablintWARNINGDeprecated Netscape extension 2.16.840.1.113730.1.1 treated as opaque extension
cablintWARNINGTLS Server auth certificates should not contain Netscape Server Gated Crypto usage
cablintINFOTLS Server certificate identified
x509lintERRORError parsing URL
x509lintERRORIP address in dns name
x509lintERRORno authorityInformationAccess extension
x509lintERRORNo OCSP over HTTP
x509lintERRORSubject with organizationName, givenName or surname but without stateOrProvince or localityName
10667897 2015-11-10 05:27:43 2018-02-10 05:27:42 x509lintWARNINGexplicitText is not using a UTF8String
x509lintWARNINGNo HTTP URL for issuing certificate
x509lintWARNINGPolicy information has qualifier other than CPS URI
x509lintWARNINGUnknown extended key usage
x509lintINFOSubject has a deprecated CommonName
x509lintINFOUnknown validation policy
zlintERRORDNSNames must have a valid TLD.
zlintERRORSubscriber Certificate: authorityInformationAccess MUST contain the HTTP URL of the Issuing CA's OSCP responder.
zlintERRORSubscriber certificate cRLDistributionPoints extension must contain the HTTP URL of the CA's CRL service
zlintERRORSubscriber Certificate: authorityInformationAccess MUST be present, with the exception of stapling.
zlintWARNINGCompliant certificates should use the utf8string encoding for explicitText
zlintWARNINGSubscriber Certificate: extKeyUsage either the value id-kp-serverAuth or id-kp-clientAuth or both values MUST be present

cablintERRORBR certificates with organizationName must include either localityName or stateOrProvinceName
cablintWARNINGCertificate does not include authorityInformationAccess. BRs require OCSP stapling for this certificate.
cablintWARNINGDeprecated Netscape extension 2.16.840.1.113730.1.1 treated as opaque extension
cablintWARNINGTLS Server auth certificates should not contain Netscape Server Gated Crypto usage
cablintINFOTLS Server certificate identified
x509lintERRORError parsing URL
x509lintERRORno authorityInformationAccess extension
x509lintERRORNo OCSP over HTTP
x509lintERRORSubject with organizationName, givenName or surname but without stateOrProvince or localityName
x509lintWARNINGexplicitText is not using a UTF8String
x509lintWARNINGNo HTTP URL for issuing certificate
230078926 2015-09-18 07:07:10 2017-12-18 07:07:09 x509lintWARNINGPolicy information has qualifier other than CPS URI
x509lintWARNINGUnknown extended key usage
x509lintINFOSubject has a deprecated CommonName
x509lintINFOUnknown validation policy
zlintERRORSubscriber Certificate: authorityInformationAccess MUST contain the HTTP URL of the Issuing CA's OSCP responder.
zlintERRORSubscriber certificate cRLDistributionPoints extension must contain the HTTP URL of the CA's CRL service
zlintERRORSubscriber Certificate: authorityInformationAccess MUST be present, with the exception of stapling.
zlintWARNINGCompliant certificates should use the utf8string encoding for explicitText
zlintWARNINGSubscriber Certificate: extKeyUsage either the value id-kp-serverAuth or id-kp-clientAuth or both values MUST be present.
zlintWARNINGSubscriber certificates authorityInformationAccess extension should contain the HTTP URL of the issuing CA's certificate
zlintNOTICESubscriber Certificate: commonName is deprecated.

cablintERRORBR certificates with organizationName must include either localityName or stateOrProvinceName
cablintWARNINGCertificate does not include authorityInformationAccess. BRs require OCSP stapling for this certificate.
cablintWARNINGDeprecated Netscape extension 2.16.840.1.113730.1.1 treated as opaque extension
cablintWARNINGTLS Server auth certificates should not contain Netscape Server Gated Crypto usage
cablintINFOTLS Server certificate identified
x509lintERRORError parsing URL
x509lintERRORno authorityInformationAccess extension
x509lintERRORNo OCSP over HTTP
x509lintERRORSubject with organizationName, givenName or surname but without stateOrProvince or localityName
x509lintWARNINGexplicitText is not using a UTF8String
x509lintWARNINGNo HTTP URL for issuing certificate
10025000 2015-10-06 06:14:39 2018-01-06 06:14:38 x509lintWARNINGPolicy information has qualifier other than CPS URI
x509lintWARNINGUnknown extended key usage
x509lintINFOSubject has a deprecated CommonName
x509lintINFOUnknown validation policy
zlintERRORSubscriber Certificate: authorityInformationAccess MUST contain the HTTP URL of the Issuing CA's OSCP responder.
zlintERRORSubscriber certificate cRLDistributionPoints extension must contain the HTTP URL of the CA's CRL service
zlintERRORSubscriber Certificate: authorityInformationAccess MUST be present, with the exception of stapling.
zlintWARNINGCompliant certificates should use the utf8string encoding for explicitText
zlintWARNINGSubscriber Certificate: extKeyUsage either the value id-kp-serverAuth or id-kp-clientAuth or both values MUST be present.
zlintWARNINGSubscriber certificates authorityInformationAccess extension should contain the HTTP URL of the issuing CA's certificate
zlintNOTICESubscriber Certificate: commonName is deprecated.

cablintERRORBR certificates with organizationName must include either localityName or stateOrProvinceName
cablintWARNINGCertificate does not include authorityInformationAccess. BRs require OCSP stapling for this certificate.
cablintWARNINGDeprecated Netscape extension 2.16.840.1.113730.1.1 treated as opaque extension
cablintWARNINGTLS Server auth certificates should not contain Netscape Server Gated Crypto usage
cablintINFOTLS Server certificate identified
x509lintERRORError parsing URL
x509lintERRORno authorityInformationAccess extension
x509lintERRORNo OCSP over HTTP
x509lintERRORSubject with organizationName, givenName or surname but without stateOrProvince or localityName
x509lintWARNINGexplicitText is not using a UTF8String
x509lintWARNINGNo HTTP URL for issuing certificate
287401680 2015-10-02 04:20:29 2018-01-02 04:20:28 x509lintWARNINGPolicy information has qualifier other than CPS URI
x509lintWARNINGUnknown extended key usage
x509lintINFOSubject has a deprecated CommonName
x509lintINFOUnknown validation policy
zlintERRORSubscriber Certificate: authorityInformationAccess MUST contain the HTTP URL of the Issuing CA's OSCP responder.
zlintERRORSubscriber certificate cRLDistributionPoints extension must contain the HTTP URL of the CA's CRL service
zlintERRORSubscriber Certificate: authorityInformationAccess MUST be present, with the exception of stapling.
zlintWARNINGCompliant certificates should use the utf8string encoding for explicitText
zlintWARNINGSubscriber Certificate: extKeyUsage either the value id-kp-serverAuth or id-kp-clientAuth or both values MUST be present.
zlintWARNINGSubscriber certificates authorityInformationAccess extension should contain the HTTP URL of the issuing CA's certificate
zlintNOTICESubscriber Certificate: commonName is deprecated.

cablintERRORBR certificates with organizationName must include either localityName or stateOrProvinceName
cablintWARNINGCertificate does not include authorityInformationAccess. BRs require OCSP stapling for this certificate.
cablintWARNINGDeprecated Netscape extension 2.16.840.1.113730.1.1 treated as opaque extension
cablintWARNINGTLS Server auth certificates should not contain Netscape Server Gated Crypto usage
cablintINFOTLS Server certificate identified
x509lintERRORError parsing URL
x509lintERRORno authorityInformationAccess extension
x509lintERRORNo OCSP over HTTP
x509lintERRORSubject with organizationName, givenName or surname but without stateOrProvince or localityName
x509lintWARNINGexplicitText is not using a UTF8String
x509lintWARNINGNo HTTP URL for issuing certificate
9246611 2015-09-03 01:12:58 2017-12-03 01:12:57 x509lintWARNINGPolicy information has qualifier other than CPS URI
x509lintWARNINGUnknown extended key usage
x509lintINFOSubject has a deprecated CommonName
x509lintINFOUnknown validation policy
zlintERRORSubscriber Certificate: authorityInformationAccess MUST contain the HTTP URL of the Issuing CA's OSCP responder.
zlintERRORSubscriber certificate cRLDistributionPoints extension must contain the HTTP URL of the CA's CRL service
zlintERRORSubscriber Certificate: authorityInformationAccess MUST be present, with the exception of stapling.
zlintWARNINGCompliant certificates should use the utf8string encoding for explicitText
zlintWARNINGSubscriber Certificate: extKeyUsage either the value id-kp-serverAuth or id-kp-clientAuth or both values MUST be present.
zlintWARNINGSubscriber certificates authorityInformationAccess extension should contain the HTTP URL of the issuing CA's certificate
zlintNOTICESubscriber Certificate: commonName is deprecated.

cablintERRORBR certificates with organizationName must include either localityName or stateOrProvinceName
cablintWARNINGCertificate does not include authorityInformationAccess. BRs require OCSP stapling for this certificate.
cablintWARNINGDeprecated Netscape extension 2.16.840.1.113730.1.1 treated as opaque extension
cablintWARNINGTLS Server auth certificates should not contain Netscape Server Gated Crypto usage
cablintINFOTLS Server certificate identified
x509lintERRORError parsing URL
x509lintERRORno authorityInformationAccess extension
x509lintERRORNo OCSP over HTTP
x509lintERRORSubject with organizationName, givenName or surname but without stateOrProvince or localityName
x509lintWARNINGexplicitText is not using a UTF8String
x509lintWARNINGNo HTTP URL for issuing certificate
10982750 2015-11-23 01:23:05 2018-02-23 01:23:04 x509lintWARNINGPolicy information has qualifier other than CPS URI
x509lintWARNINGUnknown extended key usage
x509lintINFOSubject has a deprecated CommonName
x509lintINFOUnknown validation policy
zlintERRORSubscriber Certificate: authorityInformationAccess MUST contain the HTTP URL of the Issuing CA's OSCP responder.
zlintERRORSubscriber certificate cRLDistributionPoints extension must contain the HTTP URL of the CA's CRL service
zlintERRORSubscriber Certificate: authorityInformationAccess MUST be present, with the exception of stapling.
zlintWARNINGCompliant certificates should use the utf8string encoding for explicitText
zlintWARNINGSubscriber Certificate: extKeyUsage either the value id-kp-serverAuth or id-kp-clientAuth or both values MUST be present.
zlintWARNINGSubscriber certificates authorityInformationAccess extension should contain the HTTP URL of the issuing CA's certificate
zlintNOTICESubscriber Certificate: commonName is deprecated.

cablintERRORBR certificates with organizationName must include either localityName or stateOrProvinceName
cablintWARNINGCertificate does not include authorityInformationAccess. BRs require OCSP stapling for this certificate.
cablintWARNINGDeprecated Netscape extension 2.16.840.1.113730.1.1 treated as opaque extension
cablintWARNINGTLS Server auth certificates should not contain Netscape Server Gated Crypto usage
cablintINFOTLS Server certificate identified
x509lintERRORError parsing URL
x509lintERRORno authorityInformationAccess extension
x509lintERRORNo OCSP over HTTP
x509lintERRORSubject with organizationName, givenName or surname but without stateOrProvince or localityName
x509lintWARNINGexplicitText is not using a UTF8String
x509lintWARNINGNo HTTP URL for issuing certificate
10677577 2015-11-12 05:08:14 2018-02-12 05:08:13 x509lintWARNINGPolicy information has qualifier other than CPS URI
x509lintWARNINGUnknown extended key usage
x509lintINFOSubject has a deprecated CommonName
x509lintINFOUnknown validation policy
zlintERRORSubscriber Certificate: authorityInformationAccess MUST contain the HTTP URL of the Issuing CA's OSCP responder.
zlintERRORSubscriber certificate cRLDistributionPoints extension must contain the HTTP URL of the CA's CRL service
zlintERRORSubscriber Certificate: authorityInformationAccess MUST be present, with the exception of stapling.
zlintWARNINGCompliant certificates should use the utf8string encoding for explicitText
zlintWARNINGSubscriber Certificate: extKeyUsage either the value id-kp-serverAuth or id-kp-clientAuth or both values MUST be present.
zlintWARNINGSubscriber certificates authorityInformationAccess extension should contain the HTTP URL of the issuing CA's certificate
zlintNOTICESubscriber Certificate: commonName is deprecated.

cablintERRORBR certificates with organizationName must include either localityName or stateOrProvinceName
cablintWARNINGCertificate does not include authorityInformationAccess. BRs require OCSP stapling for this certificate.
cablintWARNINGDeprecated Netscape extension 2.16.840.1.113730.1.1 treated as opaque extension
cablintWARNINGTLS Server auth certificates should not contain Netscape Server Gated Crypto usage
cablintINFOTLS Server certificate identified
x509lintERRORError parsing URL
x509lintERRORno authorityInformationAccess extension
x509lintERRORNo OCSP over HTTP
x509lintERRORSubject with organizationName, givenName or surname but without stateOrProvince or localityName
x509lintWARNINGexplicitText is not using a UTF8String
x509lintWARNINGNo HTTP URL for issuing certificate
14520827 2015-11-05 09:22:16 2018-02-05 09:22:15 x509lintWARNINGPolicy information has qualifier other than CPS URI
x509lintWARNINGUnknown extended key usage
x509lintINFOSubject has a deprecated CommonName
x509lintINFOUnknown validation policy
zlintERRORSubscriber Certificate: authorityInformationAccess MUST contain the HTTP URL of the Issuing CA's OSCP responder.
zlintERRORSubscriber certificate cRLDistributionPoints extension must contain the HTTP URL of the CA's CRL service
zlintERRORSubscriber Certificate: authorityInformationAccess MUST be present, with the exception of stapling.
zlintWARNINGCompliant certificates should use the utf8string encoding for explicitText
zlintWARNINGSubscriber Certificate: extKeyUsage either the value id-kp-serverAuth or id-kp-clientAuth or both values MUST be present.
zlintWARNINGSubscriber certificates authorityInformationAccess extension should contain the HTTP URL of the issuing CA's certificate
zlintNOTICESubscriber Certificate: commonName is deprecated.

cablintERRORBR certificates with organizationName must include either localityName or stateOrProvinceName
cablintWARNINGCertificate does not include authorityInformationAccess. BRs require OCSP stapling for this certificate.
cablintWARNINGDeprecated Netscape extension 2.16.840.1.113730.1.1 treated as opaque extension
cablintWARNINGTLS Server auth certificates should not contain Netscape Server Gated Crypto usage
cablintINFOTLS Server certificate identified
x509lintERRORError parsing URL
x509lintERRORno authorityInformationAccess extension
x509lintERRORNo OCSP over HTTP
x509lintERRORSubject with organizationName, givenName or surname but without stateOrProvince or localityName
x509lintWARNINGexplicitText is not using a UTF8String
x509lintWARNINGNo HTTP URL for issuing certificate
10609864 2015-10-29 08:26:45 2018-01-29 08:26:44 x509lintWARNINGPolicy information has qualifier other than CPS URI
x509lintWARNINGUnknown extended key usage
x509lintINFOSubject has a deprecated CommonName
x509lintINFOUnknown validation policy
zlintERRORSubscriber Certificate: authorityInformationAccess MUST contain the HTTP URL of the Issuing CA's OSCP responder.
zlintERRORSubscriber certificate cRLDistributionPoints extension must contain the HTTP URL of the CA's CRL service
zlintERRORSubscriber Certificate: authorityInformationAccess MUST be present, with the exception of stapling.
zlintWARNINGCompliant certificates should use the utf8string encoding for explicitText
zlintWARNINGSubscriber Certificate: extKeyUsage either the value id-kp-serverAuth or id-kp-clientAuth or both values MUST be present.
zlintWARNINGSubscriber certificates authorityInformationAccess extension should contain the HTTP URL of the issuing CA's certificate
zlintNOTICESubscriber Certificate: commonName is deprecated.

cablintERRORBR certificates with organizationName must include either localityName or stateOrProvinceName
cablintWARNINGCertificate does not include authorityInformationAccess. BRs require OCSP stapling for this certificate.
cablintWARNINGDeprecated Netscape extension 2.16.840.1.113730.1.1 treated as opaque extension
cablintWARNINGTLS Server auth certificates should not contain Netscape Server Gated Crypto usage
cablintINFOTLS Server certificate identified
x509lintERRORError parsing URL
x509lintERRORno authorityInformationAccess extension
x509lintERRORNo OCSP over HTTP
x509lintERRORSubject with organizationName, givenName or surname but without stateOrProvince or localityName
x509lintWARNINGexplicitText is not using a UTF8String
x509lintWARNINGNo HTTP URL for issuing certificate
10555037 2015-11-04 01:28:13 2018-02-04 01:28:12 x509lintWARNINGPolicy information has qualifier other than CPS URI
x509lintWARNINGUnknown extended key usage
x509lintINFOSubject has a deprecated CommonName
x509lintINFOUnknown validation policy
zlintERRORSubscriber Certificate: authorityInformationAccess MUST contain the HTTP URL of the Issuing CA's OSCP responder.
zlintERRORSubscriber certificate cRLDistributionPoints extension must contain the HTTP URL of the CA's CRL service
zlintERRORSubscriber Certificate: authorityInformationAccess MUST be present, with the exception of stapling.
zlintWARNINGCompliant certificates should use the utf8string encoding for explicitText
zlintWARNINGSubscriber Certificate: extKeyUsage either the value id-kp-serverAuth or id-kp-clientAuth or both values MUST be present.
zlintWARNINGSubscriber certificates authorityInformationAccess extension should contain the HTTP URL of the issuing CA's certificate
zlintNOTICESubscriber Certificate: commonName is deprecated.

cablintERRORBR certificates with organizationName must include either localityName or stateOrProvinceName
cablintWARNINGCertificate does not include authorityInformationAccess. BRs require OCSP stapling for this certificate.
cablintWARNINGDeprecated Netscape extension 2.16.840.1.113730.1.1 treated as opaque extension
cablintWARNINGTLS Server auth certificates should not contain Netscape Server Gated Crypto usage
cablintINFOTLS Server certificate identified
x509lintERRORError parsing URL
x509lintERRORno authorityInformationAccess extension
x509lintERRORNo OCSP over HTTP
x509lintERRORSubject with organizationName, givenName or surname but without stateOrProvince or localityName
x509lintWARNINGexplicitText is not using a UTF8String
x509lintWARNINGNo HTTP URL for issuing certificate
287667681 2015-10-22 08:03:22 2018-01-22 08:03:21 x509lintWARNINGPolicy information has qualifier other than CPS URI
x509lintWARNINGUnknown extended key usage
x509lintINFOSubject has a deprecated CommonName
x509lintINFOUnknown validation policy
zlintERRORSubscriber Certificate: authorityInformationAccess MUST contain the HTTP URL of the Issuing CA's OSCP responder.
zlintERRORSubscriber certificate cRLDistributionPoints extension must contain the HTTP URL of the CA's CRL service
zlintERRORSubscriber Certificate: authorityInformationAccess MUST be present, with the exception of stapling.
zlintWARNINGCompliant certificates should use the utf8string encoding for explicitText
zlintWARNINGSubscriber Certificate: extKeyUsage either the value id-kp-serverAuth or id-kp-clientAuth or both values MUST be present.
zlintWARNINGSubscriber certificates authorityInformationAccess extension should contain the HTTP URL of the issuing CA's certificate
zlintNOTICESubscriber Certificate: commonName is deprecated.

cablintERRORBR certificates with organizationName must include either localityName or stateOrProvinceName
cablintWARNINGCertificate does not include authorityInformationAccess. BRs require OCSP stapling for this certificate.
cablintWARNINGDeprecated Netscape extension 2.16.840.1.113730.1.1 treated as opaque extension
cablintWARNINGTLS Server auth certificates should not contain Netscape Server Gated Crypto usage
cablintINFOTLS Server certificate identified
x509lintERRORError parsing URL
x509lintERRORno authorityInformationAccess extension
x509lintERRORNo OCSP over HTTP
x509lintERRORSubject with organizationName, givenName or surname but without stateOrProvince or localityName
x509lintWARNINGexplicitText is not using a UTF8String
x509lintWARNINGNo HTTP URL for issuing certificate
9653918 2015-09-14 05:25:20 2017-12-14 05:25:19 x509lintWARNINGPolicy information has qualifier other than CPS URI
x509lintWARNINGUnknown extended key usage
x509lintINFOSubject has a deprecated CommonName
x509lintINFOUnknown validation policy
zlintERRORSubscriber Certificate: authorityInformationAccess MUST contain the HTTP URL of the Issuing CA's OSCP responder.
zlintERRORSubscriber certificate cRLDistributionPoints extension must contain the HTTP URL of the CA's CRL service
zlintERRORSubscriber Certificate: authorityInformationAccess MUST be present, with the exception of stapling.
zlintWARNINGCompliant certificates should use the utf8string encoding for explicitText
zlintWARNINGSubscriber Certificate: extKeyUsage either the value id-kp-serverAuth or id-kp-clientAuth or both values MUST be present.
zlintWARNINGSubscriber certificates authorityInformationAccess extension should contain the HTTP URL of the issuing CA's certificate
zlintNOTICESubscriber Certificate: commonName is deprecated.

cablintERRORBR certificates with organizationName must include either localityName or stateOrProvinceName
cablintWARNINGCertificate does not include authorityInformationAccess. BRs require OCSP stapling for this certificate.
cablintWARNINGDeprecated Netscape extension 2.16.840.1.113730.1.1 treated as opaque extension
cablintWARNINGTLS Server auth certificates should not contain Netscape Server Gated Crypto usage
cablintINFOTLS Server certificate identified
x509lintERRORError parsing URL
x509lintERRORno authorityInformationAccess extension
x509lintERRORNo OCSP over HTTP
x509lintERRORSubject with organizationName, givenName or surname but without stateOrProvince or localityName
x509lintWARNINGexplicitText is not using a UTF8String
x509lintWARNINGNo HTTP URL for issuing certificate
10382391 2015-10-26 05:57:05 2018-01-26 05:57:04 x509lintWARNINGPolicy information has qualifier other than CPS URI
x509lintWARNINGUnknown extended key usage
x509lintINFOSubject has a deprecated CommonName
x509lintINFOUnknown validation policy
zlintERRORSubscriber Certificate: authorityInformationAccess MUST contain the HTTP URL of the Issuing CA's OSCP responder.
zlintERRORSubscriber certificate cRLDistributionPoints extension must contain the HTTP URL of the CA's CRL service
zlintERRORSubscriber Certificate: authorityInformationAccess MUST be present, with the exception of stapling.
zlintWARNINGCompliant certificates should use the utf8string encoding for explicitText
zlintWARNINGSubscriber Certificate: extKeyUsage either the value id-kp-serverAuth or id-kp-clientAuth or both values MUST be present.
zlintWARNINGSubscriber certificates authorityInformationAccess extension should contain the HTTP URL of the issuing CA's certificate
zlintNOTICESubscriber Certificate: commonName is deprecated.

cablintERRORBR certificates with organizationName must include either localityName or stateOrProvinceName
cablintWARNINGCertificate does not include authorityInformationAccess. BRs require OCSP stapling for this certificate.
cablintWARNINGDeprecated Netscape extension 2.16.840.1.113730.1.1 treated as opaque extension
cablintWARNINGTLS Server auth certificates should not contain Netscape Server Gated Crypto usage
cablintINFOTLS Server certificate identified
x509lintERRORError parsing URL
x509lintERRORno authorityInformationAccess extension
x509lintERRORNo OCSP over HTTP
x509lintERRORSubject with organizationName, givenName or surname but without stateOrProvince or localityName
x509lintWARNINGexplicitText is not using a UTF8String
x509lintWARNINGNo HTTP URL for issuing certificate
9199338 2015-09-04 02:03:04 2017-12-04 02:03:03 x509lintWARNINGPolicy information has qualifier other than CPS URI
x509lintWARNINGUnknown extended key usage
x509lintINFOSubject has a deprecated CommonName
x509lintINFOUnknown validation policy
zlintERRORSubscriber Certificate: authorityInformationAccess MUST contain the HTTP URL of the Issuing CA's OSCP responder.
zlintERRORSubscriber certificate cRLDistributionPoints extension must contain the HTTP URL of the CA's CRL service
zlintERRORSubscriber Certificate: authorityInformationAccess MUST be present, with the exception of stapling.
zlintWARNINGCompliant certificates should use the utf8string encoding for explicitText
zlintWARNINGSubscriber Certificate: extKeyUsage either the value id-kp-serverAuth or id-kp-clientAuth or both values MUST be present.
zlintWARNINGSubscriber certificates authorityInformationAccess extension should contain the HTTP URL of the issuing CA's certificate
zlintNOTICESubscriber Certificate: commonName is deprecated.

cablintERRORBR certificates with organizationName must include either localityName or stateOrProvinceName
cablintWARNINGCertificate does not include authorityInformationAccess. BRs require OCSP stapling for this certificate.
cablintWARNINGDeprecated Netscape extension 2.16.840.1.113730.1.1 treated as opaque extension
cablintWARNINGTLS Server auth certificates should not contain Netscape Server Gated Crypto usage
cablintINFOTLS Server certificate identified
x509lintERRORError parsing URL
x509lintERRORno authorityInformationAccess extension
x509lintERRORNo OCSP over HTTP
x509lintERRORSubject with organizationName, givenName or surname but without stateOrProvince or localityName
x509lintWARNINGexplicitText is not using a UTF8String
x509lintWARNINGNo HTTP URL for issuing certificate
10319274 2015-10-12 08:12:29 2018-01-12 08:12:28 x509lintWARNINGPolicy information has qualifier other than CPS URI
x509lintWARNINGUnknown extended key usage
x509lintINFOSubject has a deprecated CommonName
x509lintINFOUnknown validation policy
zlintERRORSubscriber Certificate: authorityInformationAccess MUST contain the HTTP URL of the Issuing CA's OSCP responder.
zlintERRORSubscriber certificate cRLDistributionPoints extension must contain the HTTP URL of the CA's CRL service
zlintERRORSubscriber Certificate: authorityInformationAccess MUST be present, with the exception of stapling.
zlintWARNINGCompliant certificates should use the utf8string encoding for explicitText
zlintWARNINGSubscriber Certificate: extKeyUsage either the value id-kp-serverAuth or id-kp-clientAuth or both values MUST be present.
zlintWARNINGSubscriber certificates authorityInformationAccess extension should contain the HTTP URL of the issuing CA's certificate
zlintNOTICESubscriber Certificate: commonName is deprecated.

cablintERRORBR certificates with organizationName must include either localityName or stateOrProvinceName
cablintWARNINGCertificate does not include authorityInformationAccess. BRs require OCSP stapling for this certificate.
cablintWARNINGDeprecated Netscape extension 2.16.840.1.113730.1.1 treated as opaque extension
cablintWARNINGTLS Server auth certificates should not contain Netscape Server Gated Crypto usage
cablintINFOTLS Server certificate identified
x509lintERRORError parsing URL
x509lintERRORno authorityInformationAccess extension
x509lintERRORNo OCSP over HTTP
x509lintERRORSubject with organizationName, givenName or surname but without stateOrProvince or localityName
x509lintWARNINGexplicitText is not using a UTF8String
x509lintWARNINGNo HTTP URL for issuing certificate
10845801 2015-11-05 01:05:42 2018-02-05 01:05:41 x509lintWARNINGPolicy information has qualifier other than CPS URI
x509lintWARNINGUnknown extended key usage
x509lintINFOSubject has a deprecated CommonName
x509lintINFOUnknown validation policy
zlintERRORSubscriber Certificate: authorityInformationAccess MUST contain the HTTP URL of the Issuing CA's OSCP responder.
zlintERRORSubscriber certificate cRLDistributionPoints extension must contain the HTTP URL of the CA's CRL service
zlintERRORSubscriber Certificate: authorityInformationAccess MUST be present, with the exception of stapling.
zlintWARNINGCompliant certificates should use the utf8string encoding for explicitText
zlintWARNINGSubscriber Certificate: extKeyUsage either the value id-kp-serverAuth or id-kp-clientAuth or both values MUST be present.
zlintWARNINGSubscriber certificates authorityInformationAccess extension should contain the HTTP URL of the issuing CA's certificate
zlintNOTICESubscriber Certificate: commonName is deprecated.

cablintERRORBR certificates with organizationName must include either localityName or stateOrProvinceName
cablintWARNINGCertificate does not include authorityInformationAccess. BRs require OCSP stapling for this certificate.
cablintWARNINGDeprecated Netscape extension 2.16.840.1.113730.1.1 treated as opaque extension
cablintWARNINGTLS Server auth certificates should not contain Netscape Server Gated Crypto usage
cablintINFOTLS Server certificate identified
x509lintERRORError parsing URL
x509lintERRORno authorityInformationAccess extension
x509lintERRORNo OCSP over HTTP
x509lintERRORSubject with organizationName, givenName or surname but without stateOrProvince or localityName
x509lintWARNINGexplicitText is not using a UTF8String
x509lintWARNINGNo HTTP URL for issuing certificate
9357721 2015-09-16 05:03:25 2017-12-16 05:03:24 x509lintWARNINGPolicy information has qualifier other than CPS URI
x509lintWARNINGUnknown extended key usage
x509lintINFOSubject has a deprecated CommonName
x509lintINFOUnknown validation policy
zlintERRORSubscriber Certificate: authorityInformationAccess MUST contain the HTTP URL of the Issuing CA's OSCP responder.
zlintERRORSubscriber certificate cRLDistributionPoints extension must contain the HTTP URL of the CA's CRL service
zlintERRORSubscriber Certificate: authorityInformationAccess MUST be present, with the exception of stapling.
zlintWARNINGCompliant certificates should use the utf8string encoding for explicitText
zlintWARNINGSubscriber Certificate: extKeyUsage either the value id-kp-serverAuth or id-kp-clientAuth or both values MUST be present.
zlintWARNINGSubscriber certificates authorityInformationAccess extension should contain the HTTP URL of the issuing CA's certificate
zlintNOTICESubscriber Certificate: commonName is deprecated.

cablintERRORBR certificates with organizationName must include either localityName or stateOrProvinceName
cablintWARNINGCertificate does not include authorityInformationAccess. BRs require OCSP stapling for this certificate.
cablintWARNINGDeprecated Netscape extension 2.16.840.1.113730.1.1 treated as opaque extension
cablintWARNINGTLS Server auth certificates should not contain Netscape Server Gated Crypto usage
cablintINFOTLS Server certificate identified
x509lintERRORError parsing URL
x509lintERRORno authorityInformationAccess extension
x509lintERRORNo OCSP over HTTP
x509lintERRORSubject with organizationName, givenName or surname but without stateOrProvince or localityName
x509lintWARNINGexplicitText is not using a UTF8String
x509lintWARNINGNo HTTP URL for issuing certificate
10941516 2015-11-27 01:37:56 2018-02-27 01:37:55 x509lintWARNINGPolicy information has qualifier other than CPS URI
x509lintWARNINGUnknown extended key usage
x509lintINFOSubject has a deprecated CommonName
x509lintINFOUnknown validation policy
zlintERRORSubscriber Certificate: authorityInformationAccess MUST contain the HTTP URL of the Issuing CA's OSCP responder.
zlintERRORSubscriber certificate cRLDistributionPoints extension must contain the HTTP URL of the CA's CRL service
zlintERRORSubscriber Certificate: authorityInformationAccess MUST be present, with the exception of stapling.
zlintWARNINGCompliant certificates should use the utf8string encoding for explicitText
zlintWARNINGSubscriber Certificate: extKeyUsage either the value id-kp-serverAuth or id-kp-clientAuth or both values MUST be present.
zlintWARNINGSubscriber certificates authorityInformationAccess extension should contain the HTTP URL of the issuing CA's certificate
zlintNOTICESubscriber Certificate: commonName is deprecated.

cablintERRORBR certificates with CRL Distribution Point must include HTTP URL
cablintERRORBR certificates with organizationName must include either localityName or stateOrProvinceName
cablintERRORUnknown TLD in SAN
cablintWARNINGCertificate does not include authorityInformationAccess. BRs require OCSP stapling for this certificate.
cablintWARNINGDeprecated Netscape extension 2.16.840.1.113730.1.1 treated as opaque extension
cablintWARNINGTLS Server auth certificates should not contain Netscape Server Gated Crypto usage
cablintINFOTLS Server certificate identified
x509lintERRORError parsing URL
x509lintERRORIP address in dns name
x509lintERRORno authorityInformationAccess extension
x509lintERRORNo OCSP over HTTP
x509lintERRORSubject with organizationName, givenName or surname but without stateOrProvince or localityName
284285505 2015-10-15 01:57:53 2018-01-15 01:57:52 x509lintWARNINGexplicitText is not using a UTF8String
x509lintWARNINGNo HTTP URL for issuing certificate
x509lintWARNINGPolicy information has qualifier other than CPS URI
x509lintWARNINGUnknown extended key usage
x509lintINFOSubject has a deprecated CommonName
x509lintINFOUnknown validation policy
zlintERRORDNSNames must have a valid TLD.
zlintERRORSubscriber Certificate: authorityInformationAccess MUST contain the HTTP URL of the Issuing CA's OSCP responder.
zlintERRORSubscriber certificate cRLDistributionPoints extension must contain the HTTP URL of the CA's CRL service
zlintERRORSubscriber Certificate: authorityInformationAccess MUST be present, with the exception of stapling.
zlintWARNINGCompliant certificates should use the utf8string encoding for explicitText
zlintWARNINGSubscriber Certificate: extKeyUsage either the value id-kp-serverAuth or id-kp-clientAuth or both values MUST be present

cablintERRORBR certificates with organizationName must include either localityName or stateOrProvinceName
cablintWARNINGCertificate does not include authorityInformationAccess. BRs require OCSP stapling for this certificate.
cablintWARNINGDeprecated Netscape extension 2.16.840.1.113730.1.1 treated as opaque extension
cablintWARNINGTLS Server auth certificates should not contain Netscape Server Gated Crypto usage
cablintINFOTLS Server certificate identified
x509lintERRORError parsing URL
x509lintERRORno authorityInformationAccess extension
x509lintERRORNo OCSP over HTTP
x509lintERRORSubject with organizationName, givenName or surname but without stateOrProvince or localityName
x509lintWARNINGexplicitText is not using a UTF8String
x509lintWARNINGNo HTTP URL for issuing certificate
9171226 2015-09-02 06:54:25 2017-12-02 06:54:24 x509lintWARNINGPolicy information has qualifier other than CPS URI
x509lintWARNINGUnknown extended key usage
x509lintINFOSubject has a deprecated CommonName
x509lintINFOUnknown validation policy
zlintERRORSubscriber Certificate: authorityInformationAccess MUST contain the HTTP URL of the Issuing CA's OSCP responder.
zlintERRORSubscriber certificate cRLDistributionPoints extension must contain the HTTP URL of the CA's CRL service
zlintERRORSubscriber Certificate: authorityInformationAccess MUST be present, with the exception of stapling.
zlintWARNINGCompliant certificates should use the utf8string encoding for explicitText
zlintWARNINGSubscriber Certificate: extKeyUsage either the value id-kp-serverAuth or id-kp-clientAuth or both values MUST be present.
zlintWARNINGSubscriber certificates authorityInformationAccess extension should contain the HTTP URL of the issuing CA's certificate
zlintNOTICESubscriber Certificate: commonName is deprecated.

cablintERRORBR certificates with organizationName must include either localityName or stateOrProvinceName
cablintWARNINGCertificate does not include authorityInformationAccess. BRs require OCSP stapling for this certificate.
cablintWARNINGDeprecated Netscape extension 2.16.840.1.113730.1.1 treated as opaque extension
cablintWARNINGTLS Server auth certificates should not contain Netscape Server Gated Crypto usage
cablintINFOTLS Server certificate identified
x509lintERRORError parsing URL
x509lintERRORno authorityInformationAccess extension
x509lintERRORNo OCSP over HTTP
x509lintERRORSubject with organizationName, givenName or surname but without stateOrProvince or localityName
x509lintWARNINGexplicitText is not using a UTF8String
x509lintWARNINGNo HTTP URL for issuing certificate
9378807 2015-09-11 02:03:24 2017-12-11 02:03:23 x509lintWARNINGPolicy information has qualifier other than CPS URI
x509lintWARNINGUnknown extended key usage
x509lintINFOSubject has a deprecated CommonName
x509lintINFOUnknown validation policy
zlintERRORSubscriber Certificate: authorityInformationAccess MUST contain the HTTP URL of the Issuing CA's OSCP responder.
zlintERRORSubscriber certificate cRLDistributionPoints extension must contain the HTTP URL of the CA's CRL service
zlintERRORSubscriber Certificate: authorityInformationAccess MUST be present, with the exception of stapling.
zlintWARNINGCompliant certificates should use the utf8string encoding for explicitText
zlintWARNINGSubscriber Certificate: extKeyUsage either the value id-kp-serverAuth or id-kp-clientAuth or both values MUST be present.
zlintWARNINGSubscriber certificates authorityInformationAccess extension should contain the HTTP URL of the issuing CA's certificate
zlintNOTICESubscriber Certificate: commonName is deprecated.

cablintERRORBR certificates with organizationName must include either localityName or stateOrProvinceName
cablintWARNINGCertificate does not include authorityInformationAccess. BRs require OCSP stapling for this certificate.
cablintWARNINGDeprecated Netscape extension 2.16.840.1.113730.1.1 treated as opaque extension
cablintWARNINGTLS Server auth certificates should not contain Netscape Server Gated Crypto usage
cablintINFOTLS Server certificate identified
x509lintERRORError parsing URL
x509lintERRORno authorityInformationAccess extension
x509lintERRORNo OCSP over HTTP
x509lintERRORSubject with organizationName, givenName or surname but without stateOrProvince or localityName
x509lintWARNINGexplicitText is not using a UTF8String
x509lintWARNINGNo HTTP URL for issuing certificate
31712033 2015-09-21 02:14:28 2017-12-21 02:14:27 x509lintWARNINGPolicy information has qualifier other than CPS URI
x509lintWARNINGUnknown extended key usage
x509lintINFOSubject has a deprecated CommonName
x509lintINFOUnknown validation policy
zlintERRORSubscriber Certificate: authorityInformationAccess MUST contain the HTTP URL of the Issuing CA's OSCP responder.
zlintERRORSubscriber certificate cRLDistributionPoints extension must contain the HTTP URL of the CA's CRL service
zlintERRORSubscriber Certificate: authorityInformationAccess MUST be present, with the exception of stapling.
zlintWARNINGCompliant certificates should use the utf8string encoding for explicitText
zlintWARNINGSubscriber Certificate: extKeyUsage either the value id-kp-serverAuth or id-kp-clientAuth or both values MUST be present.
zlintWARNINGSubscriber certificates authorityInformationAccess extension should contain the HTTP URL of the issuing CA's certificate
zlintNOTICESubscriber Certificate: commonName is deprecated.

cablintERRORBR certificates with CRL Distribution Point must include HTTP URL
cablintERRORBR certificates with organizationName must include either localityName or stateOrProvinceName
cablintWARNINGCertificate does not include authorityInformationAccess. BRs require OCSP stapling for this certificate.
cablintWARNINGDeprecated Netscape extension 2.16.840.1.113730.1.1 treated as opaque extension
cablintWARNINGName has multiple commonName attributes
cablintWARNINGTLS Server auth certificates should not contain Netscape Server Gated Crypto usage
cablintINFOTLS Server certificate identified
x509lintERRORError parsing URL
x509lintERRORno authorityInformationAccess extension
x509lintERRORNo OCSP over HTTP
x509lintERRORSubject with organizationName, givenName or surname but without stateOrProvince or localityName
x509lintWARNINGexplicitText is not using a UTF8String
13928815 2015-10-22 09:06:11 2018-01-22 09:06:10 x509lintWARNINGNo HTTP URL for issuing certificate
x509lintWARNINGPolicy information has qualifier other than CPS URI
x509lintWARNINGUnknown extended key usage
x509lintINFOSubject has a deprecated CommonName
x509lintINFOUnknown validation policy
zlintERRORSubscriber Certificate: authorityInformationAccess MUST contain the HTTP URL of the Issuing CA's OSCP responder.
zlintERRORSubscriber certificate cRLDistributionPoints extension must contain the HTTP URL of the CA's CRL service
zlintERRORSubscriber Certificate: authorityInformationAccess MUST be present, with the exception of stapling.
zlintWARNINGCompliant certificates should use the utf8string encoding for explicitText
zlintWARNINGSubscriber Certificate: extKeyUsage either the value id-kp-serverAuth or id-kp-clientAuth or both values MUST be present.
zlintWARNINGSubscriber certificates authorityInformationAccess extension should contain the HTTP URL of the issuing CA's certificate

cablintERRORBR certificates with organizationName must include either localityName or stateOrProvinceName
cablintWARNINGCertificate does not include authorityInformationAccess. BRs require OCSP stapling for this certificate.
cablintWARNINGDeprecated Netscape extension 2.16.840.1.113730.1.1 treated as opaque extension
cablintWARNINGTLS Server auth certificates should not contain Netscape Server Gated Crypto usage
cablintINFOTLS Server certificate identified
x509lintERRORError parsing URL
x509lintERRORno authorityInformationAccess extension
x509lintERRORNo OCSP over HTTP
x509lintERRORSubject with organizationName, givenName or surname but without stateOrProvince or localityName
x509lintWARNINGexplicitText is not using a UTF8String
x509lintWARNINGNo HTTP URL for issuing certificate
10399956 2015-10-28 09:17:00 2018-01-28 09:16:59 x509lintWARNINGPolicy information has qualifier other than CPS URI
x509lintWARNINGUnknown extended key usage
x509lintINFOSubject has a deprecated CommonName
x509lintINFOUnknown validation policy
zlintERRORSubscriber Certificate: authorityInformationAccess MUST contain the HTTP URL of the Issuing CA's OSCP responder.
zlintERRORSubscriber certificate cRLDistributionPoints extension must contain the HTTP URL of the CA's CRL service
zlintERRORSubscriber Certificate: authorityInformationAccess MUST be present, with the exception of stapling.
zlintWARNINGCompliant certificates should use the utf8string encoding for explicitText
zlintWARNINGSubscriber Certificate: extKeyUsage either the value id-kp-serverAuth or id-kp-clientAuth or both values MUST be present.
zlintWARNINGSubscriber certificates authorityInformationAccess extension should contain the HTTP URL of the issuing CA's certificate
zlintNOTICESubscriber Certificate: commonName is deprecated.

cablintERRORBR certificates with organizationName must include either localityName or stateOrProvinceName
cablintWARNINGCertificate does not include authorityInformationAccess. BRs require OCSP stapling for this certificate.
cablintWARNINGDeprecated Netscape extension 2.16.840.1.113730.1.1 treated as opaque extension
cablintWARNINGTLS Server auth certificates should not contain Netscape Server Gated Crypto usage
cablintINFOTLS Server certificate identified
x509lintERRORError parsing URL
x509lintERRORno authorityInformationAccess extension
x509lintERRORNo OCSP over HTTP
x509lintERRORSubject with organizationName, givenName or surname but without stateOrProvince or localityName
x509lintWARNINGexplicitText is not using a UTF8String
x509lintWARNINGNo HTTP URL for issuing certificate
10276014 2015-10-20 00:29:45 2018-01-20 00:29:44 x509lintWARNINGPolicy information has qualifier other than CPS URI
x509lintWARNINGUnknown extended key usage
x509lintINFOSubject has a deprecated CommonName
x509lintINFOUnknown validation policy
zlintERRORSubscriber Certificate: authorityInformationAccess MUST contain the HTTP URL of the Issuing CA's OSCP responder.
zlintERRORSubscriber certificate cRLDistributionPoints extension must contain the HTTP URL of the CA's CRL service
zlintERRORSubscriber Certificate: authorityInformationAccess MUST be present, with the exception of stapling.
zlintWARNINGCompliant certificates should use the utf8string encoding for explicitText
zlintWARNINGSubscriber Certificate: extKeyUsage either the value id-kp-serverAuth or id-kp-clientAuth or both values MUST be present.
zlintWARNINGSubscriber certificates authorityInformationAccess extension should contain the HTTP URL of the issuing CA's certificate
zlintNOTICESubscriber Certificate: commonName is deprecated.

cablintERRORBR certificates with organizationName must include either localityName or stateOrProvinceName
cablintWARNINGCertificate does not include authorityInformationAccess. BRs require OCSP stapling for this certificate.
cablintWARNINGDeprecated Netscape extension 2.16.840.1.113730.1.1 treated as opaque extension
cablintWARNINGTLS Server auth certificates should not contain Netscape Server Gated Crypto usage
cablintINFOTLS Server certificate identified
x509lintERRORError parsing URL
x509lintERRORno authorityInformationAccess extension
x509lintERRORNo OCSP over HTTP
x509lintERRORSubject with organizationName, givenName or surname but without stateOrProvince or localityName
x509lintWARNINGexplicitText is not using a UTF8String
x509lintWARNINGNo HTTP URL for issuing certificate
14048263 2015-10-08 07:40:00 2018-01-08 07:39:59 x509lintWARNINGPolicy information has qualifier other than CPS URI
x509lintWARNINGUnknown extended key usage
x509lintINFOSubject has a deprecated CommonName
x509lintINFOUnknown validation policy
zlintERRORSubscriber Certificate: authorityInformationAccess MUST contain the HTTP URL of the Issuing CA's OSCP responder.
zlintERRORSubscriber certificate cRLDistributionPoints extension must contain the HTTP URL of the CA's CRL service
zlintERRORSubscriber Certificate: authorityInformationAccess MUST be present, with the exception of stapling.
zlintWARNINGCompliant certificates should use the utf8string encoding for explicitText
zlintWARNINGSubscriber Certificate: extKeyUsage either the value id-kp-serverAuth or id-kp-clientAuth or both values MUST be present.
zlintWARNINGSubscriber certificates authorityInformationAccess extension should contain the HTTP URL of the issuing CA's certificate
zlintNOTICESubscriber Certificate: commonName is deprecated.

cablintERRORBR certificates with organizationName must include either localityName or stateOrProvinceName
cablintWARNINGCertificate does not include authorityInformationAccess. BRs require OCSP stapling for this certificate.
cablintWARNINGDeprecated Netscape extension 2.16.840.1.113730.1.1 treated as opaque extension
cablintWARNINGTLS Server auth certificates should not contain Netscape Server Gated Crypto usage
cablintINFOTLS Server certificate identified
x509lintERRORError parsing URL
x509lintERRORno authorityInformationAccess extension
x509lintERRORNo OCSP over HTTP
x509lintERRORSubject with organizationName, givenName or surname but without stateOrProvince or localityName
x509lintWARNINGexplicitText is not using a UTF8String
x509lintWARNINGNo HTTP URL for issuing certificate
9209549 2015-09-01 04:07:12 2017-12-01 04:07:11 x509lintWARNINGPolicy information has qualifier other than CPS URI
x509lintWARNINGUnknown extended key usage
x509lintINFOSubject has a deprecated CommonName
x509lintINFOUnknown validation policy
zlintERRORSubscriber Certificate: authorityInformationAccess MUST contain the HTTP URL of the Issuing CA's OSCP responder.
zlintERRORSubscriber certificate cRLDistributionPoints extension must contain the HTTP URL of the CA's CRL service
zlintERRORSubscriber Certificate: authorityInformationAccess MUST be present, with the exception of stapling.
zlintWARNINGCompliant certificates should use the utf8string encoding for explicitText
zlintWARNINGSubscriber Certificate: extKeyUsage either the value id-kp-serverAuth or id-kp-clientAuth or both values MUST be present.
zlintWARNINGSubscriber certificates authorityInformationAccess extension should contain the HTTP URL of the issuing CA's certificate
zlintNOTICESubscriber Certificate: commonName is deprecated.

cablintERRORBR certificates with organizationName must include either localityName or stateOrProvinceName
cablintWARNINGCertificate does not include authorityInformationAccess. BRs require OCSP stapling for this certificate.
cablintWARNINGDeprecated Netscape extension 2.16.840.1.113730.1.1 treated as opaque extension
cablintWARNINGTLS Server auth certificates should not contain Netscape Server Gated Crypto usage
cablintINFOTLS Server certificate identified
x509lintERRORError parsing URL
x509lintERRORno authorityInformationAccess extension
x509lintERRORNo OCSP over HTTP
x509lintERRORSubject with organizationName, givenName or surname but without stateOrProvince or localityName
x509lintWARNINGexplicitText is not using a UTF8String
x509lintWARNINGNo HTTP URL for issuing certificate
10681096 2015-11-10 06:48:33 2018-02-10 06:48:32 x509lintWARNINGPolicy information has qualifier other than CPS URI
x509lintWARNINGUnknown extended key usage
x509lintINFOSubject has a deprecated CommonName
x509lintINFOUnknown validation policy
zlintERRORSubscriber Certificate: authorityInformationAccess MUST contain the HTTP URL of the Issuing CA's OSCP responder.
zlintERRORSubscriber certificate cRLDistributionPoints extension must contain the HTTP URL of the CA's CRL service
zlintERRORSubscriber Certificate: authorityInformationAccess MUST be present, with the exception of stapling.
zlintWARNINGCompliant certificates should use the utf8string encoding for explicitText
zlintWARNINGSubscriber Certificate: extKeyUsage either the value id-kp-serverAuth or id-kp-clientAuth or both values MUST be present.
zlintWARNINGSubscriber certificates authorityInformationAccess extension should contain the HTTP URL of the issuing CA's CRL service
certificate
zlintNOTICESubscriber Certificate: commonName is deprecated.

cablintERRORBR certificates with organizationName must include either localityName or stateOrProvinceName
cablintWARNINGCertificate does not include authorityInformationAccess. BRs require OCSP stapling for this certificate.
cablintWARNINGDeprecated Netscape extension 2.16.840.1.113730.1.1 treated as opaque extension
cablintWARNINGTLS Server auth certificates should not contain Netscape Server Gated Crypto usage
cablintINFOTLS Server certificate identified
x509lintERRORError parsing URL
x509lintERRORno authorityInformationAccess extension
x509lintERRORNo OCSP over HTTP
x509lintERRORSubject with organizationName, givenName or surname but without stateOrProvince or localityName
x509lintWARNINGexplicitText is not using a UTF8String
x509lintWARNINGNo HTTP URL for issuing certificate
10779459 2015-11-16 01:32:50 2018-02-16 01:32:49 x509lintWARNINGPolicy information has qualifier other than CPS URI
x509lintWARNINGUnknown extended key usage
x509lintINFOSubject has a deprecated CommonName
x509lintINFOUnknown validation policy
zlintERRORSubscriber Certificate: authorityInformationAccess MUST contain the HTTP URL of the Issuing CA's OSCP responder.
zlintERRORSubscriber certificate cRLDistributionPoints extension must contain the HTTP URL of the CA's CRL service
zlintERRORSubscriber Certificate: authorityInformationAccess MUST be present, with the exception of stapling.
zlintWARNINGCompliant certificates should use the utf8string encoding for explicitText
zlintWARNINGSubscriber Certificate: extKeyUsage either the value id-kp-serverAuth or id-kp-clientAuth or both values MUST be present.
zlintWARNINGSubscriber certificates authorityInformationAccess extension should contain the HTTP URL of the issuing CA's certificate
zlintNOTICESubscriber Certificate: commonName is deprecated.

cablintERRORBR certificates with organizationName must include either localityName or stateOrProvinceName
cablintWARNINGCertificate does not include authorityInformationAccess. BRs require OCSP stapling for this certificate.
cablintWARNINGDeprecated Netscape extension 2.16.840.1.113730.1.1 treated as opaque extension
cablintWARNINGTLS Server auth certificates should not contain Netscape Server Gated Crypto usage
cablintINFOTLS Server certificate identified
x509lintERRORError parsing URL
x509lintERRORno authorityInformationAccess extension
x509lintERRORNo OCSP over HTTP
x509lintERRORSubject with organizationName, givenName or surname but without stateOrProvince or localityName
x509lintWARNINGexplicitText is not using a UTF8String
x509lintWARNINGNo HTTP URL for issuing certificate
9356449 2015-09-05 00:58:18 2017-12-05 00:58:17 x509lintWARNINGPolicy information has qualifier other than CPS URI
x509lintWARNINGUnknown extended key usage
x509lintINFOSubject has a deprecated CommonName
x509lintINFOUnknown validation policy
zlintERRORSubscriber Certificate: authorityInformationAccess MUST contain the HTTP URL of the Issuing CA's OSCP responder.
zlintERRORSubscriber certificate cRLDistributionPoints extension must contain the HTTP URL of the CA's CRL service
zlintERRORSubscriber Certificate: authorityInformationAccess MUST be present, with the exception of stapling.
zlintWARNINGCompliant certificates should use the utf8string encoding for explicitText
zlintWARNINGSubscriber Certificate: extKeyUsage either the value id-kp-serverAuth or id-kp-clientAuth or both values MUST be present.
zlintWARNINGSubscriber certificates authorityInformationAccess extension should contain the HTTP URL of the issuing CA's certificate
zlintNOTICESubscriber Certificate: commonName is deprecated.

cablintERRORBR certificates with organizationName must include either localityName or stateOrProvinceName
cablintWARNINGCertificate does not include authorityInformationAccess. BRs require OCSP stapling for this certificate.
cablintWARNINGDeprecated Netscape extension 2.16.840.1.113730.1.1 treated as opaque extension
cablintWARNINGTLS Server auth certificates should not contain Netscape Server Gated Crypto usage
cablintINFOTLS Server certificate identified
x509lintERRORError parsing URL
x509lintERRORno authorityInformationAccess extension
x509lintERRORNo OCSP over HTTP
x509lintERRORSubject with organizationName, givenName or surname but without stateOrProvince or localityName
x509lintWARNINGexplicitText is not using a UTF8String
x509lintWARNINGNo HTTP URL for issuing certificate
14965021 2015-11-20 05:25:12 2018-02-20 05:25:11 x509lintWARNINGPolicy information has qualifier other than CPS URI
x509lintWARNINGUnknown extended key usage
x509lintINFOSubject has a deprecated CommonName
x509lintINFOUnknown validation policy
zlintERRORSubscriber Certificate: authorityInformationAccess MUST contain the HTTP URL of the Issuing CA's OSCP responder.
zlintERRORSubscriber certificate cRLDistributionPoints extension must contain the HTTP URL of the CA's CRL service
zlintERRORSubscriber Certificate: authorityInformationAccess MUST be present, with the exception of stapling.
zlintWARNINGCompliant certificates should use the utf8string encoding for explicitText
zlintWARNINGSubscriber Certificate: extKeyUsage either the value id-kp-serverAuth or id-kp-clientAuth or both values MUST be present.
zlintWARNINGSubscriber certificates authorityInformationAccess extension should contain the HTTP URL of the issuing CA's certificate
zlintNOTICESubscriber Certificate: commonName is deprecated.

cablintERRORBR certificates with organizationName must include either localityName or stateOrProvinceName
cablintWARNINGCertificate does not include authorityInformationAccess. BRs require OCSP stapling for this certificate.
cablintWARNINGDeprecated Netscape extension 2.16.840.1.113730.1.1 treated as opaque extension
cablintWARNINGTLS Server auth certificates should not contain Netscape Server Gated Crypto usage
cablintINFOTLS Server certificate identified
x509lintERRORError parsing URL
x509lintERRORno authorityInformationAccess extension
x509lintERRORNo OCSP over HTTP
x509lintERRORSubject with organizationName, givenName or surname but without stateOrProvince or localityName
x509lintWARNINGexplicitText is not using a UTF8String
x509lintWARNINGNo HTTP URL for issuing certificate
9671727 2015-09-30 06:48:39 2017-12-30 06:48:38 x509lintWARNINGPolicy information has qualifier other than CPS URI
x509lintWARNINGUnknown extended key usage
x509lintINFOSubject has a deprecated CommonName
x509lintINFOUnknown validation policy
zlintERRORSubscriber Certificate: authorityInformationAccess MUST contain the HTTP URL of the Issuing CA's OSCP responder.
zlintERRORSubscriber certificate cRLDistributionPoints extension must contain the HTTP URL of the CA's CRL service
zlintERRORSubscriber Certificate: authorityInformationAccess MUST be present, with the exception of stapling.
zlintWARNINGCompliant certificates should use the utf8string encoding for explicitText
zlintWARNINGSubscriber Certificate: extKeyUsage either the value id-kp-serverAuth or id-kp-clientAuth or both values MUST be present.
zlintWARNINGSubscriber certificates authorityInformationAccess extension should contain the HTTP URL of the issuing CA's certificate
zlintNOTICESubscriber Certificate: commonName is deprecated.

cablintERRORBR certificates with organizationName must include either localityName or stateOrProvinceName
cablintWARNINGCertificate does not include authorityInformationAccess. BRs require OCSP stapling for this certificate.
cablintWARNINGDeprecated Netscape extension 2.16.840.1.113730.1.1 treated as opaque extension
cablintWARNINGTLS Server auth certificates should not contain Netscape Server Gated Crypto usage
cablintINFOTLS Server certificate identified
x509lintERRORError parsing URL
x509lintERRORno authorityInformationAccess extension
x509lintERRORNo OCSP over HTTP
x509lintERRORSubject with organizationName, givenName or surname but without stateOrProvince or localityName
x509lintWARNINGexplicitText is not using a UTF8String
x509lintWARNINGNo HTTP URL for issuing certificate
10307491 2015-10-16 08:54:05 2018-01-16 08:54:04 x509lintWARNINGPolicy information has qualifier other than CPS URI
x509lintWARNINGUnknown extended key usage
x509lintINFOSubject has a deprecated CommonName
x509lintINFOUnknown validation policy
zlintERRORSubscriber Certificate: authorityInformationAccess MUST contain the HTTP URL of the Issuing CA's OSCP responder.
zlintERRORSubscriber certificate cRLDistributionPoints extension must contain the HTTP URL of the CA's CRL service
zlintERRORSubscriber Certificate: authorityInformationAccess MUST be present, with the exception of stapling.
zlintWARNINGCompliant certificates should use the utf8string encoding for explicitText
zlintWARNINGSubscriber Certificate: extKeyUsage either the value id-kp-serverAuth or id-kp-clientAuth or both values MUST be present.
zlintWARNINGSubscriber certificates authorityInformationAccess extension should contain the HTTP URL of the issuing CA's certificate
zlintNOTICESubscriber Certificate: commonName is deprecated.

cablintERRORBR certificates with organizationName must include either localityName or stateOrProvinceName
cablintWARNINGCertificate does not include authorityInformationAccess. BRs require OCSP stapling for this certificate.
cablintWARNINGDeprecated Netscape extension 2.16.840.1.113730.1.1 treated as opaque extension
cablintWARNINGTLS Server auth certificates should not contain Netscape Server Gated Crypto usage
cablintINFOTLS Server certificate identified
x509lintERRORError parsing URL
x509lintERRORno authorityInformationAccess extension
x509lintERRORNo OCSP over HTTP
x509lintERRORSubject with organizationName, givenName or surname but without stateOrProvince or localityName
x509lintWARNINGexplicitText is not using a UTF8String
x509lintWARNINGNo HTTP URL for issuing certificate
9133820 2015-09-01 02:10:29 2017-12-01 02:10:28 x509lintWARNINGPolicy information has qualifier other than CPS URI
x509lintWARNINGUnknown extended key usage
x509lintINFOSubject has a deprecated CommonName
x509lintINFOUnknown validation policy
zlintERRORSubscriber Certificate: authorityInformationAccess MUST contain the HTTP URL of the Issuing CA's OSCP responder.
zlintERRORSubscriber certificate cRLDistributionPoints extension must contain the HTTP URL of the CA's CRL service
zlintERRORSubscriber Certificate: authorityInformationAccess MUST be present, with the exception of stapling.
zlintWARNINGCompliant certificates should use the utf8string encoding for explicitText
zlintWARNINGSubscriber Certificate: extKeyUsage either the value id-kp-serverAuth or id-kp-clientAuth or both values MUST be present.
zlintWARNINGSubscriber certificates authorityInformationAccess extension should contain the HTTP URL of the issuing CA's certificate
zlintNOTICESubscriber Certificate: commonName is deprecated.

cablintERRORBR certificates with organizationName must include either localityName or stateOrProvinceName
cablintWARNINGCertificate does not include authorityInformationAccess. BRs require OCSP stapling for this certificate.
cablintWARNINGDeprecated Netscape extension 2.16.840.1.113730.1.1 treated as opaque extension
cablintWARNINGTLS Server auth certificates should not contain Netscape Server Gated Crypto usage
cablintINFOTLS Server certificate identified
x509lintERRORError parsing URL
x509lintERRORno authorityInformationAccess extension
x509lintERRORNo OCSP over HTTP
x509lintERRORSubject with organizationName, givenName or surname but without stateOrProvince or localityName
x509lintWARNINGexplicitText is not using a UTF8String
x509lintWARNINGNo HTTP URL for issuing certificate
10156791 2015-10-13 06:14:51 2018-01-13 06:14:50 x509lintWARNINGPolicy information has qualifier other than CPS URI
x509lintWARNINGUnknown extended key usage
x509lintINFOSubject has a deprecated CommonName
x509lintINFOUnknown validation policy
zlintERRORSubscriber Certificate: authorityInformationAccess MUST contain the HTTP URL of the Issuing CA's OSCP responder.
zlintERRORSubscriber certificate cRLDistributionPoints extension must contain the HTTP URL of the CA's CRL service
zlintERRORSubscriber Certificate: authorityInformationAccess MUST be present, with the exception of stapling.
zlintWARNINGCompliant certificates should use the utf8string encoding for explicitText
zlintWARNINGSubscriber Certificate: extKeyUsage either the value id-kp-serverAuth or id-kp-clientAuth or both values MUST be present.
zlintWARNINGSubscriber certificates authorityInformationAccess extension should contain the HTTP URL of the issuing CA's certificate
zlintNOTICESubscriber Certificate: commonName is deprecated.

cablintERRORBR certificates with organizationName must include either localityName or stateOrProvinceName
cablintWARNINGCertificate does not include authorityInformationAccess. BRs require OCSP stapling for this certificate.
cablintWARNINGDeprecated Netscape extension 2.16.840.1.113730.1.1 treated as opaque extension
cablintWARNINGTLS Server auth certificates should not contain Netscape Server Gated Crypto usage
cablintINFOTLS Server certificate identified
x509lintERRORError parsing URL
x509lintERRORno authorityInformationAccess extension
x509lintERRORNo OCSP over HTTP
x509lintERRORSubject with organizationName, givenName or surname but without stateOrProvince or localityName
x509lintWARNINGexplicitText is not using a UTF8String
x509lintWARNINGNo HTTP URL for issuing certificate
10960037 2015-11-27 04:54:35 2018-02-27 04:54:34 x509lintWARNINGPolicy information has qualifier other than CPS URI
x509lintWARNINGUnknown extended key usage
x509lintINFOSubject has a deprecated CommonName
x509lintINFOUnknown validation policy
zlintERRORSubscriber Certificate: authorityInformationAccess MUST contain the HTTP URL of the Issuing CA's OSCP responder.
zlintERRORSubscriber certificate cRLDistributionPoints extension must contain the HTTP URL of the CA's CRL service
zlintERRORSubscriber Certificate: authorityInformationAccess MUST be present, with the exception of stapling.
zlintWARNINGCompliant certificates should use the utf8string encoding for explicitText
zlintWARNINGSubscriber Certificate: extKeyUsage either the value id-kp-serverAuth or id-kp-clientAuth or both values MUST be present.
zlintWARNINGSubscriber certificates authorityInformationAccess extension should contain the HTTP URL of the issuing CA's certificate
zlintNOTICESubscriber Certificate: commonName is deprecated.

cablintERRORBR certificates with CRL Distribution Point must include HTTP URL
cablintERRORBR certificates with organizationName must include either localityName or stateOrProvinceName
cablintERRORUnknown TLD in SAN
cablintWARNINGCertificate does not include authorityInformationAccess. BRs require OCSP stapling for this certificate.
cablintWARNINGDeprecated Netscape extension 2.16.840.1.113730.1.1 treated as opaque extension
cablintWARNINGTLS Server auth certificates should not contain Netscape Server Gated Crypto usage
cablintINFOTLS Server certificate identified
x509lintERRORError parsing URL
x509lintERRORIP address in dns name
x509lintERRORno authorityInformationAccess extension
x509lintERRORNo OCSP over HTTP
x509lintERRORSubject with organizationName, givenName or surname but without stateOrProvince or localityName
284163158 2015-10-16 02:06:16 2018-01-16 02:06:15 x509lintWARNINGexplicitText is not using a UTF8String
x509lintWARNINGNo HTTP URL for issuing certificate
x509lintWARNINGPolicy information has qualifier other than CPS URI
x509lintWARNINGUnknown extended key usage
x509lintINFOSubject has a deprecated CommonName
x509lintINFOUnknown validation policy
zlintERRORDNSNames must have a valid TLD.
zlintERRORSubscriber Certificate: authorityInformationAccess MUST contain the HTTP URL of the Issuing CA's OSCP responder.
zlintERRORSubscriber certificate cRLDistributionPoints extension must contain the HTTP URL of the CA's CRL service
zlintERRORSubscriber Certificate: authorityInformationAccess MUST be present, with the exception of stapling.
zlintWARNINGCompliant certificates should use the utf8string encoding for explicitText
zlintWARNINGSubscriber Certificate: extKeyUsage either the value id-kp-serverAuth or id-kp-clientAuth or both values MUST be present

cablintERRORBR certificates with organizationName must include either localityName or stateOrProvinceName
cablintWARNINGCertificate does not include authorityInformationAccess. BRs require OCSP stapling for this certificate.
cablintWARNINGDeprecated Netscape extension 2.16.840.1.113730.1.1 treated as opaque extension
cablintWARNINGTLS Server auth certificates should not contain Netscape Server Gated Crypto usage
cablintINFOTLS Server certificate identified
x509lintERRORError parsing URL
x509lintERRORno authorityInformationAccess extension
x509lintERRORNo OCSP over HTTP
x509lintERRORSubject with organizationName, givenName or surname but without stateOrProvince or localityName
x509lintWARNINGexplicitText is not using a UTF8String
x509lintWARNINGNo HTTP URL for issuing certificate
9333934 2015-09-04 06:12:01 2017-12-04 06:12:00 x509lintWARNINGPolicy information has qualifier other than CPS URI
x509lintWARNINGUnknown extended key usage
x509lintINFOSubject has a deprecated CommonName
x509lintINFOUnknown validation policy
zlintERRORSubscriber Certificate: authorityInformationAccess MUST contain the HTTP URL of the Issuing CA's OSCP responder.
zlintERRORSubscriber certificate cRLDistributionPoints extension must contain the HTTP URL of the CA's CRL service
zlintERRORSubscriber Certificate: authorityInformationAccess MUST be present, with the exception of stapling.
zlintWARNINGCompliant certificates should use the utf8string encoding for explicitText
zlintWARNINGSubscriber Certificate: extKeyUsage either the value id-kp-serverAuth or id-kp-clientAuth or both values MUST be present.
zlintWARNINGSubscriber certificates authorityInformationAccess extension should contain the HTTP URL of the issuing CA's certificate
zlintNOTICESubscriber Certificate: commonName is deprecated.

cablintERRORBR certificates with organizationName must include either localityName or stateOrProvinceName
cablintWARNINGCertificate does not include authorityInformationAccess. BRs require OCSP stapling for this certificate.
cablintWARNINGDeprecated Netscape extension 2.16.840.1.113730.1.1 treated as opaque extension
cablintWARNINGTLS Server auth certificates should not contain Netscape Server Gated Crypto usage
cablintINFOTLS Server certificate identified
x509lintERRORError parsing URL
x509lintERRORno authorityInformationAccess extension
x509lintERRORNo OCSP over HTTP
x509lintERRORSubject with organizationName, givenName or surname but without stateOrProvince or localityName
x509lintWARNINGexplicitText is not using a UTF8String
x509lintWARNINGNo HTTP URL for issuing certificate
10843599 2015-11-17 09:02:55 2018-02-17 09:02:54 x509lintWARNINGPolicy information has qualifier other than CPS URI
x509lintWARNINGUnknown extended key usage
x509lintINFOSubject has a deprecated CommonName
x509lintINFOUnknown validation policy
zlintERRORSubscriber Certificate: authorityInformationAccess MUST contain the HTTP URL of the Issuing CA's OSCP responder.
zlintERRORSubscriber certificate cRLDistributionPoints extension must contain the HTTP URL of the CA's CRL service
zlintERRORSubscriber Certificate: authorityInformationAccess MUST be present, with the exception of stapling.
zlintWARNINGCompliant certificates should use the utf8string encoding for explicitText
zlintWARNINGSubscriber Certificate: extKeyUsage either the value id-kp-serverAuth or id-kp-clientAuth or both values MUST be present.
zlintWARNINGSubscriber certificates authorityInformationAccess extension should contain the HTTP URL of the issuing CA's certificate
zlintNOTICESubscriber Certificate: commonName is deprecated.

cablintERRORBR certificates with organizationName must include either localityName or stateOrProvinceName
cablintWARNINGCertificate does not include authorityInformationAccess. BRs require OCSP stapling for this certificate.
cablintWARNINGDeprecated Netscape extension 2.16.840.1.113730.1.1 treated as opaque extension
cablintWARNINGTLS Server auth certificates should not contain Netscape Server Gated Crypto usage
cablintINFOTLS Server certificate identified
x509lintERRORError parsing URL
x509lintERRORno authorityInformationAccess extension
x509lintERRORNo OCSP over HTTP
x509lintERRORSubject with organizationName, givenName or surname but without stateOrProvince or localityName
x509lintWARNINGexplicitText is not using a UTF8String
x509lintWARNINGNo HTTP URL for issuing certificate
10756192 2015-11-12 09:24:59 2018-02-12 09:24:58 x509lintWARNINGPolicy information has qualifier other than CPS URI
x509lintWARNINGUnknown extended key usage
x509lintINFOSubject has a deprecated CommonName
x509lintINFOUnknown validation policy
zlintERRORSubscriber Certificate: authorityInformationAccess MUST contain the HTTP URL of the Issuing CA's OSCP responder.
zlintERRORSubscriber certificate cRLDistributionPoints extension must contain the HTTP URL of the CA's CRL service
zlintERRORSubscriber Certificate: authorityInformationAccess MUST be present, with the exception of stapling.
zlintWARNINGCompliant certificates should use the utf8string encoding for explicitText
zlintWARNINGSubscriber Certificate: extKeyUsage either the value id-kp-serverAuth or id-kp-clientAuth or both values MUST be present.
zlintWARNINGSubscriber certificates authorityInformationAccess extension should contain the HTTP URL of the issuing CA's certificate
zlintNOTICESubscriber Certificate: commonName is deprecated.

cablintERRORBR certificates with organizationName must include either localityName or stateOrProvinceName
cablintWARNINGCertificate does not include authorityInformationAccess. BRs require OCSP stapling for this certificate.
cablintWARNINGDeprecated Netscape extension 2.16.840.1.113730.1.1 treated as opaque extension
cablintWARNINGTLS Server auth certificates should not contain Netscape Server Gated Crypto usage
cablintINFOTLS Server certificate identified
x509lintERRORError parsing URL
x509lintERRORno authorityInformationAccess extension
x509lintERRORNo OCSP over HTTP
x509lintERRORSubject with organizationName, givenName or surname but without stateOrProvince or localityName
x509lintWARNINGexplicitText is not using a UTF8String
x509lintWARNINGNo HTTP URL for issuing certificate
9703582 2015-10-02 01:31:58 2018-01-02 01:31:57 x509lintWARNINGPolicy information has qualifier other than CPS URI
x509lintWARNINGUnknown extended key usage
x509lintINFOSubject has a deprecated CommonName
x509lintINFOUnknown validation policy
zlintERRORSubscriber Certificate: authorityInformationAccess MUST contain the HTTP URL of the Issuing CA's OSCP responder.
zlintERRORSubscriber certificate cRLDistributionPoints extension must contain the HTTP URL of the CA's CRL service
zlintERRORSubscriber Certificate: authorityInformationAccess MUST be present, with the exception of stapling.
zlintWARNINGCompliant certificates should use the utf8string encoding for explicitText
zlintWARNINGSubscriber Certificate: extKeyUsage either the value id-kp-serverAuth or id-kp-clientAuth or both values MUST be present.
zlintWARNINGSubscriber certificates authorityInformationAccess extension should contain the HTTP URL of the issuing CA's certificate
zlintNOTICESubscriber Certificate: commonName is deprecated.

cablintERRORBR certificates with organizationName must include either localityName or stateOrProvinceName
cablintWARNINGCertificate does not include authorityInformationAccess. BRs require OCSP stapling for this certificate.
cablintWARNINGDeprecated Netscape extension 2.16.840.1.113730.1.1 treated as opaque extension
cablintWARNINGTLS Server auth certificates should not contain Netscape Server Gated Crypto usage
cablintINFOTLS Server certificate identified
x509lintERRORError parsing URL
x509lintERRORno authorityInformationAccess extension
x509lintERRORNo OCSP over HTTP
x509lintERRORSubject with organizationName, givenName or surname but without stateOrProvince or localityName
x509lintWARNINGexplicitText is not using a UTF8String
x509lintWARNINGNo HTTP URL for issuing certificate
29955733 2015-09-01 01:03:49 2017-12-01 01:03:48 x509lintWARNINGPolicy information has qualifier other than CPS URI
x509lintWARNINGUnknown extended key usage
x509lintINFOSubject has a deprecated CommonName
x509lintINFOUnknown validation policy
zlintERRORSubscriber Certificate: authorityInformationAccess MUST contain the HTTP URL of the Issuing CA's OSCP responder.
zlintERRORSubscriber certificate cRLDistributionPoints extension must contain the HTTP URL of the CA's CRL service
zlintERRORSubscriber Certificate: authorityInformationAccess MUST be present, with the exception of stapling.
zlintWARNINGCompliant certificates should use the utf8string encoding for explicitText
zlintWARNINGSubscriber Certificate: extKeyUsage either the value id-kp-serverAuth or id-kp-clientAuth or both values MUST be present.
zlintWARNINGSubscriber certificates authorityInformationAccess extension should contain the HTTP URL of the issuing CA's certificate
zlintNOTICESubscriber Certificate: commonName is deprecated.

cablintERRORBR certificates with organizationName must include either localityName or stateOrProvinceName
cablintWARNINGCertificate does not include authorityInformationAccess. BRs require OCSP stapling for this certificate.
cablintWARNINGDeprecated Netscape extension 2.16.840.1.113730.1.1 treated as opaque extension
cablintWARNINGTLS Server auth certificates should not contain Netscape Server Gated Crypto usage
cablintINFOTLS Server certificate identified
x509lintERRORError parsing URL
x509lintERRORno authorityInformationAccess extension
x509lintERRORNo OCSP over HTTP
x509lintERRORSubject with organizationName, givenName or surname but without stateOrProvince or localityName
x509lintWARNINGexplicitText is not using a UTF8String
x509lintWARNINGNo HTTP URL for issuing certificate
10836445 2015-11-13 06:47:48 2018-02-13 06:47:47 x509lintWARNINGPolicy information has qualifier other than CPS URI
x509lintWARNINGUnknown extended key usage
x509lintINFOSubject has a deprecated CommonName
x509lintINFOUnknown validation policy
zlintERRORSubscriber Certificate: authorityInformationAccess MUST contain the HTTP URL of the Issuing CA's OSCP responder.
zlintERRORSubscriber certificate cRLDistributionPoints extension must contain the HTTP URL of the CA's CRL service
zlintERRORSubscriber Certificate: authorityInformationAccess MUST be present, with the exception of stapling.
zlintWARNINGCompliant certificates should use the utf8string encoding for explicitText
zlintWARNINGSubscriber Certificate: extKeyUsage either the value id-kp-serverAuth or id-kp-clientAuth or both values MUST be present.
zlintWARNINGSubscriber certificates authorityInformationAccess extension should contain the HTTP URL of the issuing CA's certificate
zlintNOTICESubscriber Certificate: commonName is deprecated.

cablintERRORBR certificates with organizationName must include either localityName or stateOrProvinceName
cablintWARNINGCertificate does not include authorityInformationAccess. BRs require OCSP stapling for this certificate.
cablintWARNINGDeprecated Netscape extension 2.16.840.1.113730.1.1 treated as opaque extension
cablintWARNINGTLS Server auth certificates should not contain Netscape Server Gated Crypto usage
cablintINFOTLS Server certificate identified
x509lintERRORError parsing URL
x509lintERRORno authorityInformationAccess extension
x509lintERRORNo OCSP over HTTP
x509lintERRORSubject with organizationName, givenName or surname but without stateOrProvince or localityName
x509lintWARNINGexplicitText is not using a UTF8String
x509lintWARNINGNo HTTP URL for issuing certificate
10845830 2015-11-03 06:26:26 2018-02-03 06:26:25 x509lintWARNINGPolicy information has qualifier other than CPS URI
x509lintWARNINGUnknown extended key usage
x509lintINFOSubject has a deprecated CommonName
x509lintINFOUnknown validation policy
zlintERRORSubscriber Certificate: authorityInformationAccess MUST contain the HTTP URL of the Issuing CA's OSCP responder.
zlintERRORSubscriber certificate cRLDistributionPoints extension must contain the HTTP URL of the CA's CRL service
zlintERRORSubscriber Certificate: authorityInformationAccess MUST be present, with the exception of stapling.
zlintWARNINGCompliant certificates should use the utf8string encoding for explicitText
zlintWARNINGSubscriber Certificate: extKeyUsage either the value id-kp-serverAuth or id-kp-clientAuth or both values MUST be present.
zlintWARNINGSubscriber certificates authorityInformationAccess extension should contain the HTTP URL of the issuing CA's certificate
zlintNOTICESubscriber Certificate: commonName is deprecated.

cablintERRORBR certificates with organizationName must include either localityName or stateOrProvinceName
cablintWARNINGCertificate does not include authorityInformationAccess. BRs require OCSP stapling for this certificate.
cablintWARNINGDeprecated Netscape extension 2.16.840.1.113730.1.1 treated as opaque extension
cablintWARNINGTLS Server auth certificates should not contain Netscape Server Gated Crypto usage
cablintINFOTLS Server certificate identified
x509lintERRORError parsing URL
x509lintERRORno authorityInformationAccess extension
x509lintERRORNo OCSP over HTTP
x509lintERRORSubject with organizationName, givenName or surname but without stateOrProvince or localityName
x509lintWARNINGexplicitText is not using a UTF8String
x509lintWARNINGNo HTTP URL for issuing certificate
9411037 2015-09-18 07:34:48 2017-12-18 07:34:47 x509lintWARNINGPolicy information has qualifier other than CPS URI
x509lintWARNINGUnknown extended key usage
x509lintINFOSubject has a deprecated CommonName
x509lintINFOUnknown validation policy
zlintERRORSubscriber Certificate: authorityInformationAccess MUST contain the HTTP URL of the Issuing CA's OSCP responder.
zlintERRORSubscriber certificate cRLDistributionPoints extension must contain the HTTP URL of the CA's CRL service
zlintERRORSubscriber Certificate: authorityInformationAccess MUST be present, with the exception of stapling.
zlintWARNINGCompliant certificates should use the utf8string encoding for explicitText
zlintWARNINGSubscriber Certificate: extKeyUsage either the value id-kp-serverAuth or id-kp-clientAuth or both values MUST be present.
zlintWARNINGSubscriber certificates authorityInformationAccess extension should contain the HTTP URL of the issuing CA's certificate
zlintNOTICESubscriber Certificate: commonName is deprecated.

cablintERRORBR certificates with organizationName must include either localityName or stateOrProvinceName
cablintWARNINGCertificate does not include authorityInformationAccess. BRs require OCSP stapling for this certificate.
cablintWARNINGDeprecated Netscape extension 2.16.840.1.113730.1.1 treated as opaque extension
cablintWARNINGTLS Server auth certificates should not contain Netscape Server Gated Crypto usage
cablintINFOTLS Server certificate identified
x509lintERRORError parsing URL
x509lintERRORno authorityInformationAccess extension
x509lintERRORNo OCSP over HTTP
x509lintERRORSubject with organizationName, givenName or surname but without stateOrProvince or localityName
x509lintWARNINGexplicitText is not using a UTF8String
x509lintWARNINGNo HTTP URL for issuing certificate
9698547 2015-09-30 00:54:02 2017-12-30 00:54:01 x509lintWARNINGPolicy information has qualifier other than CPS URI
x509lintWARNINGUnknown extended key usage
x509lintINFOSubject has a deprecated CommonName
x509lintINFOUnknown validation policy
zlintERRORSubscriber Certificate: authorityInformationAccess MUST contain the HTTP URL of the Issuing CA's OSCP responder.
zlintERRORSubscriber certificate cRLDistributionPoints extension must contain the HTTP URL of the CA's CRL service
zlintERRORSubscriber Certificate: authorityInformationAccess MUST be present, with the exception of stapling.
zlintWARNINGCompliant certificates should use the utf8string encoding for explicitText
zlintWARNINGSubscriber Certificate: extKeyUsage either the value id-kp-serverAuth or id-kp-clientAuth or both values MUST be present.
zlintWARNINGSubscriber certificates authorityInformationAccess extension should contain the HTTP URL of the issuing CA's certificate
zlintNOTICESubscriber Certificate: commonName is deprecated.

cablintERRORBR certificates with organizationName must include either localityName or stateOrProvinceName
cablintWARNINGCertificate does not include authorityInformationAccess. BRs require OCSP stapling for this certificate.
cablintWARNINGDeprecated Netscape extension 2.16.840.1.113730.1.1 treated as opaque extension
cablintWARNINGTLS Server auth certificates should not contain Netscape Server Gated Crypto usage
cablintINFOTLS Server certificate identified
x509lintERRORError parsing URL
x509lintERRORno authorityInformationAccess extension
x509lintERRORNo OCSP over HTTP
x509lintERRORSubject with organizationName, givenName or surname but without stateOrProvince or localityName
x509lintWARNINGexplicitText is not using a UTF8String
x509lintWARNINGNo HTTP URL for issuing certificate
10253569 2015-10-20 02:02:36 2018-01-20 02:02:35 x509lintWARNINGPolicy information has qualifier other than CPS URI
x509lintWARNINGUnknown extended key usage
x509lintINFOSubject has a deprecated CommonName
x509lintINFOUnknown validation policy
zlintERRORSubscriber Certificate: authorityInformationAccess MUST contain the HTTP URL of the Issuing CA's OSCP responder.
zlintERRORSubscriber certificate cRLDistributionPoints extension must contain the HTTP URL of the CA's CRL service
zlintERRORSubscriber Certificate: authorityInformationAccess MUST be present, with the exception of stapling.
zlintWARNINGCompliant certificates should use the utf8string encoding for explicitText
zlintWARNINGSubscriber Certificate: extKeyUsage either the value id-kp-serverAuth or id-kp-clientAuth or both values MUST be present.
zlintWARNINGSubscriber certificates authorityInformationAccess extension should contain the HTTP URL of the issuing CA's certificate
zlintNOTICESubscriber Certificate: commonName is deprecated.

cablintERRORBR certificates with organizationName must include either localityName or stateOrProvinceName
cablintWARNINGCertificate does not include authorityInformationAccess. BRs require OCSP stapling for this certificate.
cablintWARNINGDeprecated Netscape extension 2.16.840.1.113730.1.1 treated as opaque extension
cablintWARNINGTLS Server auth certificates should not contain Netscape Server Gated Crypto usage
cablintINFOTLS Server certificate identified
x509lintERRORError parsing URL
x509lintERRORno authorityInformationAccess extension
x509lintERRORNo OCSP over HTTP
x509lintERRORSubject with organizationName, givenName or surname but without stateOrProvince or localityName
x509lintWARNINGexplicitText is not using a UTF8String
x509lintWARNINGNo HTTP URL for issuing certificate
290064733 2015-09-04 06:00:32 2017-12-04 06:00:31 x509lintWARNINGPolicy information has qualifier other than CPS URI
x509lintWARNINGUnknown extended key usage
x509lintINFOSubject has a deprecated CommonName
x509lintINFOUnknown validation policy
zlintERRORSubscriber Certificate: authorityInformationAccess MUST contain the HTTP URL of the Issuing CA's OSCP responder.
zlintERRORSubscriber certificate cRLDistributionPoints extension must contain the HTTP URL of the CA's CRL service
zlintERRORSubscriber Certificate: authorityInformationAccess MUST be present, with the exception of stapling.
zlintWARNINGCompliant certificates should use the utf8string encoding for explicitText
zlintWARNINGSubscriber Certificate: extKeyUsage either the value id-kp-serverAuth or id-kp-clientAuth or both values MUST be present.
zlintWARNINGSubscriber certificates authorityInformationAccess extension should contain the HTTP URL of the issuing CA's certificate
zlintNOTICESubscriber Certificate: commonName is deprecated.

cablintERRORBR certificates with organizationName must include either localityName or stateOrProvinceName
cablintWARNINGCertificate does not include authorityInformationAccess. BRs require OCSP stapling for this certificate.
cablintWARNINGDeprecated Netscape extension 2.16.840.1.113730.1.1 treated as opaque extension
cablintWARNINGTLS Server auth certificates should not contain Netscape Server Gated Crypto usage
cablintINFOTLS Server certificate identified
x509lintERRORError parsing URL
x509lintERRORno authorityInformationAccess extension
x509lintERRORNo OCSP over HTTP
x509lintERRORSubject with organizationName, givenName or surname but without stateOrProvince or localityName
x509lintWARNINGexplicitText is not using a UTF8String
x509lintWARNINGNo HTTP URL for issuing certificate
10184313 2015-10-14 05:12:52 2018-01-14 05:12:51 x509lintWARNINGPolicy information has qualifier other than CPS URI
x509lintWARNINGUnknown extended key usage
x509lintINFOSubject has a deprecated CommonName
x509lintINFOUnknown validation policy
zlintERRORSubscriber Certificate: authorityInformationAccess MUST contain the HTTP URL of the Issuing CA's OSCP responder.
zlintERRORSubscriber certificate cRLDistributionPoints extension must contain the HTTP URL of the CA's CRL service
zlintERRORSubscriber Certificate: authorityInformationAccess MUST be present, with the exception of stapling.
zlintWARNINGCompliant certificates should use the utf8string encoding for explicitText
zlintWARNINGSubscriber Certificate: extKeyUsage either the value id-kp-serverAuth or id-kp-clientAuth or both values MUST be present.
zlintWARNINGSubscriber certificates authorityInformationAccess extension should contain the HTTP URL of the issuing CA's certificate
zlintNOTICESubscriber Certificate: commonName is deprecated.

cablintERRORBR certificates with organizationName must include either localityName or stateOrProvinceName
cablintWARNINGCertificate does not include authorityInformationAccess. BRs require OCSP stapling for this certificate.
cablintWARNINGDeprecated Netscape extension 2.16.840.1.113730.1.1 treated as opaque extension
cablintWARNINGTLS Server auth certificates should not contain Netscape Server Gated Crypto usage
cablintINFOTLS Server certificate identified
x509lintERRORError parsing URL
x509lintERRORno authorityInformationAccess extension
x509lintERRORNo OCSP over HTTP
x509lintERRORSubject with organizationName, givenName or surname but without stateOrProvince or localityName
x509lintWARNINGexplicitText is not using a UTF8String
x509lintWARNINGNo HTTP URL for issuing certificate
9716399 2015-09-04 08:31:26 2017-12-04 08:31:25 x509lintWARNINGPolicy information has qualifier other than CPS URI
x509lintWARNINGUnknown extended key usage
x509lintINFOSubject has a deprecated CommonName
x509lintINFOUnknown validation policy
zlintERRORSubscriber Certificate: authorityInformationAccess MUST contain the HTTP URL of the Issuing CA's OSCP responder.
zlintERRORSubscriber certificate cRLDistributionPoints extension must contain the HTTP URL of the CA's CRL service
zlintERRORSubscriber Certificate: authorityInformationAccess MUST be present, with the exception of stapling.
zlintWARNINGCompliant certificates should use the utf8string encoding for explicitText
zlintWARNINGSubscriber Certificate: extKeyUsage either the value id-kp-serverAuth or id-kp-clientAuth or both values MUST be present.
zlintWARNINGSubscriber certificates authorityInformationAccess extension should contain the HTTP URL of the issuing CA's certificate
zlintNOTICESubscriber Certificate: commonName is deprecated.

cablintERRORBR certificates with organizationName must include either localityName or stateOrProvinceName
cablintWARNINGCertificate does not include authorityInformationAccess. BRs require OCSP stapling for this certificate.
cablintWARNINGDeprecated Netscape extension 2.16.840.1.113730.1.1 treated as opaque extension
cablintWARNINGTLS Server auth certificates should not contain Netscape Server Gated Crypto usage
cablintINFOTLS Server certificate identified
x509lintERRORError parsing URL
x509lintERRORno authorityInformationAccess extension
x509lintERRORNo OCSP over HTTP
x509lintERRORSubject with organizationName, givenName or surname but without stateOrProvince or localityName
x509lintWARNINGexplicitText is not using a UTF8String
x509lintWARNINGNo HTTP URL for issuing certificate
9674931 2015-09-24 09:22:16 2017-12-24 09:22:15 x509lintWARNINGPolicy information has qualifier other than CPS URI
x509lintWARNINGUnknown extended key usage
x509lintINFOSubject has a deprecated CommonName
x509lintINFOUnknown validation policy
zlintERRORSubscriber Certificate: authorityInformationAccess MUST contain the HTTP URL of the Issuing CA's OSCP responder.
zlintERRORSubscriber certificate cRLDistributionPoints extension must contain the HTTP URL of the CA's CRL service
zlintERRORSubscriber Certificate: authorityInformationAccess MUST be present, with the exception of stapling.
zlintWARNINGCompliant certificates should use the utf8string encoding for explicitText
zlintWARNINGSubscriber Certificate: extKeyUsage either the value id-kp-serverAuth or id-kp-clientAuth or both values MUST be present.
zlintWARNINGSubscriber certificates authorityInformationAccess extension should contain the HTTP URL of the issuing CA's certificate
zlintNOTICESubscriber Certificate: commonName is deprecated.

cablintERRORBR certificates with organizationName must include either localityName or stateOrProvinceName
cablintWARNINGCertificate does not include authorityInformationAccess. BRs require OCSP stapling for this certificate.
cablintWARNINGDeprecated Netscape extension 2.16.840.1.113730.1.1 treated as opaque extension
cablintWARNINGTLS Server auth certificates should not contain Netscape Server Gated Crypto usage
cablintINFOTLS Server certificate identified
x509lintERRORError parsing URL
x509lintERRORno authorityInformationAccess extension
x509lintERRORNo OCSP over HTTP
x509lintERRORSubject with organizationName, givenName or surname but without stateOrProvince or localityName
x509lintWARNINGexplicitText is not using a UTF8String
x509lintWARNINGNo HTTP URL for issuing certificate
10450086 2015-10-30 09:51:13 2018-01-30 09:51:12 x509lintWARNINGPolicy information has qualifier other than CPS URI
x509lintWARNINGUnknown extended key usage
x509lintINFOSubject has a deprecated CommonName
x509lintINFOUnknown validation policy
zlintERRORSubscriber Certificate: authorityInformationAccess MUST contain the HTTP URL of the Issuing CA's OSCP responder.
zlintERRORSubscriber certificate cRLDistributionPoints extension must contain the HTTP URL of the CA's CRL service
zlintERRORSubscriber Certificate: authorityInformationAccess MUST be present, with the exception of stapling.
zlintWARNINGCompliant certificates should use the utf8string encoding for explicitText
zlintWARNINGSubscriber Certificate: extKeyUsage either the value id-kp-serverAuth or id-kp-clientAuth or both values MUST be present.
zlintWARNINGSubscriber certificates authorityInformationAccess extension should contain the HTTP URL of the issuing CA's certificate
zlintNOTICESubscriber Certificate: commonName is deprecated.

cablintERRORBR certificates with CRL Distribution Point must include HTTP URL
cablintERRORBR certificates with organizationName must include either localityName or stateOrProvinceName
cablintERRORUnknown TLD in SAN
cablintWARNINGCertificate does not include authorityInformationAccess. BRs require OCSP stapling for this certificate.
cablintWARNINGDeprecated Netscape extension 2.16.840.1.113730.1.1 treated as opaque extension
cablintWARNINGTLS Server auth certificates should not contain Netscape Server Gated Crypto usage
cablintINFOTLS Server certificate identified
x509lintERRORError parsing URL
x509lintERRORIP address in dns name
x509lintERRORno authorityInformationAccess extension
x509lintERRORNo OCSP over HTTP
x509lintERRORSubject with organizationName, givenName or surname but without stateOrProvince or localityName
10555515 2015-10-15 08:34:34 2018-01-15 08:34:33 x509lintWARNINGexplicitText is not using a UTF8String
x509lintWARNINGNo HTTP URL for issuing certificate
x509lintWARNINGPolicy information has qualifier other than CPS URI
x509lintWARNINGUnknown extended key usage
x509lintINFOSubject has a deprecated CommonName
x509lintINFOUnknown validation policy
zlintERRORDNSNames must have a valid TLD.
zlintERRORSubscriber Certificate: authorityInformationAccess MUST contain the HTTP URL of the Issuing CA's OSCP responder.
zlintERRORSubscriber certificate cRLDistributionPoints extension must contain the HTTP URL of the CA's CRL service
zlintERRORSubscriber Certificate: authorityInformationAccess MUST be present, with the exception of stapling.
zlintWARNINGCompliant certificates should use the utf8string encoding for explicitText
zlintWARNINGSubscriber Certificate: extKeyUsage either the value id-kp-serverAuth or id-kp-clientAuth or both values MUST be present

cablintERRORBR certificates with organizationName must include either localityName or stateOrProvinceName
cablintWARNINGCertificate does not include authorityInformationAccess. BRs require OCSP stapling for this certificate.
cablintWARNINGDeprecated Netscape extension 2.16.840.1.113730.1.1 treated as opaque extension
cablintWARNINGTLS Server auth certificates should not contain Netscape Server Gated Crypto usage
cablintINFOTLS Server certificate identified
x509lintERRORError parsing URL
x509lintERRORno authorityInformationAccess extension
x509lintERRORNo OCSP over HTTP
x509lintERRORSubject with organizationName, givenName or surname but without stateOrProvince or localityName
x509lintWARNINGexplicitText is not using a UTF8String
x509lintWARNINGNo HTTP URL for issuing certificate
12623748 2015-10-23 02:37:03 2018-01-23 02:37:02 x509lintWARNINGPolicy information has qualifier other than CPS URI
x509lintWARNINGUnknown extended key usage
x509lintINFOSubject has a deprecated CommonName
x509lintINFOUnknown validation policy
zlintERRORSubscriber Certificate: authorityInformationAccess MUST contain the HTTP URL of the Issuing CA's OSCP responder.
zlintERRORSubscriber certificate cRLDistributionPoints extension must contain the HTTP URL of the CA's CRL service
zlintERRORSubscriber Certificate: authorityInformationAccess MUST be present, with the exception of stapling.
zlintWARNINGCompliant certificates should use the utf8string encoding for explicitText
zlintWARNINGSubscriber Certificate: extKeyUsage either the value id-kp-serverAuth or id-kp-clientAuth or both values MUST be present.
zlintWARNINGSubscriber certificates authorityInformationAccess extension should contain the HTTP URL of the issuing CA's certificate
zlintNOTICESubscriber Certificate: commonName is deprecated.

cablintERRORBR certificates with organizationName must include either localityName or stateOrProvinceName
cablintWARNINGCertificate does not include authorityInformationAccess. BRs require OCSP stapling for this certificate.
cablintWARNINGDeprecated Netscape extension 2.16.840.1.113730.1.1 treated as opaque extension
cablintWARNINGTLS Server auth certificates should not contain Netscape Server Gated Crypto usage
cablintINFOTLS Server certificate identified
x509lintERRORError parsing URL
x509lintERRORno authorityInformationAccess extension
x509lintERRORNo OCSP over HTTP
x509lintERRORSubject with organizationName, givenName or surname but without stateOrProvince or localityName
x509lintWARNINGexplicitText is not using a UTF8String
x509lintWARNINGNo HTTP URL for issuing certificate
9927213 2015-10-06 01:11:07 2018-01-06 01:11:06 x509lintWARNINGPolicy information has qualifier other than CPS URI
x509lintWARNINGUnknown extended key usage
x509lintINFOSubject has a deprecated CommonName
x509lintINFOUnknown validation policy
zlintERRORSubscriber Certificate: authorityInformationAccess MUST contain the HTTP URL of the Issuing CA's OSCP responder.
zlintERRORSubscriber certificate cRLDistributionPoints extension must contain the HTTP URL of the CA's CRL service
zlintERRORSubscriber Certificate: authorityInformationAccess MUST be present, with the exception of stapling.
zlintWARNINGCompliant certificates should use the utf8string encoding for explicitText
zlintWARNINGSubscriber Certificate: extKeyUsage either the value id-kp-serverAuth or id-kp-clientAuth or both values MUST be present.
zlintWARNINGSubscriber certificates authorityInformationAccess extension should contain the HTTP URL of the issuing CA's certificate
zlintNOTICESubscriber Certificate: commonName is deprecated.

cablintERRORBR certificates with organizationName must include either localityName or stateOrProvinceName
cablintWARNINGCertificate does not include authorityInformationAccess. BRs require OCSP stapling for this certificate.
cablintWARNINGDeprecated Netscape extension 2.16.840.1.113730.1.1 treated as opaque extension
cablintWARNINGTLS Server auth certificates should not contain Netscape Server Gated Crypto usage
cablintINFOTLS Server certificate identified
x509lintERRORError parsing URL
x509lintERRORno authorityInformationAccess extension
x509lintERRORNo OCSP over HTTP
x509lintERRORSubject with organizationName, givenName or surname but without stateOrProvince or localityName
x509lintWARNINGexplicitText is not using a UTF8String
x509lintWARNINGNo HTTP URL for issuing certificate
10258313 2015-10-20 02:18:45 2018-01-20 02:18:44 x509lintWARNINGPolicy information has qualifier other than CPS URI
x509lintWARNINGUnknown extended key usage
x509lintINFOSubject has a deprecated CommonName
x509lintINFOUnknown validation policy
zlintERRORSubscriber Certificate: authorityInformationAccess MUST contain the HTTP URL of the Issuing CA's OSCP responder.
zlintERRORSubscriber certificate cRLDistributionPoints extension must contain the HTTP URL of the CA's CRL service
zlintERRORSubscriber Certificate: authorityInformationAccess MUST be present, with the exception of stapling.
zlintWARNINGCompliant certificates should use the utf8string encoding for explicitText
zlintWARNINGSubscriber Certificate: extKeyUsage either the value id-kp-serverAuth or id-kp-clientAuth or both values MUST be present.
zlintWARNINGSubscriber certificates authorityInformationAccess extension should contain the HTTP URL of the issuing CA's certificate
zlintNOTICESubscriber Certificate: commonName is deprecated.

cablintERRORBR certificates with organizationName must include either localityName or stateOrProvinceName
cablintWARNINGCertificate does not include authorityInformationAccess. BRs require OCSP stapling for this certificate.
cablintWARNINGDeprecated Netscape extension 2.16.840.1.113730.1.1 treated as opaque extension
cablintWARNINGTLS Server auth certificates should not contain Netscape Server Gated Crypto usage
cablintINFOTLS Server certificate identified
x509lintERRORError parsing URL
x509lintERRORno authorityInformationAccess extension
x509lintERRORNo OCSP over HTTP
x509lintERRORSubject with organizationName, givenName or surname but without stateOrProvince or localityName
x509lintWARNINGexplicitText is not using a UTF8String
x509lintWARNINGNo HTTP URL for issuing certificate
10503374 2015-10-27 11:41:37 2018-01-27 11:41:36 x509lintWARNINGPolicy information has qualifier other than CPS URI
x509lintWARNINGUnknown extended key usage
x509lintINFOSubject has a deprecated CommonName
x509lintINFOUnknown validation policy
zlintERRORSubscriber Certificate: authorityInformationAccess MUST contain the HTTP URL of the Issuing CA's OSCP responder.
zlintERRORSubscriber certificate cRLDistributionPoints extension must contain the HTTP URL of the CA's CRL service
zlintERRORSubscriber Certificate: authorityInformationAccess MUST be present, with the exception of stapling.
zlintWARNINGCompliant certificates should use the utf8string encoding for explicitText
zlintWARNINGSubscriber Certificate: extKeyUsage either the value id-kp-serverAuth or id-kp-clientAuth or both values MUST be present.
zlintWARNINGSubscriber certificates authorityInformationAccess extension should contain the HTTP URL of the issuing CA's certificate
zlintNOTICESubscriber Certificate: commonName is deprecated.

cablintERRORBR certificates with organizationName must include either localityName or stateOrProvinceName
cablintWARNINGCertificate does not include authorityInformationAccess. BRs require OCSP stapling for this certificate.
cablintWARNINGDeprecated Netscape extension 2.16.840.1.113730.1.1 treated as opaque extension
cablintWARNINGTLS Server auth certificates should not contain Netscape Server Gated Crypto usage
cablintINFOTLS Server certificate identified
x509lintERRORError parsing URL
x509lintERRORno authorityInformationAccess extension
x509lintERRORNo OCSP over HTTP
x509lintERRORSubject with organizationName, givenName or surname but without stateOrProvince or localityName
x509lintWARNINGexplicitText is not using a UTF8String
x509lintWARNINGNo HTTP URL for issuing certificate
13441339 2015-11-17 07:37:18 2018-02-17 07:37:17 x509lintWARNINGPolicy information has qualifier other than CPS URI
x509lintWARNINGUnknown extended key usage
x509lintINFOSubject has a deprecated CommonName
x509lintINFOUnknown validation policy
zlintERRORSubscriber Certificate: authorityInformationAccess MUST contain the HTTP URL of the Issuing CA's OSCP responder.
zlintERRORSubscriber certificate cRLDistributionPoints extension must contain the HTTP URL of the CA's CRL service
zlintERRORSubscriber Certificate: authorityInformationAccess MUST be present, with the exception of stapling.
zlintWARNINGCompliant certificates should use the utf8string encoding for explicitText
zlintWARNINGSubscriber Certificate: extKeyUsage either the value id-kp-serverAuth or id-kp-clientAuth or both values MUST be present.
zlintWARNINGSubscriber certificates authorityInformationAccess extension should contain the HTTP URL of the issuing CA's certificate
zlintNOTICESubscriber Certificate: commonName is deprecated.

cablintERRORBR certificates with organizationName must include either localityName or stateOrProvinceName
cablintWARNINGCertificate does not include authorityInformationAccess. BRs require OCSP stapling for this certificate.
cablintWARNINGDeprecated Netscape extension 2.16.840.1.113730.1.1 treated as opaque extension
cablintWARNINGTLS Server auth certificates should not contain Netscape Server Gated Crypto usage
cablintINFOTLS Server certificate identified
x509lintERRORError parsing URL
x509lintERRORno authorityInformationAccess extension
x509lintERRORNo OCSP over HTTP
x509lintERRORSubject with organizationName, givenName or surname but without stateOrProvince or localityName
x509lintWARNINGexplicitText is not using a UTF8String
x509lintWARNINGNo HTTP URL for issuing certificate
14725904 2015-09-01 01:21:31 2017-12-01 01:21:30 x509lintWARNINGPolicy information has qualifier other than CPS URI
x509lintWARNINGUnknown extended key usage
x509lintINFOSubject has a deprecated CommonName
x509lintINFOUnknown validation policy
zlintERRORSubscriber Certificate: authorityInformationAccess MUST contain the HTTP URL of the Issuing CA's OSCP responder.
zlintERRORSubscriber certificate cRLDistributionPoints extension must contain the HTTP URL of the CA's CRL service
zlintERRORSubscriber Certificate: authorityInformationAccess MUST be present, with the exception of stapling.
zlintWARNINGCompliant certificates should use the utf8string encoding for explicitText
zlintWARNINGSubscriber Certificate: extKeyUsage either the value id-kp-serverAuth or id-kp-clientAuth or both values MUST be present.
zlintWARNINGSubscriber certificates authorityInformationAccess extension should contain the HTTP URL of the issuing CA's certificate
zlintNOTICESubscriber Certificate: commonName is deprecated.

cablintERRORBR certificates with organizationName must include either localityName or stateOrProvinceName
cablintWARNINGCertificate does not include authorityInformationAccess. BRs require OCSP stapling for this certificate.
cablintWARNINGDeprecated Netscape extension 2.16.840.1.113730.1.1 treated as opaque extension
cablintWARNINGTLS Server auth certificates should not contain Netscape Server Gated Crypto usage
cablintINFOTLS Server certificate identified
x509lintERRORError parsing URL
x509lintERRORno authorityInformationAccess extension
x509lintERRORNo OCSP over HTTP
x509lintERRORSubject with organizationName, givenName or surname but without stateOrProvince or localityName
x509lintWARNINGexplicitText is not using a UTF8String
x509lintWARNINGNo HTTP URL for issuing certificate
10814977 2015-11-17 08:19:30 2018-02-17 08:19:29 x509lintWARNINGPolicy information has qualifier other than CPS URI
x509lintWARNINGUnknown extended key usage
x509lintINFOSubject has a deprecated CommonName
x509lintINFOUnknown validation policy
zlintERRORSubscriber Certificate: authorityInformationAccess MUST contain the HTTP URL of the Issuing CA's OSCP responder.
zlintERRORSubscriber certificate cRLDistributionPoints extension must contain the HTTP URL of the CA's CRL service
zlintERRORSubscriber Certificate: authorityInformationAccess MUST be present, with the exception of stapling.
zlintWARNINGCompliant certificates should use the utf8string encoding for explicitText
zlintWARNINGSubscriber Certificate: extKeyUsage either the value id-kp-serverAuth or id-kp-clientAuth or both values MUST be present.
zlintWARNINGSubscriber certificates authorityInformationAccess extension should contain the HTTP URL of the issuing CA's certificate
zlintNOTICESubscriber Certificate: commonName is deprecated.

cablintERRORBR certificates with organizationName must include either localityName or stateOrProvinceName
cablintWARNINGCertificate does not include authorityInformationAccess. BRs require OCSP stapling for this certificate.
cablintWARNINGDeprecated Netscape extension 2.16.840.1.113730.1.1 treated as opaque extension
cablintWARNINGTLS Server auth certificates should not contain Netscape Server Gated Crypto usage
cablintINFOTLS Server certificate identified
x509lintERRORError parsing URL
x509lintERRORno authorityInformationAccess extension
x509lintERRORNo OCSP over HTTP
x509lintERRORSubject with organizationName, givenName or surname but without stateOrProvince or localityName
x509lintWARNINGexplicitText is not using a UTF8String
x509lintWARNINGNo HTTP URL for issuing certificate
10639525 2015-11-06 06:44:09 2018-02-06 06:44:08 x509lintWARNINGPolicy information has qualifier other than CPS URI
x509lintWARNINGUnknown extended key usage
x509lintINFOSubject has a deprecated CommonName
x509lintINFOUnknown validation policy
zlintERRORSubscriber Certificate: authorityInformationAccess MUST contain the HTTP URL of the Issuing CA's OSCP responder.
zlintERRORSubscriber certificate cRLDistributionPoints extension must contain the HTTP URL of the CA's CRL service
zlintERRORSubscriber Certificate: authorityInformationAccess MUST be present, with the exception of stapling.
zlintWARNINGCompliant certificates should use the utf8string encoding for explicitText
zlintWARNINGSubscriber Certificate: extKeyUsage either the value id-kp-serverAuth or id-kp-clientAuth or both values MUST be present.
zlintWARNINGSubscriber certificates authorityInformationAccess extension should contain the HTTP URL of the issuing CA's certificate
zlintNOTICESubscriber Certificate: commonName is deprecated.

cablintERRORBR certificates with organizationName must include either localityName or stateOrProvinceName
cablintWARNINGCertificate does not include authorityInformationAccess. BRs require OCSP stapling for this certificate.
cablintWARNINGDeprecated Netscape extension 2.16.840.1.113730.1.1 treated as opaque extension
cablintWARNINGTLS Server auth certificates should not contain Netscape Server Gated Crypto usage
cablintINFOTLS Server certificate identified
x509lintERRORError parsing URL
x509lintERRORno authorityInformationAccess extension
x509lintERRORNo OCSP over HTTP
x509lintERRORSubject with organizationName, givenName or surname but without stateOrProvince or localityName
x509lintWARNINGexplicitText is not using a UTF8String
x509lintWARNINGNo HTTP URL for issuing certificate
10427254 2015-10-13 02:55:12 2018-01-13 02:55:11 x509lintWARNINGPolicy information has qualifier other than CPS URI
x509lintWARNINGUnknown extended key usage
x509lintINFOSubject has a deprecated CommonName
x509lintINFOUnknown validation policy
zlintERRORSubscriber Certificate: authorityInformationAccess MUST contain the HTTP URL of the Issuing CA's OSCP responder.
zlintERRORSubscriber certificate cRLDistributionPoints extension must contain the HTTP URL of the CA's CRL service
zlintERRORSubscriber Certificate: authorityInformationAccess MUST be present, with the exception of stapling.
zlintWARNINGCompliant certificates should use the utf8string encoding for explicitText
zlintWARNINGSubscriber Certificate: extKeyUsage either the value id-kp-serverAuth or id-kp-clientAuth or both values MUST be present.
zlintWARNINGSubscriber certificates authorityInformationAccess extension should contain the HTTP URL of the issuing CA's certificate
zlintNOTICESubscriber Certificate: commonName is deprecated.

cablintERRORBR certificates with organizationName must include either localityName or stateOrProvinceName
cablintWARNINGCertificate does not include authorityInformationAccess. BRs require OCSP stapling for this certificate.
cablintWARNINGDeprecated Netscape extension 2.16.840.1.113730.1.1 treated as opaque extension
cablintWARNINGTLS Server auth certificates should not contain Netscape Server Gated Crypto usage
cablintINFOTLS Server certificate identified
x509lintERRORError parsing URL
x509lintERRORno authorityInformationAccess extension
x509lintERRORNo OCSP over HTTP
x509lintERRORSubject with organizationName, givenName or surname but without stateOrProvince or localityName
x509lintWARNINGexplicitText is not using a UTF8String
x509lintWARNINGNo HTTP URL for issuing certificate
9996055 2015-09-22 00:56:16 2017-12-22 00:56:15 x509lintWARNINGPolicy information has qualifier other than CPS URI
x509lintWARNINGUnknown extended key usage
x509lintINFOSubject has a deprecated CommonName
x509lintINFOUnknown validation policy
zlintERRORSubscriber Certificate: authorityInformationAccess MUST contain the HTTP URL of the Issuing CA's OSCP responder.
zlintERRORSubscriber certificate cRLDistributionPoints extension must contain the HTTP URL of the CA's CRL service
zlintERRORSubscriber Certificate: authorityInformationAccess MUST be present, with the exception of stapling.
zlintWARNINGCompliant certificates should use the utf8string encoding for explicitText
zlintWARNINGSubscriber Certificate: extKeyUsage either the value id-kp-serverAuth or id-kp-clientAuth or both values MUST be present.
zlintWARNINGSubscriber certificates authorityInformationAccess extension should contain the HTTP URL of the issuing CA's certificate
zlintNOTICESubscriber Certificate: commonName is deprecated.

cablintERRORBR certificates with organizationName must include either localityName or stateOrProvinceName
cablintWARNINGCertificate does not include authorityInformationAccess. BRs require OCSP stapling for this certificate.
cablintWARNINGDeprecated Netscape extension 2.16.840.1.113730.1.1 treated as opaque extension
cablintWARNINGTLS Server auth certificates should not contain Netscape Server Gated Crypto usage
cablintINFOTLS Server certificate identified
x509lintERRORError parsing URL
x509lintERRORno authorityInformationAccess extension
x509lintERRORNo OCSP over HTTP
x509lintERRORSubject with organizationName, givenName or surname but without stateOrProvince or localityName
x509lintWARNINGexplicitText is not using a UTF8String
x509lintWARNINGNo HTTP URL for issuing certificate
10432508 2015-10-30 10:11:43 2018-01-30 10:11:42 x509lintWARNINGPolicy information has qualifier other than CPS URI
x509lintWARNINGUnknown extended key usage
x509lintINFOSubject has a deprecated CommonName
x509lintINFOUnknown validation policy
zlintERRORSubscriber Certificate: authorityInformationAccess MUST contain the HTTP URL of the Issuing CA's OSCP responder.
zlintERRORSubscriber certificate cRLDistributionPoints extension must contain the HTTP URL of the CA's CRL service
zlintERRORSubscriber Certificate: authorityInformationAccess MUST be present, with the exception of stapling.
zlintWARNINGCompliant certificates should use the utf8string encoding for explicitText
zlintWARNINGSubscriber Certificate: extKeyUsage either the value id-kp-serverAuth or id-kp-clientAuth or both values MUST be present.
zlintWARNINGSubscriber certificates authorityInformationAccess extension should contain the HTTP URL of the issuing CA's certificate
zlintNOTICESubscriber Certificate: commonName is deprecated.

cablintERRORBR certificates with organizationName must include either localityName or stateOrProvinceName
cablintWARNINGCertificate does not include authorityInformationAccess. BRs require OCSP stapling for this certificate.
cablintWARNINGDeprecated Netscape extension 2.16.840.1.113730.1.1 treated as opaque extension
cablintWARNINGTLS Server auth certificates should not contain Netscape Server Gated Crypto usage
cablintINFOTLS Server certificate identified
x509lintERRORError parsing URL
x509lintERRORno authorityInformationAccess extension
x509lintERRORNo OCSP over HTTP
x509lintERRORSubject with organizationName, givenName or surname but without stateOrProvince or localityName
x509lintWARNINGexplicitText is not using a UTF8String
x509lintWARNINGNo HTTP URL for issuing certificate
10191806 2015-10-13 02:51:44 2018-01-13 02:51:43 x509lintWARNINGPolicy information has qualifier other than CPS URI
x509lintWARNINGUnknown extended key usage
x509lintINFOSubject has a deprecated CommonName
x509lintINFOUnknown validation policy
zlintERRORSubscriber Certificate: authorityInformationAccess MUST contain the HTTP URL of the Issuing CA's OSCP responder.
zlintERRORSubscriber certificate cRLDistributionPoints extension must contain the HTTP URL of the CA's CRL service
zlintERRORSubscriber Certificate: authorityInformationAccess MUST be present, with the exception of stapling.
zlintWARNINGCompliant certificates should use the utf8string encoding for explicitText
zlintWARNINGSubscriber Certificate: extKeyUsage either the value id-kp-serverAuth or id-kp-clientAuth or both values MUST be present.
zlintWARNINGSubscriber certificates authorityInformationAccess extension should contain the HTTP URL of the issuing CA's certificate
zlintNOTICESubscriber Certificate: commonName is deprecated.

cablintERRORBR certificates with organizationName must include either localityName or stateOrProvinceName
cablintWARNINGCertificate does not include authorityInformationAccess. BRs require OCSP stapling for this certificate.
cablintWARNINGDeprecated Netscape extension 2.16.840.1.113730.1.1 treated as opaque extension
cablintWARNINGTLS Server auth certificates should not contain Netscape Server Gated Crypto usage
cablintINFOTLS Server certificate identified
x509lintERRORError parsing URL
x509lintERRORno authorityInformationAccess extension
x509lintERRORNo OCSP over HTTP
x509lintERRORSubject with organizationName, givenName or surname but without stateOrProvince or localityName
x509lintWARNINGexplicitText is not using a UTF8String
x509lintWARNINGNo HTTP URL for issuing certificate
9511680 2015-09-11 05:47:43 2017-12-11 05:47:42 x509lintWARNINGPolicy information has qualifier other than CPS URI
x509lintWARNINGUnknown extended key usage
x509lintINFOSubject has a deprecated CommonName
x509lintINFOUnknown validation policy
zlintERRORSubscriber Certificate: authorityInformationAccess MUST contain the HTTP URL of the Issuing CA's OSCP responder.
zlintERRORSubscriber certificate cRLDistributionPoints extension must contain the HTTP URL of the CA's CRL service
zlintERRORSubscriber Certificate: authorityInformationAccess MUST be present, with the exception of stapling.
zlintWARNINGCompliant certificates should use the utf8string encoding for explicitText
zlintWARNINGSubscriber Certificate: extKeyUsage either the value id-kp-serverAuth or id-kp-clientAuth or both values MUST be present.
zlintWARNINGSubscriber certificates authorityInformationAccess extension should contain the HTTP URL of the issuing CA's certificate
zlintNOTICESubscriber Certificate: commonName is deprecated.

cablintERRORBR certificates with organizationName must include either localityName or stateOrProvinceName
cablintWARNINGCertificate does not include authorityInformationAccess. BRs require OCSP stapling for this certificate.
cablintWARNINGDeprecated Netscape extension 2.16.840.1.113730.1.1 treated as opaque extension
cablintWARNINGTLS Server auth certificates should not contain Netscape Server Gated Crypto usage
cablintINFOTLS Server certificate identified
x509lintERRORError parsing URL
x509lintERRORno authorityInformationAccess extension
x509lintERRORNo OCSP over HTTP
x509lintERRORSubject with organizationName, givenName or surname but without stateOrProvince or localityName
x509lintWARNINGexplicitText is not using a UTF8String
x509lintWARNINGNo HTTP URL for issuing certificate
70204177 2015-10-15 23:42:44 2018-01-15 23:42:43 x509lintWARNINGPolicy information has qualifier other than CPS URI
x509lintWARNINGUnknown extended key usage
x509lintINFOSubject has a deprecated CommonName
x509lintINFOUnknown validation policy
zlintERRORSubscriber Certificate: authorityInformationAccess MUST contain the HTTP URL of the Issuing CA's OSCP responder.
zlintERRORSubscriber certificate cRLDistributionPoints extension must contain the HTTP URL of the CA's CRL service
zlintERRORSubscriber Certificate: authorityInformationAccess MUST be present, with the exception of stapling.
zlintWARNINGCompliant certificates should use the utf8string encoding for explicitText
zlintWARNINGSubscriber Certificate: extKeyUsage either the value id-kp-serverAuth or id-kp-clientAuth or both values MUST be present.
zlintWARNINGSubscriber certificates authorityInformationAccess extension should contain the HTTP URL of the issuing CA's certificate
zlintNOTICESubscriber Certificate: commonName is deprecated.

cablintERRORBR certificates with organizationName must include either localityName or stateOrProvinceName
cablintWARNINGCertificate does not include authorityInformationAccess. BRs require OCSP stapling for this certificate.
cablintWARNINGDeprecated Netscape extension 2.16.840.1.113730.1.1 treated as opaque extension
cablintWARNINGTLS Server auth certificates should not contain Netscape Server Gated Crypto usage
cablintINFOTLS Server certificate identified
x509lintERRORError parsing URL
x509lintERRORno authorityInformationAccess extension
x509lintERRORNo OCSP over HTTP
x509lintERRORSubject with organizationName, givenName or surname but without stateOrProvince or localityName
x509lintWARNINGexplicitText is not using a UTF8String
x509lintWARNINGNo HTTP URL for issuing certificate
10753878 2015-11-16 04:13:48 2018-02-16 04:13:47 x509lintWARNINGPolicy information has qualifier other than CPS URI
x509lintWARNINGUnknown extended key usage
x509lintINFOSubject has a deprecated CommonName
x509lintINFOUnknown validation policy
zlintERRORSubscriber Certificate: authorityInformationAccess MUST contain the HTTP URL of the Issuing CA's OSCP responder.
zlintERRORSubscriber certificate cRLDistributionPoints extension must contain the HTTP URL of the CA's CRL service
zlintERRORSubscriber Certificate: authorityInformationAccess MUST be present, with the exception of stapling.
zlintWARNINGCompliant certificates should use the utf8string encoding for explicitText
zlintWARNINGSubscriber Certificate: extKeyUsage either the value id-kp-serverAuth or id-kp-clientAuth or both values MUST be present.
zlintWARNINGSubscriber certificates authorityInformationAccess extension should contain the HTTP URL of the issuing CA's certificate
zlintNOTICESubscriber Certificate: commonName is deprecated.

cablintERRORBR certificates with organizationName must include either localityName or stateOrProvinceName
cablintWARNINGCertificate does not include authorityInformationAccess. BRs require OCSP stapling for this certificate.
cablintWARNINGDeprecated Netscape extension 2.16.840.1.113730.1.1 treated as opaque extension
cablintWARNINGTLS Server auth certificates should not contain Netscape Server Gated Crypto usage
cablintINFOTLS Server certificate identified
x509lintERRORError parsing URL
x509lintERRORno authorityInformationAccess extension
x509lintERRORNo OCSP over HTTP
x509lintERRORSubject with organizationName, givenName or surname but without stateOrProvince or localityName
x509lintWARNINGexplicitText is not using a UTF8String
x509lintWARNINGNo HTTP URL for issuing certificate
9263666 2015-09-09 07:07:18 2017-12-09 07:07:17 x509lintWARNINGPolicy information has qualifier other than CPS URI
x509lintWARNINGUnknown extended key usage
x509lintINFOSubject has a deprecated CommonName
x509lintINFOUnknown validation policy
zlintERRORSubscriber Certificate: authorityInformationAccess MUST contain the HTTP URL of the Issuing CA's OSCP responder.
zlintERRORSubscriber certificate cRLDistributionPoints extension must contain the HTTP URL of the CA's CRL service
zlintERRORSubscriber Certificate: authorityInformationAccess MUST be present, with the exception of stapling.
zlintWARNINGCompliant certificates should use the utf8string encoding for explicitText
zlintWARNINGSubscriber Certificate: extKeyUsage either the value id-kp-serverAuth or id-kp-clientAuth or both values MUST be present.
zlintWARNINGSubscriber certificates authorityInformationAccess extension should contain the HTTP URL of the issuing CA's certificate
zlintNOTICESubscriber Certificate: commonName is deprecated.

cablintERRORBR certificates with organizationName must include either localityName or stateOrProvinceName
cablintWARNINGCertificate does not include authorityInformationAccess. BRs require OCSP stapling for this certificate.
cablintWARNINGDeprecated Netscape extension 2.16.840.1.113730.1.1 treated as opaque extension
cablintWARNINGTLS Server auth certificates should not contain Netscape Server Gated Crypto usage
cablintINFOTLS Server certificate identified
x509lintERRORError parsing URL
x509lintERRORno authorityInformationAccess extension
x509lintERRORNo OCSP over HTTP
x509lintERRORSubject with organizationName, givenName or surname but without stateOrProvince or localityName
x509lintWARNINGexplicitText is not using a UTF8String
x509lintWARNINGNo HTTP URL for issuing certificate
10816235 2015-11-12 08:19:18 2018-02-12 08:19:17 x509lintWARNINGPolicy information has qualifier other than CPS URI
x509lintWARNINGUnknown extended key usage
x509lintINFOSubject has a deprecated CommonName
x509lintINFOUnknown validation policy
zlintERRORSubscriber Certificate: authorityInformationAccess MUST contain the HTTP URL of the Issuing CA's OSCP responder.
zlintERRORSubscriber certificate cRLDistributionPoints extension must contain the HTTP URL of the CA's CRL service
zlintERRORSubscriber Certificate: authorityInformationAccess MUST be present, with the exception of stapling.
zlintWARNINGCompliant certificates should use the utf8string encoding for explicitText
zlintWARNINGSubscriber Certificate: extKeyUsage either the value id-kp-serverAuth or id-kp-clientAuth or both values MUST be present.
zlintWARNINGSubscriber certificates authorityInformationAccess extension should contain the HTTP URL of the issuing CA's certificate
zlintNOTICESubscriber Certificate: commonName is deprecated.

cablintERRORBR certificates with organizationName must include either localityName or stateOrProvinceName
cablintWARNINGCertificate does not include authorityInformationAccess. BRs require OCSP stapling for this certificate.
cablintWARNINGDeprecated Netscape extension 2.16.840.1.113730.1.1 treated as opaque extension
cablintWARNINGTLS Server auth certificates should not contain Netscape Server Gated Crypto usage
cablintINFOTLS Server certificate identified
x509lintERRORError parsing URL
x509lintERRORno authorityInformationAccess extension
x509lintERRORNo OCSP over HTTP
x509lintERRORSubject with organizationName, givenName or surname but without stateOrProvince or localityName
x509lintWARNINGexplicitText is not using a UTF8String
x509lintWARNINGNo HTTP URL for issuing certificate
10920482 2015-11-23 05:13:11 2018-02-23 05:13:10 x509lintWARNINGPolicy information has qualifier other than CPS URI
x509lintWARNINGUnknown extended key usage
x509lintINFOSubject has a deprecated CommonName
x509lintINFOUnknown validation policy
zlintERRORSubscriber Certificate: authorityInformationAccess MUST contain the HTTP URL of the Issuing CA's OSCP responder.
zlintERRORSubscriber certificate cRLDistributionPoints extension must contain the HTTP URL of the CA's CRL service
zlintERRORSubscriber Certificate: authorityInformationAccess MUST be present, with the exception of stapling.
zlintWARNINGCompliant certificates should use the utf8string encoding for explicitText
zlintWARNINGSubscriber Certificate: extKeyUsage either the value id-kp-serverAuth or id-kp-clientAuth or both values MUST be present.
zlintWARNINGSubscriber certificates authorityInformationAccess extension should contain the HTTP URL of the issuing CA's certificate
zlintNOTICESubscriber Certificate: commonName is deprecated.

cablintERRORBR certificates with organizationName must include either localityName or stateOrProvinceName
cablintWARNINGCertificate does not include authorityInformationAccess. BRs require OCSP stapling for this certificate.
cablintWARNINGDeprecated Netscape extension 2.16.840.1.113730.1.1 treated as opaque extension
cablintWARNINGTLS Server auth certificates should not contain Netscape Server Gated Crypto usage
cablintINFOTLS Server certificate identified
x509lintERRORError parsing URL
x509lintERRORno authorityInformationAccess extension
x509lintERRORNo OCSP over HTTP
x509lintERRORSubject with organizationName, givenName or surname but without stateOrProvince or localityName
x509lintWARNINGexplicitText is not using a UTF8String
x509lintWARNINGNo HTTP URL for issuing certificate
14827461 2015-09-08 05:59:33 2017-12-08 05:59:32 x509lintWARNINGPolicy information has qualifier other than CPS URI
x509lintWARNINGUnknown extended key usage
x509lintINFOSubject has a deprecated CommonName
x509lintINFOUnknown validation policy
zlintERRORSubscriber Certificate: authorityInformationAccess MUST contain the HTTP URL of the Issuing CA's OSCP responder.
zlintERRORSubscriber certificate cRLDistributionPoints extension must contain the HTTP URL of the CA's CRL service
zlintERRORSubscriber Certificate: authorityInformationAccess MUST be present, with the exception of stapling.
zlintWARNINGCompliant certificates should use the utf8string encoding for explicitText
zlintWARNINGSubscriber Certificate: extKeyUsage either the value id-kp-serverAuth or id-kp-clientAuth or both values MUST be present.
zlintWARNINGSubscriber certificates authorityInformationAccess extension should contain the HTTP URL of the issuing CA's certificate
zlintNOTICESubscriber Certificate: commonName is deprecated.

cablintERRORBR certificates with organizationName must include either localityName or stateOrProvinceName
cablintWARNINGCertificate does not include authorityInformationAccess. BRs require OCSP stapling for this certificate.
cablintWARNINGDeprecated Netscape extension 2.16.840.1.113730.1.1 treated as opaque extension
cablintWARNINGTLS Server auth certificates should not contain Netscape Server Gated Crypto usage
cablintINFOTLS Server certificate identified
x509lintERRORError parsing URL
x509lintERRORno authorityInformationAccess extension
x509lintERRORNo OCSP over HTTP
x509lintERRORSubject with organizationName, givenName or surname but without stateOrProvince or localityName
x509lintWARNINGexplicitText is not using a UTF8String
x509lintWARNINGNo HTTP URL for issuing certificate
10229208 2015-09-09 07:52:44 2017-12-09 07:52:43 x509lintWARNINGPolicy information has qualifier other than CPS URI
x509lintWARNINGUnknown extended key usage
x509lintINFOSubject has a deprecated CommonName
x509lintINFOUnknown validation policy
zlintERRORSubscriber Certificate: authorityInformationAccess MUST contain the HTTP URL of the Issuing CA's OSCP responder.
zlintERRORSubscriber certificate cRLDistributionPoints extension must contain the HTTP URL of the CA's CRL service
zlintERRORSubscriber Certificate: authorityInformationAccess MUST be present, with the exception of stapling.
zlintWARNINGCompliant certificates should use the utf8string encoding for explicitText
zlintWARNINGSubscriber Certificate: extKeyUsage either the value id-kp-serverAuth or id-kp-clientAuth or both values MUST be present.
zlintWARNINGSubscriber certificates authorityInformationAccess extension should contain the HTTP URL of the issuing CA's certificate
zlintNOTICESubscriber Certificate: commonName is deprecated.

cablintERRORBR certificates with organizationName must include either localityName or stateOrProvinceName
cablintWARNINGCertificate does not include authorityInformationAccess. BRs require OCSP stapling for this certificate.
cablintWARNINGDeprecated Netscape extension 2.16.840.1.113730.1.1 treated as opaque extension
cablintWARNINGTLS Server auth certificates should not contain Netscape Server Gated Crypto usage
cablintINFOTLS Server certificate identified
x509lintERRORError parsing URL
x509lintERRORno authorityInformationAccess extension
x509lintERRORNo OCSP over HTTP
x509lintERRORSubject with organizationName, givenName or surname but without stateOrProvince or localityName
x509lintWARNINGexplicitText is not using a UTF8String
x509lintWARNINGNo HTTP URL for issuing certificate
10848471 2015-11-17 01:41:41 2018-02-17 01:41:40 x509lintWARNINGPolicy information has qualifier other than CPS URI
x509lintWARNINGUnknown extended key usage
x509lintINFOSubject has a deprecated CommonName
x509lintINFOUnknown validation policy
zlintERRORSubscriber Certificate: authorityInformationAccess MUST contain the HTTP URL of the Issuing CA's OSCP responder.
zlintERRORSubscriber certificate cRLDistributionPoints extension must contain the HTTP URL of the CA's CRL service
zlintERRORSubscriber Certificate: authorityInformationAccess MUST be present, with the exception of stapling.
zlintWARNINGCompliant certificates should use the utf8string encoding for explicitText
zlintWARNINGSubscriber Certificate: extKeyUsage either the value id-kp-serverAuth or id-kp-clientAuth or both values MUST be present.
zlintWARNINGSubscriber certificates authorityInformationAccess extension should contain the HTTP URL of the issuing CA's certificate
zlintNOTICESubscriber Certificate: commonName is deprecated.

cablintERRORBR certificates with organizationName must include either localityName or stateOrProvinceName
cablintWARNINGCertificate does not include authorityInformationAccess. BRs require OCSP stapling for this certificate.
cablintWARNINGDeprecated Netscape extension 2.16.840.1.113730.1.1 treated as opaque extension
cablintWARNINGTLS Server auth certificates should not contain Netscape Server Gated Crypto usage
cablintINFOTLS Server certificate identified
x509lintERRORError parsing URL
x509lintERRORno authorityInformationAccess extension
x509lintERRORNo OCSP over HTTP
x509lintERRORSubject with organizationName, givenName or surname but without stateOrProvince or localityName
x509lintWARNINGexplicitText is not using a UTF8String
x509lintWARNINGNo HTTP URL for issuing certificate
10684749 2015-11-11 18:22:42 2018-02-11 18:22:41 x509lintWARNINGPolicy information has qualifier other than CPS URI
x509lintWARNINGUnknown extended key usage
x509lintINFOSubject has a deprecated CommonName
x509lintINFOUnknown validation policy
zlintERRORSubscriber Certificate: authorityInformationAccess MUST contain the HTTP URL of the Issuing CA's OSCP responder.
zlintERRORSubscriber certificate cRLDistributionPoints extension must contain the HTTP URL of the CA's CRL service
zlintERRORSubscriber Certificate: authorityInformationAccess MUST be present, with the exception of stapling.
zlintWARNINGCompliant certificates should use the utf8string encoding for explicitText
zlintWARNINGSubscriber Certificate: extKeyUsage either the value id-kp-serverAuth or id-kp-clientAuth or both values MUST be present.
zlintWARNINGSubscriber certificates authorityInformationAccess extension should contain the HTTP URL of the issuing CA's certificate
zlintNOTICESubscriber Certificate: commonName is deprecated.

cablintERRORBR certificates with organizationName must include either localityName or stateOrProvinceName
cablintWARNINGCertificate does not include authorityInformationAccess. BRs require OCSP stapling for this certificate.
cablintWARNINGDeprecated Netscape extension 2.16.840.1.113730.1.1 treated as opaque extension
cablintWARNINGTLS Server auth certificates should not contain Netscape Server Gated Crypto usage
cablintINFOTLS Server certificate identified
x509lintERRORError parsing URL
x509lintERRORno authorityInformationAccess extension
x509lintERRORNo OCSP over HTTP
x509lintERRORSubject with organizationName, givenName or surname but without stateOrProvince or localityName
x509lintWARNINGexplicitText is not using a UTF8String
x509lintWARNINGNo HTTP URL for issuing certificate
9960436 2015-10-05 08:09:41 2018-01-05 08:09:40 x509lintWARNINGPolicy information has qualifier other than CPS URI
x509lintWARNINGUnknown extended key usage
x509lintINFOSubject has a deprecated CommonName
x509lintINFOUnknown validation policy
zlintERRORSubscriber Certificate: authorityInformationAccess MUST contain the HTTP URL of the Issuing CA's OSCP responder.
zlintERRORSubscriber certificate cRLDistributionPoints extension must contain the HTTP URL of the CA's CRL service
zlintERRORSubscriber Certificate: authorityInformationAccess MUST be present, with the exception of stapling.
zlintWARNINGCompliant certificates should use the utf8string encoding for explicitText
zlintWARNINGSubscriber Certificate: extKeyUsage either the value id-kp-serverAuth or id-kp-clientAuth or both values MUST be present.
zlintWARNINGSubscriber certificates authorityInformationAccess extension should contain the HTTP URL of the issuing CA's certificate
zlintNOTICESubscriber Certificate: commonName is deprecated.

cablintERRORBR certificates with organizationName must include either localityName or stateOrProvinceName
cablintWARNINGCertificate does not include authorityInformationAccess. BRs require OCSP stapling for this certificate.
cablintWARNINGDeprecated Netscape extension 2.16.840.1.113730.1.1 treated as opaque extension
cablintWARNINGTLS Server auth certificates should not contain Netscape Server Gated Crypto usage
cablintINFOTLS Server certificate identified
x509lintERRORError parsing URL
x509lintERRORno authorityInformationAccess extension
x509lintERRORNo OCSP over HTTP
x509lintERRORSubject with organizationName, givenName or surname but without stateOrProvince or localityName
x509lintWARNINGexplicitText is not using a UTF8String
x509lintWARNINGNo HTTP URL for issuing certificate
10874282 2015-10-30 08:32:37 2018-01-30 08:32:36 x509lintWARNINGPolicy information has qualifier other than CPS URI
x509lintWARNINGUnknown extended key usage
x509lintINFOSubject has a deprecated CommonName
x509lintINFOUnknown validation policy
zlintERRORSubscriber Certificate: authorityInformationAccess MUST contain the HTTP URL of the Issuing CA's OSCP responder.
zlintERRORSubscriber certificate cRLDistributionPoints extension must contain the HTTP URL of the CA's CRL service
zlintERRORSubscriber Certificate: authorityInformationAccess MUST be present, with the exception of stapling.
zlintWARNINGCompliant certificates should use the utf8string encoding for explicitText
zlintWARNINGSubscriber Certificate: extKeyUsage either the value id-kp-serverAuth or id-kp-clientAuth or both values MUST be present.
zlintWARNINGSubscriber certificates authorityInformationAccess extension should contain the HTTP URL of the issuing CA's certificate
zlintNOTICESubscriber Certificate: commonName is deprecated.

cablintERRORBR certificates with organizationName must include either localityName or stateOrProvinceName
cablintWARNINGCertificate does not include authorityInformationAccess. BRs require OCSP stapling for this certificate.
cablintWARNINGDeprecated Netscape extension 2.16.840.1.113730.1.1 treated as opaque extension
cablintWARNINGTLS Server auth certificates should not contain Netscape Server Gated Crypto usage
cablintINFOTLS Server certificate identified
x509lintERRORError parsing URL
x509lintERRORno authorityInformationAccess extension
x509lintERRORNo OCSP over HTTP
x509lintERRORSubject with organizationName, givenName or surname but without stateOrProvince or localityName
x509lintWARNINGexplicitText is not using a UTF8String
x509lintWARNINGNo HTTP URL for issuing certificate
287402315 2015-11-16 07:29:09 2018-02-16 07:29:08 x509lintWARNINGPolicy information has qualifier other than CPS URI
x509lintWARNINGUnknown extended key usage
x509lintINFOSubject has a deprecated CommonName
x509lintINFOUnknown validation policy
zlintERRORSubscriber Certificate: authorityInformationAccess MUST contain the HTTP URL of the Issuing CA's OSCP responder.
zlintERRORSubscriber certificate cRLDistributionPoints extension must contain the HTTP URL of the CA's CRL service
zlintERRORSubscriber Certificate: authorityInformationAccess MUST be present, with the exception of stapling.
zlintWARNINGCompliant certificates should use the utf8string encoding for explicitText
zlintWARNINGSubscriber Certificate: extKeyUsage either the value id-kp-serverAuth or id-kp-clientAuth or both values MUST be present.
zlintWARNINGSubscriber certificates authorityInformationAccess extension should contain the HTTP URL of the issuing CA's certificate
zlintNOTICESubscriber Certificate: commonName is deprecated.

cablintERRORBR certificates with organizationName must include either localityName or stateOrProvinceName
cablintWARNINGCertificate does not include authorityInformationAccess. BRs require OCSP stapling for this certificate.
cablintWARNINGDeprecated Netscape extension 2.16.840.1.113730.1.1 treated as opaque extension
cablintWARNINGTLS Server auth certificates should not contain Netscape Server Gated Crypto usage
cablintINFOTLS Server certificate identified
x509lintERRORError parsing URL
x509lintERRORno authorityInformationAccess extension
x509lintERRORNo OCSP over HTTP
x509lintERRORSubject with organizationName, givenName or surname but without stateOrProvince or localityName
x509lintWARNINGexplicitText is not using a UTF8String
x509lintWARNINGNo HTTP URL for issuing certificate
10915724 2015-11-25 16:12:25 2018-02-25 16:12:24 x509lintWARNINGPolicy information has qualifier other than CPS URI
x509lintWARNINGUnknown extended key usage
x509lintINFOSubject has a deprecated CommonName
x509lintINFOUnknown validation policy
zlintERRORSubscriber Certificate: authorityInformationAccess MUST contain the HTTP URL of the Issuing CA's OSCP responder.
zlintERRORSubscriber certificate cRLDistributionPoints extension must contain the HTTP URL of the CA's CRL service
zlintERRORSubscriber Certificate: authorityInformationAccess MUST be present, with the exception of stapling.
zlintWARNINGCompliant certificates should use the utf8string encoding for explicitText
zlintWARNINGSubscriber Certificate: extKeyUsage either the value id-kp-serverAuth or id-kp-clientAuth or both values MUST be present.
zlintWARNINGSubscriber certificates authorityInformationAccess extension should contain the HTTP URL of the issuing CA's certificate
zlintNOTICESubscriber Certificate: commonName is deprecated.

cablintERRORBR certificates with organizationName must include either localityName or stateOrProvinceName
cablintWARNINGCertificate does not include authorityInformationAccess. BRs require OCSP stapling for this certificate.
cablintWARNINGDeprecated Netscape extension 2.16.840.1.113730.1.1 treated as opaque extension
cablintWARNINGTLS Server auth certificates should not contain Netscape Server Gated Crypto usage
cablintINFOTLS Server certificate identified
x509lintERRORError parsing URL
x509lintERRORno authorityInformationAccess extension
x509lintERRORNo OCSP over HTTP
x509lintERRORSubject with organizationName, givenName or surname but without stateOrProvince or localityName
x509lintWARNINGexplicitText is not using a UTF8String
x509lintWARNINGNo HTTP URL for issuing certificate
16613663 2015-09-21 00:27:51 2017-12-21 00:27:50 x509lintWARNINGPolicy information has qualifier other than CPS URI
x509lintWARNINGUnknown extended key usage
x509lintINFOSubject has a deprecated CommonName
x509lintINFOUnknown validation policy
zlintERRORSubscriber Certificate: authorityInformationAccess MUST contain the HTTP URL of the Issuing CA's OSCP responder.
zlintERRORSubscriber certificate cRLDistributionPoints extension must contain the HTTP URL of the CA's CRL service
zlintERRORSubscriber Certificate: authorityInformationAccess MUST be present, with the exception of stapling.
zlintWARNINGCompliant certificates should use the utf8string encoding for explicitText
zlintWARNINGSubscriber Certificate: extKeyUsage either the value id-kp-serverAuth or id-kp-clientAuth or both values MUST be present.
zlintWARNINGSubscriber certificates authorityInformationAccess extension should contain the HTTP URL of the issuing CA's certificate
zlintNOTICESubscriber Certificate: commonName is deprecated.

cablintERRORBR certificates with organizationName must include either localityName or stateOrProvinceName
cablintWARNINGCertificate does not include authorityInformationAccess. BRs require OCSP stapling for this certificate.
cablintWARNINGDeprecated Netscape extension 2.16.840.1.113730.1.1 treated as opaque extension
cablintWARNINGTLS Server auth certificates should not contain Netscape Server Gated Crypto usage
cablintINFOTLS Server certificate identified
x509lintERRORError parsing URL
x509lintERRORno authorityInformationAccess extension
x509lintERRORNo OCSP over HTTP
x509lintERRORSubject with organizationName, givenName or surname but without stateOrProvince or localityName
x509lintWARNINGexplicitText is not using a UTF8String
x509lintWARNINGNo HTTP URL for issuing certificate
9511637 2015-09-24 08:45:26 2017-12-24 08:45:25 x509lintWARNINGPolicy information has qualifier other than CPS URI
x509lintWARNINGUnknown extended key usage
x509lintINFOSubject has a deprecated CommonName
x509lintINFOUnknown validation policy
zlintERRORSubscriber Certificate: authorityInformationAccess MUST contain the HTTP URL of the Issuing CA's OSCP responder.
zlintERRORSubscriber certificate cRLDistributionPoints extension must contain the HTTP URL of the CA's CRL service
zlintERRORSubscriber Certificate: authorityInformationAccess MUST be present, with the exception of stapling.
zlintWARNINGCompliant certificates should use the utf8string encoding for explicitText
zlintWARNINGSubscriber Certificate: extKeyUsage either the value id-kp-serverAuth or id-kp-clientAuth or both values MUST be present.
zlintWARNINGSubscriber certificates authorityInformationAccess extension should contain the HTTP URL of the issuing CA's certificate
zlintNOTICESubscriber Certificate: commonName is deprecated.

cablintERRORBR certificates with organizationName must include either localityName or stateOrProvinceName
cablintWARNINGCertificate does not include authorityInformationAccess. BRs require OCSP stapling for this certificate.
cablintWARNINGDeprecated Netscape extension 2.16.840.1.113730.1.1 treated as opaque extension
cablintWARNINGTLS Server auth certificates should not contain Netscape Server Gated Crypto usage
cablintINFOTLS Server certificate identified
x509lintERRORError parsing URL
x509lintERRORno authorityInformationAccess extension
x509lintERRORNo OCSP over HTTP
x509lintERRORSubject with organizationName, givenName or surname but without stateOrProvince or localityName
x509lintWARNINGexplicitText is not using a UTF8String
x509lintWARNINGNo HTTP URL for issuing certificate
10672120 2015-11-10 09:06:06 2018-02-10 09:06:05 x509lintWARNINGPolicy information has qualifier other than CPS URI
x509lintWARNINGUnknown extended key usage
x509lintINFOSubject has a deprecated CommonName
x509lintINFOUnknown validation policy
zlintERRORSubscriber Certificate: authorityInformationAccess MUST contain the HTTP URL of the Issuing CA's OSCP responder.
zlintERRORSubscriber certificate cRLDistributionPoints extension must contain the HTTP URL of the CA's CRL service
zlintERRORSubscriber Certificate: authorityInformationAccess MUST be present, with the exception of stapling.
zlintWARNINGCompliant certificates should use the utf8string encoding for explicitText
zlintWARNINGSubscriber Certificate: extKeyUsage either the value id-kp-serverAuth or id-kp-clientAuth or both values MUST be present.
zlintWARNINGSubscriber certificates authorityInformationAccess extension should contain the HTTP URL of the issuing CA's certificate
zlintNOTICESubscriber Certificate: commonName is deprecated.

cablintERRORBR certificates with organizationName must include either localityName or stateOrProvinceName
cablintWARNINGCertificate does not include authorityInformationAccess. BRs require OCSP stapling for this certificate.
cablintWARNINGDeprecated Netscape extension 2.16.840.1.113730.1.1 treated as opaque extension
cablintWARNINGTLS Server auth certificates should not contain Netscape Server Gated Crypto usage
cablintINFOTLS Server certificate identified
x509lintERRORError parsing URL
x509lintERRORno authorityInformationAccess extension
x509lintERRORNo OCSP over HTTP
x509lintERRORSubject with organizationName, givenName or surname but without stateOrProvince or localityName
x509lintWARNINGexplicitText is not using a UTF8String
x509lintWARNINGNo HTTP URL for issuing certificate
9897954 2015-10-05 07:03:49 2018-01-05 07:03:48 x509lintWARNINGPolicy information has qualifier other than CPS URI
x509lintWARNINGUnknown extended key usage
x509lintINFOSubject has a deprecated CommonName
x509lintINFOUnknown validation policy
zlintERRORSubscriber Certificate: authorityInformationAccess MUST contain the HTTP URL of the Issuing CA's OSCP responder.
zlintERRORSubscriber certificate cRLDistributionPoints extension must contain the HTTP URL of the CA's CRL service
zlintERRORSubscriber Certificate: authorityInformationAccess MUST be present, with the exception of stapling.
zlintWARNINGCompliant certificates should use the utf8string encoding for explicitText
zlintWARNINGSubscriber Certificate: extKeyUsage either the value id-kp-serverAuth or id-kp-clientAuth or both values MUST be present.
zlintWARNINGSubscriber certificates authorityInformationAccess extension should contain the HTTP URL of the issuing CA's certificate
zlintNOTICESubscriber Certificate: commonName is deprecated.

cablintERRORBR certificates with organizationName must include either localityName or stateOrProvinceName
cablintWARNINGCertificate does not include authorityInformationAccess. BRs require OCSP stapling for this certificate.
cablintWARNINGDeprecated Netscape extension 2.16.840.1.113730.1.1 treated as opaque extension
cablintWARNINGTLS Server auth certificates should not contain Netscape Server Gated Crypto usage
cablintINFOTLS Server certificate identified
x509lintERRORError parsing URL
x509lintERRORno authorityInformationAccess extension
x509lintERRORNo OCSP over HTTP
x509lintERRORSubject with organizationName, givenName or surname but without stateOrProvince or localityName
x509lintWARNINGexplicitText is not using a UTF8String
x509lintWARNINGNo HTTP URL for issuing certificate
9473571 2015-09-22 07:52:20 2017-12-22 07:52:19 x509lintWARNINGPolicy information has qualifier other than CPS URI
x509lintWARNINGUnknown extended key usage
x509lintINFOSubject has a deprecated CommonName
x509lintINFOUnknown validation policy
zlintERRORSubscriber Certificate: authorityInformationAccess MUST contain the HTTP URL of the Issuing CA's OSCP responder.
zlintERRORSubscriber certificate cRLDistributionPoints extension must contain the HTTP URL of the CA's CRL service
zlintERRORSubscriber Certificate: authorityInformationAccess MUST be present, with the exception of stapling.
zlintWARNINGCompliant certificates should use the utf8string encoding for explicitText
zlintWARNINGSubscriber Certificate: extKeyUsage either the value id-kp-serverAuth or id-kp-clientAuth or both values MUST be present.
zlintWARNINGSubscriber certificates authorityInformationAccess extension should contain the HTTP URL of the issuing CA's certificate
zlintNOTICESubscriber Certificate: commonName is deprecated.

cablintERRORBR certificates with organizationName must include either localityName or stateOrProvinceName
cablintWARNINGCertificate does not include authorityInformationAccess. BRs require OCSP stapling for this certificate.
cablintWARNINGDeprecated Netscape extension 2.16.840.1.113730.1.1 treated as opaque extension
cablintWARNINGTLS Server auth certificates should not contain Netscape Server Gated Crypto usage
cablintINFOTLS Server certificate identified
x509lintERRORError parsing URL
x509lintERRORno authorityInformationAccess extension
x509lintERRORNo OCSP over HTTP
x509lintERRORSubject with organizationName, givenName or surname but without stateOrProvince or localityName
x509lintWARNINGexplicitText is not using a UTF8String
x509lintWARNINGNo HTTP URL for issuing certificate
10845003 2015-11-18 00:43:38 2018-02-18 00:43:37 x509lintWARNINGPolicy information has qualifier other than CPS URI
x509lintWARNINGUnknown extended key usage
x509lintINFOSubject has a deprecated CommonName
x509lintINFOUnknown validation policy
zlintERRORSubscriber Certificate: authorityInformationAccess MUST contain the HTTP URL of the Issuing CA's OSCP responder.
zlintERRORSubscriber certificate cRLDistributionPoints extension must contain the HTTP URL of the CA's CRL service
zlintERRORSubscriber Certificate: authorityInformationAccess MUST be present, with the exception of stapling.
zlintWARNINGCompliant certificates should use the utf8string encoding for explicitText
zlintWARNINGSubscriber Certificate: extKeyUsage either the value id-kp-serverAuth or id-kp-clientAuth or both values MUST be present.
zlintWARNINGSubscriber certificates authorityInformationAccess extension should contain the HTTP URL of the issuing CA's certificate
zlintNOTICESubscriber Certificate: commonName is deprecated.

cablintERRORBR certificates with organizationName must include either localityName or stateOrProvinceName
cablintWARNINGCertificate does not include authorityInformationAccess. BRs require OCSP stapling for this certificate.
cablintWARNINGDeprecated Netscape extension 2.16.840.1.113730.1.1 treated as opaque extension
cablintWARNINGTLS Server auth certificates should not contain Netscape Server Gated Crypto usage
cablintINFOTLS Server certificate identified
x509lintERRORError parsing URL
x509lintERRORno authorityInformationAccess extension
x509lintERRORNo OCSP over HTTP
x509lintERRORSubject with organizationName, givenName or surname but without stateOrProvince or localityName
x509lintWARNINGexplicitText is not using a UTF8String
x509lintWARNINGNo HTTP URL for issuing certificate
10508122 2015-10-30 04:54:11 2018-01-30 04:54:10 x509lintWARNINGPolicy information has qualifier other than CPS URI
x509lintWARNINGUnknown extended key usage
x509lintINFOSubject has a deprecated CommonName
x509lintINFOUnknown validation policy
zlintERRORSubscriber Certificate: authorityInformationAccess MUST contain the HTTP URL of the Issuing CA's OSCP responder.
zlintERRORSubscriber certificate cRLDistributionPoints extension must contain the HTTP URL of the CA's CRL service
zlintERRORSubscriber Certificate: authorityInformationAccess MUST be present, with the exception of stapling.
zlintWARNINGCompliant certificates should use the utf8string encoding for explicitText
zlintWARNINGSubscriber Certificate: extKeyUsage either the value id-kp-serverAuth or id-kp-clientAuth or both values MUST be present.
zlintWARNINGSubscriber certificates authorityInformationAccess extension should contain the HTTP URL of the issuing CA's certificate
zlintNOTICESubscriber Certificate: commonName is deprecated.

cablintERRORBR certificates with organizationName must include either localityName or stateOrProvinceName
cablintWARNINGCertificate does not include authorityInformationAccess. BRs require OCSP stapling for this certificate.
cablintWARNINGDeprecated Netscape extension 2.16.840.1.113730.1.1 treated as opaque extension
cablintWARNINGTLS Server auth certificates should not contain Netscape Server Gated Crypto usage
cablintINFOTLS Server certificate identified
x509lintERRORError parsing URL
x509lintERRORno authorityInformationAccess extension
x509lintERRORNo OCSP over HTTP
x509lintERRORSubject with organizationName, givenName or surname but without stateOrProvince or localityName
x509lintWARNINGexplicitText is not using a UTF8String
x509lintWARNINGNo HTTP URL for issuing certificate
10441577 2015-10-30 05:42:06 2018-01-30 05:42:05 x509lintWARNINGPolicy information has qualifier other than CPS URI
x509lintWARNINGUnknown extended key usage
x509lintINFOSubject has a deprecated CommonName
x509lintINFOUnknown validation policy
zlintERRORSubscriber Certificate: authorityInformationAccess MUST contain the HTTP URL of the Issuing CA's OSCP responder.
zlintERRORSubscriber certificate cRLDistributionPoints extension must contain the HTTP URL of the CA's CRL service
zlintERRORSubscriber Certificate: authorityInformationAccess MUST be present, with the exception of stapling.
zlintWARNINGCompliant certificates should use the utf8string encoding for explicitText
zlintWARNINGSubscriber Certificate: extKeyUsage either the value id-kp-serverAuth or id-kp-clientAuth or both values MUST be present.
zlintWARNINGSubscriber certificates authorityInformationAccess extension should contain the HTTP URL of the issuing CA's certificate
zlintNOTICESubscriber Certificate: commonName is deprecated.

cablintERRORBR certificates with organizationName must include either localityName or stateOrProvinceName
cablintWARNINGCertificate does not include authorityInformationAccess. BRs require OCSP stapling for this certificate.
cablintWARNINGDeprecated Netscape extension 2.16.840.1.113730.1.1 treated as opaque extension
cablintWARNINGTLS Server auth certificates should not contain Netscape Server Gated Crypto usage
cablintINFOTLS Server certificate identified
x509lintERRORError parsing URL
x509lintERRORno authorityInformationAccess extension
x509lintERRORNo OCSP over HTTP
x509lintERRORSubject with organizationName, givenName or surname but without stateOrProvince or localityName
x509lintWARNINGexplicitText is not using a UTF8String
x509lintWARNINGNo HTTP URL for issuing certificate
10557962 2015-11-03 08:01:29 2018-02-03 08:01:28 x509lintWARNINGPolicy information has qualifier other than CPS URI
x509lintWARNINGUnknown extended key usage
x509lintINFOSubject has a deprecated CommonName
x509lintINFOUnknown validation policy
zlintERRORSubscriber Certificate: authorityInformationAccess MUST contain the HTTP URL of the Issuing CA's OSCP responder.
zlintERRORSubscriber certificate cRLDistributionPoints extension must contain the HTTP URL of the CA's CRL service
zlintERRORSubscriber Certificate: authorityInformationAccess MUST be present, with the exception of stapling.
zlintWARNINGCompliant certificates should use the utf8string encoding for explicitText
zlintWARNINGSubscriber Certificate: extKeyUsage either the value id-kp-serverAuth or id-kp-clientAuth or both values MUST be present.
zlintWARNINGSubscriber certificates authorityInformationAccess extension should contain the HTTP URL of the issuing CA's certificate
zlintNOTICESubscriber Certificate: commonName is deprecated.

cablintERRORBR certificates with organizationName must include either localityName or stateOrProvinceName
cablintWARNINGCertificate does not include authorityInformationAccess. BRs require OCSP stapling for this certificate.
cablintWARNINGDeprecated Netscape extension 2.16.840.1.113730.1.1 treated as opaque extension
cablintWARNINGTLS Server auth certificates should not contain Netscape Server Gated Crypto usage
cablintINFOTLS Server certificate identified
x509lintERRORError parsing URL
x509lintERRORno authorityInformationAccess extension
x509lintERRORNo OCSP over HTTP
x509lintERRORSubject with organizationName, givenName or surname but without stateOrProvince or localityName
x509lintWARNINGexplicitText is not using a UTF8String
x509lintWARNINGNo HTTP URL for issuing certificate
13903595 2015-10-08 07:37:43 2018-01-08 07:37:42 x509lintWARNINGPolicy information has qualifier other than CPS URI
x509lintWARNINGUnknown extended key usage
x509lintINFOSubject has a deprecated CommonName
x509lintINFOUnknown validation policy
zlintERRORSubscriber Certificate: authorityInformationAccess MUST contain the HTTP URL of the Issuing CA's OSCP responder.
zlintERRORSubscriber certificate cRLDistributionPoints extension must contain the HTTP URL of the CA's CRL service
zlintERRORSubscriber Certificate: authorityInformationAccess MUST be present, with the exception of stapling.
zlintWARNINGCompliant certificates should use the utf8string encoding for explicitText
zlintWARNINGSubscriber Certificate: extKeyUsage either the value id-kp-serverAuth or id-kp-clientAuth or both values MUST be present.
zlintWARNINGSubscriber certificates authorityInformationAccess extension should contain the HTTP URL of the issuing CA's certificate
zlintNOTICESubscriber Certificate: commonName is deprecated.

cablintERRORBR certificates with organizationName must include either localityName or stateOrProvinceName
cablintWARNINGCertificate does not include authorityInformationAccess. BRs require OCSP stapling for this certificate.
cablintWARNINGDeprecated Netscape extension 2.16.840.1.113730.1.1 treated as opaque extension
cablintWARNINGTLS Server auth certificates should not contain Netscape Server Gated Crypto usage
cablintINFOTLS Server certificate identified
x509lintERRORError parsing URL
x509lintERRORno authorityInformationAccess extension
x509lintERRORNo OCSP over HTTP
x509lintERRORSubject with organizationName, givenName or surname but without stateOrProvince or localityName
x509lintWARNINGexplicitText is not using a UTF8String
x509lintWARNINGNo HTTP URL for issuing certificate
9686297 2015-10-02 04:25:19 2018-01-02 04:25:18 x509lintWARNINGPolicy information has qualifier other than CPS URI
x509lintWARNINGUnknown extended key usage
x509lintINFOSubject has a deprecated CommonName
x509lintINFOUnknown validation policy
zlintERRORSubscriber Certificate: authorityInformationAccess MUST contain the HTTP URL of the Issuing CA's OSCP responder.
zlintERRORSubscriber certificate cRLDistributionPoints extension must contain the HTTP URL of the CA's CRL service
zlintERRORSubscriber Certificate: authorityInformationAccess MUST be present, with the exception of stapling.
zlintWARNINGCompliant certificates should use the utf8string encoding for explicitText
zlintWARNINGSubscriber Certificate: extKeyUsage either the value id-kp-serverAuth or id-kp-clientAuth or both values MUST be present.
zlintWARNINGSubscriber certificates authorityInformationAccess extension should contain the HTTP URL of the issuing CA's certificate
zlintNOTICESubscriber Certificate: commonName is deprecated.

cablintERRORBR certificates with organizationName must include either localityName or stateOrProvinceName
cablintWARNINGCertificate does not include authorityInformationAccess. BRs require OCSP stapling for this certificate.
cablintWARNINGDeprecated Netscape extension 2.16.840.1.113730.1.1 treated as opaque extension
cablintWARNINGTLS Server auth certificates should not contain Netscape Server Gated Crypto usage
cablintINFOTLS Server certificate identified
x509lintERRORError parsing URL
x509lintERRORno authorityInformationAccess extension
x509lintERRORNo OCSP over HTTP
x509lintERRORSubject with organizationName, givenName or surname but without stateOrProvince or localityName
x509lintWARNINGexplicitText is not using a UTF8String
x509lintWARNINGNo HTTP URL for issuing certificate
289368287 2015-09-14 01:29:43 2017-12-14 01:29:42 x509lintWARNINGPolicy information has qualifier other than CPS URI
x509lintWARNINGUnknown extended key usage
x509lintINFOSubject has a deprecated CommonName
x509lintINFOUnknown validation policy
zlintERRORSubscriber Certificate: authorityInformationAccess MUST contain the HTTP URL of the Issuing CA's OSCP responder.
zlintERRORSubscriber certificate cRLDistributionPoints extension must contain the HTTP URL of the CA's CRL service
zlintERRORSubscriber Certificate: authorityInformationAccess MUST be present, with the exception of stapling.
zlintWARNINGCompliant certificates should use the utf8string encoding for explicitText
zlintWARNINGSubscriber Certificate: extKeyUsage either the value id-kp-serverAuth or id-kp-clientAuth or both values MUST be present.
zlintWARNINGSubscriber certificates authorityInformationAccess extension should contain the HTTP URL of the issuing CA's certificate
zlintNOTICESubscriber Certificate: commonName is deprecated.