```
HTTP/1.1 200 OK
Date: Wed, 21 Nov 2018 09:55:06 GMT
Content-Type: application/json
Transfer-Encoding: chunked
Content-Length: 31957
{
  "diagnosticData" : {
    "documentName" : "xades-detached.xml",
    "validationDate" : 1542794106070,
    "containerInfo" : null,
    "signatures" : [ {
      "signatureFilename" : "xades-detached.xml",
      "parentId" : null,
      "errorMessage" : null,
      "dateTime" : 1506596944000,
      "signatureFormat" : "XAdES-BASELINE-B",
      "structuralValidation" : {
        "valid" : true,
        "message" : null
      "digestMatchers" : [ {
        "digestMethod" : "SHA256",
        "digestValue" : "kcDHOZjwZhVfuDhuhCeCERRmYpTH4Jj4RmfVVi31Q9g=",
        "dataFound" : true,
        "dataIntact" : true,
        "type": "REFERENCE",
        "name" : "r-id-1"
      }, {
        "digestMethod" : "SHA256",
        "digestValue": "DztwNTmRoOAm6/lMI8Rym5xZPzIvLYDzn/ebYYkPsr4=",
        "dataFound" : true,
        "dataIntact" : true,
        "type" : "SIGNED_PROPERTIES",
        "name" : "#xades-id-afde782436468dd74eeb181f7ce110e1"
      }],
      "basicSignature" : {
        "encryptionAlgoUsedToSignThisToken": "RSA",
        "keyLengthUsedToSignThisToken": "2048",
        "digestAlgoUsedToSignThisToken": "SHA256",
        "maskGenerationFunctionUsedToSignThisToken" : null,
        "signatureIntact" : true,
        "signatureValid" : true
      "signingCertificate" : {
        "attributePresent" : true,
        "digestValuePresent" : true,
        "digestValueMatch" : true,
        "issuerSerialMatch" : true,
        "id": "F0FF0B4514D316304F2817DBA0BFB05DEDB98527C0E47C73E8D8FDFE16DF267E"
```

```
"certificateChain" : [ {
    "source": "SIGNATURE",
    "id": "F0FF0B4514D316304F2817DBA0BFB05DEDB98527C0E47C73E8D8FDFE16DF267E"
 }, {
    "source": "SIGNATURE",
    "id": "6F35DE3965B9A69BC3661D1A355B0AE60907ADB741CC1911EFD0F3BE72D6A6E9"
 } ],
  "contentType" : "text/xml",
  "contentIdentifier" : null,
  "contentHints" : null,
  "signatureProductionPlace" : null,
  "commitmentTypeIndication" : [ ],
  "claimedRoles" : [ ],
  "certifiedRoles" : [ ],
  "policy" : null,
  "timestamps" : [ ],
  "signatureScopes" : [ {
    "value" : "Full document",
    "name" : "sample.xml",
    "scope" : "FULL"
 } ],
  "id" : "id-afde782436468dd74eeb181f7ce110e1",
 "counterSignature" : null
"usedCertificates" : [ {
  "subjectDistinguishedName" : [ {
    "value" : "c=lu,ou=pki-test,o=nowina solutions,cn=good-ca",
    "format" : "CANONICAL"
 }, {
    "value" : "C=LU,OU=PKI-TEST,O=Nowina Solutions,CN=good-ca",
    "format" : "RFC2253"
 } ],
  "issuerDistinguishedName" : [ {
    "value" : "c=lu,ou=pki-test,o=nowina solutions,cn=root-ca",
    "format" : "CANONICAL"
 }, {
    "value" : "C=LU,OU=PKI-TEST,O=Nowina Solutions,CN=root-ca",
    "format" : "RFC2253"
 }],
  "serialNumber" : 4,
  "commonName" : "good-ca",
  "locality" : null,
  "state" : null,
  "countryName" : "LU",
  "organizationName" : "Nowina Solutions",
  "givenName" : null,
  "organizationalUnit": "PKI-TEST",
  "surname" : null,
  "pseudonym" : null,
  "email" : null,
```

```
"authorityInformationAccessUrls" : [ "http://dss.nowina.lu/pki-factory/crt/root-
ca.crt"],
      "digestAlgoAndValues" : [ ],
      "notAfter" : 1535270070000,
      "notBefore" : 1477468470000,
      "publicKeySize" : 2048,
      "publicKeyEncryptionAlgo" : "RSA",
      "keyUsageBits" : [ "digitalSignature" ],
      "extendedKeyUsages" : [ ],
      "idPkixOcspNoCheck" : false,
      "basicSignature" : {
        "encryptionAlgoUsedToSignThisToken": "RSA",
        "keyLengthUsedToSignThisToken": "?",
        "digestAlgoUsedToSignThisToken": "SHA256",
        "maskGenerationFunctionUsedToSignThisToken" : null,
        "signatureIntact" : false,
        "signatureValid" : false
     },
      "signingCertificate" : null,
      "certificateChain" : [ ],
      "trusted" : false,
      "selfSigned" : false,
      "certificatePolicies" : [ ],
      "trustedServiceProviders" : [ ],
      "revocations" : [ ],
      "base64Encoded":
"MIID6jCCAtKgAwIBAgIBBDANBgkghkiG9w0BAQsFADBNMRAwDgYDVQQDDAdyb290LWNhMRkwFwYDVQQKDBBOb
3dpbmEgU29sdXRpb25zMREwDwYDVQQLDAhQS0ktVEVTVDELMAkGA1UEBhMCTFUwHhcNMTYxMDI2MDc1NDMwWhc
NMTgwODI2MDc1NDMwWjBNMRAwDgYDVQQDDAdnb29kLWNhMRkwFwYDVQQKDBBOb3dpbmEgU29sdXRpb25zMREwD
wYDVQQLDAhQS0ktVEVTVDELMAkGA1UEBhMCTFUwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCbbl5
sKBCjSB8TMdacymx/Wf0jMW1giIjVJRY28JbNWkCVmtzgmitghfrPQPlueu0DTalbDkrSSyhCvzzPSGPwCFOah
F/n7hQa1F3UaHSxTKrFC5n0wdLzxKRO3WjVtIGRSX2kv1FfUpQy5Eyy+rsfSzJ59dU5ZZdWpdaDuDxVVyDer3E
IyCbG7/5H9MD4YuzNpeTFWmM6cUST0796XDlbExSTTGQXFJA2+CCsy9DXnJa8nz0FE8fmcvQHeU6k9QbpzGjMd
3DWlE6no7UdCYD1H04+usBp5hhCrAB670NdoTrNTmGNAFt4JT0vitjKHq9KEId6Lhdcm2Tq93dDcWFtAgMBAAG
jgdQwgdEwDgYDVR0PAQH/BAQDAgeAMEEGA1UdHwQ6MDgwNgA0oDKGMGh0dHA6Ly9kc3Mubm93aW5hLmx1L3Bra
S1mYWN0b3J5L2NybC9yb290LWNhLmNybDBMBggrBgEFBQcBAQRAMD4wPAYIKwYBBQUHMAKGMGh0dHA6Ly9kc3M
ubm93aW5hLmx1L3BraS1mYWN0b3J5L2NydC9yb290LWNhLmNydDAdBgNVHQ4EFgQU+2tFqpNe3G23YR8yqBZIi
VWS3vUwDwYDVR0TAQH/BAUwAwEB/zANBgkqhkiG9w0BAQsFAAOCAQEAE+Nud05XGOM6FEZHWTc8+bmz/6B0XQX
N564KWBBhch9i5GadjqpSsevkn+teLq5m6CLo3e4lX2dJ7hsPAvyaLq0Ipzq49TGdib1n0B2074+yAhT8v9FZt
H1ECHXxYsuySGIKvd+L5IjJTis3l14vU8FHzyR1M9IQnwZR506jFcJeGlOgyZh+ULWnRNEEwqN8DTF2D0XogYB
srCxCBj0PpaJFruvEQqpUuuYq14R1DJFahLwqVYS0D5qPhmA0HR4z3GF3jHSz0i9jXSTOsUcdkvUJy0tIOnujs
UEkg3H6Wg3lz8Tw3Ic7V1NHb+MC5K4ZvX+5SYyu0+er7bFscIrYZw==",
      "id": "6F35DE3965B9A69BC3661D1A355B0AE60907ADB741CC1911EFD0F3BE72D6A6E9",
      "qctypes" : [ ],
      "ocspaccessUrls" : [ ],
      "crldistributionPoints" : [ "http://dss.nowina.lu/pki-factory/crl/root-ca.crl"
],
      "qcstatementIds" : [ ]
   }, {
      "subjectDistinguishedName" : [ {
        "value" : "c=lu,ou=pki-test,o=nowina solutions,cn=root-ca",
```

```
"format" : "CANONICAL"
     }, {
        "value" : "C=LU,OU=PKI-TEST,O=Nowina Solutions,CN=root-ca",
        "format" : "RFC2253"
     } ],
      "issuerDistinguishedName" : [ {
        "value" : "c=lu,ou=pki-test,o=nowina solutions,cn=root-ca",
        "format" : "CANONICAL"
     }, {
        "value" : "C=LU,OU=PKI-TEST,O=Nowina Solutions,CN=root-ca",
        "format" : "RFC2253"
     } ],
      "serialNumber" : 1,
      "commonName" : "root-ca",
      "locality" : null,
      "state" : null,
      "countryName" : "LU",
      "organizationName" : "Nowina Solutions",
      "givenName" : null,
      "organizationalUnit" : "PKI-TEST",
      "surname" : null,
      "pseudonym" : null,
      "email" : null,
      "authorityInformationAccessUrls" : [ ],
      "digestAlgoAndValues" : [ ],
      "notAfter" : 1571924603000,
      "notBefore": 1508852603000,
      "publicKeySize" : 2048,
      "publicKeyEncryptionAlgo" : "RSA",
      "keyUsageBits" : [ "keyCertSign", "crlSign" ],
      "extendedKeyUsages" : [ ],
      "idPkixOcspNoCheck" : false,
      "basicSignature" : {
        "encryptionAlgoUsedToSignThisToken": "RSA",
        "keyLengthUsedToSignThisToken": "2048",
        "digestAlgoUsedToSignThisToken": "SHA512",
        "maskGenerationFunctionUsedToSignThisToken" : null,
        "signatureIntact" : true,
        "signatureValid" : true
     },
      "signingCertificate" : null,
      "certificateChain" : [ ],
      "trusted" : false,
      "selfSigned" : true,
      "certificatePolicies" : [ ],
      "trustedServiceProviders" : [ ],
      "revocations" : [ ],
      "base64Encoded":
"MIIDVzCCAj+gAwIBAgIBATANBgkqhkiG9w0BAQ0FADBNMRAwDgYDVQQDDAdyb290LWNhMRkwFwYDVQQKDBBOb
3dpbmEqU29sdXRpb25zMREwDwYDVQQLDAhQS0ktVEVTVDELMAkGA1UEBhMCTFUwHhcNMTcxMDI0MTM0MzIzWhc
NMTkxMDI0MTM0MzIzWjBNMRAwDgYDVQQDDAdyb290LWNhMRkwFwYDVQQKDBB0b3dpbmEgU29sdXRpb25zMREwD
```

WYDVQQLDAhQS0ktVEVTVDELMAkGA1UEBhMCTFUwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCcPx2 j00cAL0qmQ99apDybqwXCMvzwTDzNU7RkDYvGRQVTaqthrp7abnJn0zgjeCsu4N/9GgwXn8ICQTYEq00QVD6fabZT4ophtPbuIPF0CCL8FIXkpK2p6qpBNeHNxvgpQegMXMNUVqcYyp1v39/zyYI+iimBLhSTz09QP54i32Katfn7ophaaYnsc02TJ0s9aBGRxekzyliUimWekr/KSY9fIHLEU09lgmdYhk1P+0AcuGQHrNYn0E2Jyl9NLN+3gtBuzTSxwJEvQIvTGAWIz+qCnCugMH6eH0s3CkbWlRSEy1qIgidqsNYm0yP6B02hJdim9r0A3z809HSe4KFlAgMBAAGjQjBAMA4GA1UdDwEB/wQEAwIBBjAdBgNVHQ4EFgQUw91nslwAwQ7I31tDQp2Y0rBeFxowDwYDVR0TAQH/BAUwAwEB/zANBgkqhkiG9w0BAQ0FAA0CAQEA04PsY/jm4VkJKDA19mlpy2/qRaAj5n3MlgX2/8UaVRm4+5HUZ1z0rXM9D14gofS1eYvAD2HeBnHrY+6mfwBcH+NF54YDRjRibXp48F0n91HjnkMNjYB5o16tl8y0frI+eWJbq+GgLLvlruWShXCSQuWgDbY5jXcHV+TQskSQOcOy1hh82jdH2ysEtd4Kc0/E20GDUy+M7ZffBnLxPjxZRm198eyeC/gcVjBZoqHykwkivkYazbWhWvMkV95htR6x7dL2fp2sr9s12Gbq8Y9PfpXfXJ06qCQtojJiml4rF3YWWPVOUK6Gy1DFAv1U2i0ASiV4sVwLkp1WAIFwKSChHQ==",

```
"id": "9B3449709FC4B27B39B4BB289BF5C368A4FEA913A901E183163B3D8E32462E02",
      "qctypes" : [ ],
      "ocspaccessUrls" : [ ],
      "crldistributionPoints" : [ ],
      "qcstatementIds" : [ ]
   }, {
      "subjectDistinguishedName" : [ {
        "value" : "c=lu,ou=pki-test,o=nowina solutions,cn=good-user",
        "format" : "CANONICAL"
      }, {
        "value" : "C=LU,OU=PKI-TEST,O=Nowina Solutions,CN=good-user",
        "format" : "RFC2253"
      } ],
      "issuerDistinguishedName" : [ {
        "value" : "c=lu,ou=pki-test,o=nowina solutions,cn=good-ca",
        "format" : "CANONICAL"
        "value": "C=LU,OU=PKI-TEST,O=Nowina Solutions,CN=good-ca",
        "format" : "RFC2253"
      } ],
      "serialNumber" : 10,
      "commonName" : "good-user",
      "locality" : null,
      "state" : null,
      "countryName" : "LU",
      "organizationName" : "Nowina Solutions",
      "givenName" : null,
      "organizationalUnit" : "PKI-TEST",
      "surname" : null,
      "pseudonym" : null,
      "email" : null,
      "authorityInformationAccessUrls" : [ "http://dss.nowina.lu/pki-factory/crt/good-
ca.crt" ],
      "digestAlgoAndValues" : [ ],
      "notAfter" : 1535270071000,
      "notBefore": 1477468471000,
      "publicKeySize" : 2048,
      "publicKeyEncryptionAlgo" : "RSA",
      "keyUsageBits" : [ "nonRepudiation" ],
      "extendedKeyUsages" : [ ],
```

```
"idPkixOcspNoCheck" : false,
      "basicSignature" : {
        "encryptionAlgoUsedToSignThisToken" : "RSA",
        "keyLengthUsedToSignThisToken": "2048",
        "digestAlgoUsedToSignThisToken" : "SHA256",
        "maskGenerationFunctionUsedToSignThisToken" : null,
        "signatureIntact" : true,
        "signatureValid" : true
      },
      "signingCertificate" : {
        "attributePresent" : null,
        "digestValuePresent" : null,
        "digestValueMatch" : null,
        "issuerSerialMatch" : null,
        "id": "6F35DE3965B9A69BC3661D1A355B0AE60907ADB741CC1911EFD0F3BE72D6A6E9"
      "certificateChain" : [ {
        "source": "SIGNATURE",
        "id": "6F35DE3965B9A69BC3661D1A355B0AE60907ADB741CC1911EFD0F3BE72D6A6E9"
      } ],
      "trusted" : false,
      "selfSigned" : false,
      "certificatePolicies" : [ ],
      "trustedServiceProviders" : [ ],
      "revocations" : [ ],
      "base64Encoded" :
"MIID1DCCArygAwIBAgIBCjANBgkghkiG9w0BAQsFADBNMRAwDgYDVQQDDAdnb29kLWNhMRkwFwYDVQQKDBBOb
3dpbmEgU29sdXRpb25zMREwDwYDVQQLDAhQS0ktVEVTVDELMAkGA1UEBhMCTFUwHhcNMTYxMDI2MDc1NDMxWhc
NMTgwODI2MDc1NDMxWjBPMRIwEAYDVQQDDAlnb29kLXVzZXIxGTAXBgNVBAoMEE5vd2luYSBTb2x1dGlvbnMxE
TAPBqNVBAsMCFBLSS1URVNUMQswCQYDVQQGEwJMVTCCASIwDQYJKoZIhvcNAQEBBQADqqEPADCCAQoCqqEBALR
CUIQZbw3nSdLp+B9czECgpZkkQ5xV4g9M/7wlg97oCCf7UEh9BA1d+zYjszv+BJ1bJZPgan2144AvgsoGJfb6U
IyVW4gklUgIl1arUvon+WkKnseFuQOfJyjSFUDIwnuvp0hzcJXHXRmLdmyh+n+6NMH0om5tVoSfQrtBViCLeSM
VzuD5EPj0mIRcx91pL38e3FNTW7NaGZLeezuFuR/q7z931LkvZ4VAMNGGLvIXOYeRBZMyPhpBZ4L3A8I3EE1KW
H/1LwiiXTTSG1sM6WvMTVbf2vbd47nZRQA2mSpNGjQouOAErfeVVUqzICqhQCHRGONuSLG/HfqFHb4jWg0CAwE
AAaOBvDCBuTAOBqNVHQ8BAf8EBAMCBkAwqYcGCCsGAQUFBwEBBHsweTA5BqqrBqEFBQcwAYYtaHR0cDovL2Rzc
y5ub3dpbmEubHUvcGtpLWZhY3Rvcnkvb2NzcC9nb29kLWNhMDwGCCsGAQUFBzAChjBodHRwOi8vZHNzLm5vd2l
uYS5sdS9wa2ktZmFjdG9yeS9jcnQvZ29vZC1jYS5jcnQwHQYDVR00BBYEFN2pHD/7PefmBT8oX29ZhWy/OHJ1M
A0GCSqGSIb3DQEBCwUAA4IBAQBK3V0LhDIVWKoFrrhhWzaddtk6XQtcwRoNPVSsi/g0rzsdM70A31xITw7YfLh
poVA1xo7ovHldpLlhqy9o5wh282yCpqBUAtqrSkDGoq+K7CL6qUprlYiZuGZrtq2X3fHS2Usx4ZJ3tIj6wVecD
EUqISFfFT2Esm0QXUngIKFM195Xgmtw2wxXbOzUeDd4DIPrv+mW5poAWr6ItsV+H2VQ+ZL/kBnwWHjSTOaGFis
qXY/aH/1PtBXA+15+YIWemJBSv3kDaFzOXAEtR9ZI81YOJarnY7Ay/aN6b9uGffrbo/hVAcL4WDdhkbBN3m8w+
q76LoAXNeEeu04A/0xLZzUB",
      "id": "F0FF0B4514D316304F2817DBA0BFB05DEDB98527C0E47C73E8D8FDFE16DF267E",
      "qctypes" : [ ],
      "ocspaccessUrls" : [ "http://dss.nowina.lu/pki-factory/ocsp/good-ca" ],
      "crldistributionPoints" : [ ],
      "qcstatementIds" : [ ]
    }, {
      "subjectDistinguishedName" : [ {
        "value" : "c=lu,ou=pki-test,o=nowina solutions,cn=good-ca",
        "format" : "CANONICAL"
```

```
"value" : "C=LU,OU=PKI-TEST,O=Nowina Solutions,CN=good-ca",
        "format" : "RFC2253"
      "issuerDistinguishedName" : [ {
        "value" : "c=lu,ou=pki-test,o=nowina solutions,cn=root-ca",
        "format" : "CANONICAL"
     }, {
        "value" : "C=LU,OU=PKI-TEST,O=Nowina Solutions,CN=root-ca",
        "format" : "RFC2253"
     } ],
      "serialNumber" : 4,
      "commonName" : "good-ca",
      "locality" : null,
      "state" : null,
      "countryName" : "LU",
      "organizationName" : "Nowina Solutions",
      "givenName" : null,
      "organizationalUnit" : "PKI-TEST",
      "surname" : null,
      "pseudonym" : null,
      "email" : null,
      "authorityInformationAccessUrls" : [ "http://dss.nowina.lu/pki-factory/crt/root-
ca.crt" ],
      "digestAlgoAndValues" : [ ],
      "notAfter" : 1569332604000,
      "notBefore": 1511534604000,
      "publicKeySize" : 2048,
      "publicKeyEncryptionAlgo" : "RSA",
      "keyUsageBits" : [ "digitalSignature" ],
      "extendedKeyUsages" : [ ],
      "idPkixOcspNoCheck" : false,
      "basicSignature" : {
        "encryptionAlgoUsedToSignThisToken": "RSA",
        "keyLengthUsedToSignThisToken": "2048",
        "digestAlgoUsedToSignThisToken": "SHA256",
        "maskGenerationFunctionUsedToSignThisToken" : null,
        "signatureIntact" : true,
        "signatureValid" : true
     },
      "signingCertificate" : {
        "attributePresent" : null,
        "digestValuePresent" : null,
        "digestValueMatch" : null,
        "issuerSerialMatch" : null,
        "id": "9B3449709FC4B27B39B4BB289BF5C368A4FEA913A901E183163B3D8E32462E02"
     },
      "certificateChain" : [ {
        "source": "AIA",
        "id": "9B3449709FC4B27B39B4BB289BF5C368A4FEA913A901E183163B3D8E32462E02"
     }],
```

```
"trusted" : false,
      "selfSigned" : false,
      "certificatePolicies" : [ ],
      "trustedServiceProviders" : [ ],
      "revocations" : [ ],
      "base64Encoded" :
"MIID6jCCAtKgAwIBAgIBBDANBgkghkiG9w0BAQsFADBNMRAwDgYDVQQDDAdyb290LWNhMRkwFwYDVQQKDBBOb
3dpbmEgU29sdXRpb25zMREwDwYDVQQLDAhQS0ktVEVTVDELMAkGA1UEBhMCTFUwHhcNMTcxMTI0MTQ0MzI0Whc
NMTkwOTI0MTM0MzI0WjBNMRAwDgYDVQQDDAdnb29kLWNhMRkwFwYDVQQKDBB0b3dpbmEgU29sdXRpb25zMREwD
wYDVQQLDAhQS0ktVEVTVDELMAkGA1UEBhMCTFUwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDE0Jt
jEg9q261R5tJnvPLkgtWaMrRkeDfABta1qI3XLC2+AwLketU11PuwK5HopmHkSTpXFE/cWfGmbgsHSkYlfcsXD
6CKtYtinjzeekMQE7xiPWM5b9QtyGoh6BZUyydw934LnNjJNHfMgQVtyVnQ8L6SwFhyT3BTWU9SzVCNSlyUSJC
AEsNQrFP1mxiHsdXJlUUykqxhaLC0qGZhIyhTZB3qNaRSIcGr4IlXTCXUkB8oaWNqwe/sS1+JlkiGdGED3NR9Z
h4SBAk65wfL1xjzN+JgDrTTbPoKJ0lqeTrv3NMsW9rzG/Fx4AlJgA7Lo+ujrHwggyC9zg3pRRQaH+LpAgMBAAG
jgdQwgdEwDgYDVR0PAQH/BAQDAgeAMEEGA1UdHwQ6MDgwNgA0oDKGMGh0dHA6Ly9kc3Mubm93aW5hLmx1L3Bra
S1mYWN0b3J5L2NybC9yb290LWNhLmNybDBMBggrBgEFBQcBAQRAMD4wPAYIKwYBBQUHMAKGMGh0dHA6Ly9kc3M
ubm93aW5hLmx1L3BraS1mYWN0b3J5L2NydC9yb290LWNhLmNydDAdBgNVHQ4EFgQUYEoTfXrajcuuURqGnbZIZ
lxBRQ0wDwYDVR0TAQH/BAUwAwEB/zANBgkqhkiG9w0BAQsFAAOCAQEAMEZzOXyFl4FEUr0XIaI2ha74zIbGsmt
Kdk2p801cYh4vrsldN8hbXUu7sbWTJ9BP6HdFJ+89fP+OUbyHm1NwFYf+BN11+NFKQoDniheezha9Z08m0aKST
Qvt/J3SHr/Ui7F00cDZhPa4SNHWdtl2capxYUY0o7ww/WpI+z5bIUauwiimBEqK2Dr2jwxbztM0qlDjKgHpCtr
iW48e5NmT9IBnJhMqqlLJpt9/AwepRMakcz65/wu40YcPd42TINMWwcIAWAZLPxdemIuwMrCQnGKZSmi1GkCWu
MOwFcHXk7Yb2xku6PQPvcLWqSRMjD0RzVy8G2kK52VMwwwjoDi+Gg==",
      "id": "AB3AE83863C1B024F54BFCCB363792CD9051E540853820756EA46D2A2E2B9E43",
      "qctypes" : [ ],
      "ocspaccessUrls" : [ ],
      "crldistributionPoints" : [ "http://dss.nowina.lu/pki-factory/crl/root-ca.crl"
],
      "qcstatementIds" : [ ]
    } ],
    "trustedLists" : [ ],
    "listOfTrustedLists" : null
 },
  "simpleReport" : {
    "policy" : {
      "policyName" : "QES AdESQC TL based",
      "policyDescription" : "Validate electronic signatures and indicates whether they
are Advanced electronic Signatures (AdES), AdES supported by a Qualified Certificate
(AdES/QC) or a\n\t\tQualified electronic Signature (QES). All certificates and their
related chains supporting the signatures are validated against the EU Member State
Trusted Lists (this includes\n\t\tsigner's certificate and certificates used to
validate certificate validity status services - CRLs, OCSP, and time-stamps).\n\t"
    "validationTime" : 1542794106070,
    "documentName" : "xades-detached.xml",
    "validSignaturesCount" : 0,
    "signaturesCount" : 1,
    "containerType" : null,
    "signature" : [ {
      "filename" : null,
      "signingTime" : 1506596944000,
      "bestSignatureTime" : 1542794106070,
```

```
"signedBy" : "good-user",
      "certificateChain" : {
        "certificate" : [ {
          "id": "F0FF0B4514D316304F2817DBA0BFB05DEDB98527C0E47C73E8D8FDFE16DF267E",
         "qualifiedName" : "good-user"
        }, {
          "id": "6F35DE3965B9A69BC3661D1A355B0AE60907ADB741CC1911EFD0F3BE72D6A6E9",
         "qualifiedName" : "good-ca"
       } ]
     },
      "signatureLevel" : {
        "value" : "NA",
        "description" : "Not applicable"
     },
      "indication": "INDETERMINATE",
      "subIndication" : "NO_CERTIFICATE_CHAIN_FOUND",
      "errors" : [ "The certificate path is not trusted!", "The result of the LTV
validation process is not acceptable to continue the process!" ],
      "warnings" : [ "The signature/seal is an INDETERMINATE AdES!" ],
      "infos" : [ ],
      "signatureScope" : [ {
        "value" : "Full document",
        "name" : "sample.xml",
       "scope" : "FULL"
     } ],
      "id": "id-afde782436468dd74eeb181f7ce110e1",
      "counterSignature" : null,
      "parentId" : null,
     "signatureFormat": "XAdES-BASELINE-B"
   } ]
 },
  "detailedReport" : {
    "signatures" : [ {
      "validationProcessBasicSignatures" : {
        "constraint" : [ {
          "name" : {
            "value" : "Is the result of the Basic Validation Process conclusive?",
            "nameId" : "ADEST ROBVPIIC"
         },
          "status" : "NOT_OK",
          "error" : {
            "value": "The result of the Basic validation process is not conclusive!",
            "nameId": "ADEST_ROBVPIIC_ANS"
         },
          "warning" : null,
         "info" : null,
          "additionalInfo" : null,
          "id" : "id-afde782436468dd74eeb181f7ce110e1"
        } ],
        "conclusion" : {
          "indication": "INDETERMINATE",
```

```
"subIndication" : "NO_CERTIFICATE_CHAIN_FOUND",
          "errors" : [ {
            "value" : "The certificate chain for signature is not trusted, there is no
trusted anchor.",
            "nameId" : "BBB_XCV_CCCBB_SIG_ANS"
          "warnings" : [ ],
         "infos" : [ ]
        },
        "bestSignatureTime" : 1542794106070
      "validationProcessTimestamps" : [ ],
      "validationProcessLongTermData" : {
        "constraint" : [ {
          "name" : {
            "value": "Is the result of the Basic Validation Process acceptable?",
            "nameId" : "LTV ABSV"
          },
          "status" : "NOT_OK",
          "error" : {
            "value": "The result of the Basic validation process is not acceptable to
continue the process!",
            "nameId" : "LTV_ABSV_ANS"
          },
          "warning" : null,
          "info" : null,
          "additionalInfo" : null,
          "id" : null
        } ],
        "conclusion" : {
          "indication": "INDETERMINATE",
          "subIndication": "NO CERTIFICATE CHAIN FOUND",
          "errors" : [ {
            "value" : "The certificate chain for signature is not trusted, there is no
trusted anchor.",
            "nameId" : "BBB_XCV_CCCBB_SIG_ANS"
          "warnings" : [ ],
          "infos" : [ ]
        "bestSignatureTime" : 1542794106070
      "validationProcessArchivalData" : {
        "constraint" : [ {
          "name" : {
            "value" : "Is the result of the LTV validation process acceptable?",
            "nameId" : "ARCH_LTVV"
          "status" : "NOT_OK",
          "error" : {
            "value" : "The result of the LTV validation process is not acceptable to
```

```
continue the process!",
            "nameId" : "ARCH_LTVV_ANS"
          },
          "warning" : null,
          "info" : null,
          "additionalInfo" : null,
          "id" : null
        } ],
        "conclusion" : {
          "indication" : "INDETERMINATE",
          "subIndication": "NO_CERTIFICATE_CHAIN_FOUND",
          "errors" : [ {
            "value" : "The certificate chain for signature is not trusted, there is no
trusted anchor.",
            "nameId" : "BBB_XCV_CCCBB_SIG_ANS"
          "warnings" : [ ],
          "infos" : [ ]
        },
        "bestSignatureTime" : 1542794106070
      },
      "validationSignatureQualification" : {
        "constraint" : [ {
          "name" : {
            "value" : "Is the signature/seal an acceptable AdES (ETSI EN 319 102-1)
?",
            "nameId" : "QUAL_IS_ADES"
          },
          "status" : "WARNING",
          "error" : null,
          "warning" : {
            "value": "The signature/seal is an INDETERMINATE AdES!",
            "nameId" : "QUAL IS ADES IND"
          },
          "info" : null,
          "additionalInfo" : null,
          "id" : null
        }, {
          "name" : {
            "value" : "Is the certificate path trusted?",
            "nameId": "QUAL TRUSTED CERT PATH"
          },
          "status" : "NOT_OK",
          "error" : {
            "value" : "The certificate path is not trusted!",
            "nameId" : "QUAL_TRUSTED_CERT_PATH_ANS"
          },
          "warning" : null,
          "info" : null,
          "additionalInfo" : null,
          "id" : null
```

```
}],
    "conclusion" : {
      "indication": "FAILED",
      "subIndication" : null,
      "errors" : [ {
        "value" : "The certificate path is not trusted!",
        "nameId" : "QUAL_TRUSTED_CERT_PATH_ANS"
      }, {
        "value" : "The certificate path is not trusted!",
        "nameId": "QUAL_TRUSTED_CERT_PATH_ANS"
      } ],
      "warnings" : [ {
        "value": "The signature/seal is an INDETERMINATE AdES!",
        "nameId" : "QUAL_IS_ADES_IND"
      } ],
      "infos" : [ ]
    },
    "validationCertificateQualification" : [ ],
    "id" : null,
    "signatureQualification": "NA"
 },
 "id" : "id-afde782436468dd74eeb181f7ce110e1",
  "counterSignature" : null
} ],
"certificate" : null,
"basicBuildingBlocks" : [ {
  "fc" : {
    "constraint" : [ {
      "name" : {
        "value" : "Is the expected format found?",
        "nameId" : "BBB_FC_IEFF"
      },
      "status" : "OK",
      "error" : null,
      "warning" : null,
      "info" : null,
      "additionalInfo" : null,
      "id" : null
    } ],
    "conclusion" : {
      "indication": "PASSED",
      "subIndication" : null,
      "errors" : [ ],
      "warnings" : [ ],
      "infos" : [ ]
   }
 },
  "isc" : {
    "constraint" : [ {
      "name" : {
        "value": "Is there an identified candidate for the signing certificate?",
```

```
"nameId" : "BBB_ICS_ISCI"
          },
          "status" : "OK",
          "error" : null,
          "warning" : null,
          "info" : null,
          "additionalInfo" : null,
          "id" : null
        }, {
          "name" : {
            "value" : "Is the signed attribute: 'signing-certificate' present?",
            "nameId" : "BBB ICS ISASCP"
          },
          "status" : "OK",
          "error" : null,
          "warning" : null,
          "info" : null,
          "additionalInfo" : null,
          "id" : null
        }, {
          "name" : {
            "value" : "Is the signed attribute: 'cert-digest' of the certificate
present?",
            "nameId" : "BBB_ICS_ISACDP"
          "status" : "OK",
          "error" : null,
          "warning" : null,
          "info" : null,
          "additionalInfo" : null,
          "id" : null
        }, {
            "value" : "Is the certificate's digest value valid?",
            "nameId" : "BBB_ICS_ICDVV"
          },
          "status" : "OK",
          "error" : null,
          "warning" : null,
          "info" : null,
          "additionalInfo" : null,
          "id" : null
        }, {
          "name" : {
            "value" : "Are the issuer distinguished name and the serial number
equal?",
            "nameId" : "BBB_ICS_AIDNASNE"
          "status" : "OK",
          "error" : null,
          "warning" : null,
```

```
"info" : null,
    "additionalInfo" : null,
    "id" : null
  } ],
  "conclusion" : {
    "indication": "PASSED",
    "subIndication" : null,
    "errors" : [ ],
    "warnings" : [ ],
    "infos" : [ ]
  },
  "certificateChain" : {
    "chainItem" : [ {
      "source": "SIGNATURE",
      "id": "F0FF0B4514D316304F2817DBA0BFB05DEDB98527C0E47C73E8D8FDFE16DF267E"
      "source": "SIGNATURE",
      "id": "6F35DE3965B9A69BC3661D1A355B0AE60907ADB741CC1911EFD0F3BE72D6A6E9"
    } ]
  }
},
"vci" : {
  "constraint" : [ {
    "name" : {
      "value": "Is the signature policy known?",
      "nameId" : "BBB_VCI_ISPK"
    },
    "status" : "OK",
    "error" : null,
    "warning" : null,
    "info" : null,
    "additionalInfo" : null,
    "id" : null
  } ],
  "conclusion" : {
    "indication": "PASSED",
    "subIndication" : null,
    "errors" : [ ],
    "warnings" : [ ],
    "infos" : [ ]
  }
},
"cv" : {
  "constraint" : [ {
    "name" : {
      "value": "Is the reference data object found?",
      "nameId" : "BBB_CV_IRDOF"
    "status" : "OK",
    "error" : null,
    "warning" : null,
```

```
"info" : null,
  "additionalInfo" : "Reference : r-id-1",
  "id" : null
}, {
  "name" : {
    "value": "Is the reference data object intact?",
    "nameId" : "BBB_CV_IRDOI"
  },
  "status" : "OK",
  "error" : null,
  "warning" : null,
  "info" : null,
  "additionalInfo": "Reference: r-id-1",
  "id" : null
}, {
  "name" : {
    "value": "Is the reference data object found?",
    "nameId" : "BBB_CV_IRDOF"
  },
  "status" : "OK",
  "error" : null,
  "warning" : null,
  "info" : null,
  "additionalInfo": "Reference: #xades-id-afde782436468dd74eeb181f7ce110e1",
  "id" : null
}, {
    "value" : "Is the reference data object intact?",
    "nameId" : "BBB_CV_IRDOI"
  },
  "status" : "OK",
  "error" : null,
  "warning" : null,
  "info" : null,
  "additionalInfo": "Reference: #xades-id-afde782436468dd74eeb181f7ce110e1",
  "id" : null
}, {
  "name" : {
    "value": "Is the signature intact?",
    "nameId" : "BBB_CV_ISI"
  },
  "status" : "OK",
  "error" : null,
  "warning" : null,
  "info" : null,
  "additionalInfo" : null,
  "id" : null
} ],
"conclusion" : {
  "indication": "PASSED",
  "subIndication" : null,
```

```
"errors" : [ ],
          "warnings" : [ ],
          "infos" : [ ]
       }
      },
      "sav" : {
        "constraint" : [ {
          "name" : {
            "value": "Is signed qualifying property: 'signing-time' present?",
            "nameId" : "BBB_SAV_ISQPSTP"
          },
          "status" : "OK",
          "error" : null,
          "warning" : null,
          "info" : null,
          "additionalInfo" : null,
          "id" : null
        }, {
          "name" : {
            "value" : "Are signature cryptographic constraints met?",
            "nameId" : "ASCCM"
          },
          "status" : "OK",
          "error" : null,
          "warning" : null,
          "info" : null,
          "additionalInfo": "Validation time: 2018-11-21 09:55",
          "id" : null
        } ],
        "conclusion" : {
          "indication" : "PASSED",
          "subIndication" : null,
          "errors" : [ ],
          "warnings" : [ ],
          "infos" : [ ]
       }
     },
      "xcv" : {
        "constraint" : [ {
          "name" : {
            "value" : "Can the certificate chain be built till the trust anchor?",
            "nameId" : "BBB_XCV_CCCBB"
          },
          "status": "NOT OK",
            "value" : "The certificate chain for signature is not trusted, there is no
trusted anchor.",
            "nameId" : "BBB_XCV_CCCBB_SIG_ANS"
          "warning" : null,
          "info" : null,
```

```
"additionalInfo" : null,
          "id" : null
        }],
        "conclusion" : {
          "indication" : "INDETERMINATE",
          "subIndication": "NO CERTIFICATE CHAIN FOUND",
          "errors" : [ {
            "value" : "The certificate chain for signature is not trusted, there is no
trusted anchor.",
            "nameId" : "BBB_XCV_CCCBB_SIG_ANS"
          "warnings" : [ ],
          "infos" : [ ]
        },
        "subXCV" : [ ]
      "psv" : null,
      "pcv" : null,
      "vts" : null,
      "certificateChain" : {
        "chainItem" : [ {
          "source": "SIGNATURE",
          "id": "F0FF0B4514D316304F2817DBA0BFB05DEDB98527C0E47C73E8D8FDFE16DF267E"
        }, {
          "source": "SIGNATURE",
          "id": "6F35DE3965B9A69BC3661D1A355B0AE60907ADB741CC1911EFD0F3BE72D6A6E9"
       } ]
      },
      "conclusion" : {
        "indication" : "INDETERMINATE",
        "subIndication" : "NO_CERTIFICATE_CHAIN_FOUND",
        "errors" : [ {
          "value" : "The certificate chain for signature is not trusted, there is no
trusted anchor.",
          "nameId" : "BBB_XCV_CCCBB_SIG_ANS"
        } ],
        "warnings" : [ ],
        "infos" : [ ]
      "id": "id-afde782436468dd74eeb181f7ce110e1",
     "type" : "SIGNATURE"
    } ],
    "tlanalysis" : [ ]
 }
}
```