```
<DiagnosticData xmlns="http://dss.esig.europa.eu/validation/diagnostic">
    <DocumentName>testdocument.pdf</DocumentName>
    <ValidationDate>2018-02-23T05:50:46</ValidationDate>
    <Signatures>
        <Signature Id="id-
2056753e8b67ab9c96a6fe80ec9f619f8e9b4505b66b078c7a2b6e151edc2bbb">
            <SignatureFilename>testdocument.pdf</SignatureFilename>
            <DateTime>2017-10-27T11:54:56</DateTime>
            <SignatureFormat>PAdES-BASE-LTA</SignatureFormat>
            <StructuralValidation>
                <Valid>true</Valid>
            </StructuralValidation>
            <BasicSignature>
                <EncryptionAlgoUsedToSignThisToken>
RSA</EncryptionAlgoUsedToSignThisToken>
                <KeyLengthUsedToSignThisToken>2048</KeyLengthUsedToSignThisToken>
                <DigestAlgoUsedToSignThisToken>SHA256</DigestAlgoUsedToSignThisToken>
                <ReferenceDataFound>true</ReferenceDataFound>
                <ReferenceDataIntact>true</ReferenceDataIntact>
                <SignatureIntact>true</SignatureIntact>
                <SignatureValid>true</SignatureValid>
            </BasicSignature>
            <SigningCertificate Id=
"021EC5069EB8A903BD62B6769EDDFE439DFA90A720C9A362D5FE76B9C31D0302">
                <AttributePresent>true</AttributePresent>
                <DigestValuePresent>true</DigestValuePresent>
                <DigestValueMatch>true</DigestValueMatch>
                <IssuerSerialMatch>true</IssuerSerialMatch>
            </SigningCertificate>
            <CertificateChain>
                <ChainItem Id=
"021EC5069EB8A903BD62B6769EDDFE439DFA90A720C9A362D5FE76B9C31D0302">
                    <Source>UNKNOWN</Source>
                </ChainItem>
                <ChainItem Id=
"80AC352930875BA0AFE7F70DD389130C8E1E7BEFFDC96477356AD2A9E003AD2B">
                    <Source>UNKNOWN</Source>
                </ChainItem>
                <ChainItem Id=
"702DD5C1A093CF0A9D71FADD9BF9A7C5857D89FB73B716E867228B3C2BEB968F">
                    <Source>TRUSTED_LIST</Source>
                </ChainItem>
            </CertificateChain>
            <ContentType>application/pdf</ContentType>
            <CommitmentTypeIndication/>
            <ClaimedRoles/>
            <Timestamps>
                <Timestamp Id=
"F8B72B7574450E84664DE88950BC781CA2528CF5B39ABB3E1F93947B752BE79F" Type=
"SIGNATURE_TIMESTAMP">
```

```
                    <ProductionTime>2017-10-27T11:55:08</ProductionTime>
                    <SignedDataDigestAlgo>SHA512</SignedDataDigestAlgo>

<EncodedSignedDataDigestValue>kS17/pxPekqLwE8UcpnhxyZd/8gkQ8IAhho9KI+2yuh25qyB4qS7ozZ7
L85YSssCy66ByRGweAG/mwK8RfXJoA==</EncodedSignedDataDigestValue>
                    <MessageImprintDataFound>true</MessageImprintDataFound>
                    <MessageImprintDataIntact>true</MessageImprintDataIntact>
                    <BasicSignature>
                        <EncryptionAlgoUsedToSignThisToken>
RSA</EncryptionAlgoUsedToSignThisToken>
                        <KeyLengthUsedToSignThisToken>
2048</KeyLengthUsedToSignThisToken>
                        <DigestAlgoUsedToSignThisToken>
SHA512</DigestAlgoUsedToSignThisToken>
                        <ReferenceDataFound>true</ReferenceDataFound>
                        <ReferenceDataIntact>true</ReferenceDataIntact>
                        <SignatureIntact>true</SignatureIntact>
                        <SignatureValid>true</SignatureValid>
                    </BasicSignature>
                    <SigningCertificate Id=
"EE3C22E06087BFEC213709AD3E7F2DDA9CE9D19CE238DCA81A6433E9070A9FBE"/>
                    <CertificateChain>
                        <ChainItem Id=
"EE3C22E06087BFEC213709AD3E7F2DDA9CE9D19CE238DCA81A6433E9070A9FBE">
                            <Source>TIMESTAMP</Source>
                        </ChainItem>
                        <ChainItem Id=
"702DD5C1A093CF0A9D71FADD9BF9A7C5857D89FB73B716E867228B3C2BEB968F">
                            <Source>TRUSTED_LIST</Source>
                        </ChainItem>
                    </CertificateChain>
                    <TimestampedObjects>
                        <TimestampedObject Id="id-
2056753e8b67ab9c96a6fe80ec9f619f8e9b4505b66b078c7a2b6e151edc2bbb" Category="SIGNATURE
"/>
                        <TimestampedObject Category="CERTIFICATE">
                            <DigestAlgoAndValue>
                                <DigestMethod>SHA256</DigestMethod>

<DigestValue>Ah7FBp64qQO9YrZ2nt3+Q536kKcgyaNi1f52ucMdAwI=</DigestValue>
                            </DigestAlgoAndValue>
                        </TimestampedObject>
                    </TimestampedObjects>
                </Timestamp>
                <Timestamp Id=
"7F9B88A8161CC87905298FF8E0CD080516452FBA1480DD6AFAE38B7DD18E2A1B" Type=
"ARCHIVE_TIMESTAMP">
                    ....
                </Timestamp>
            </Timestamps>
            <SignatureScopes>
```

```
                <SignatureScope name="PDF previous version #1" scope=
"PdfByteRangeSignatureScope">The document byte range: [0, 9258, 32602,
495939]</SignatureScope>
            </SignatureScopes>
        </Signature>
    </Signatures>
    <UsedCertificates>
        <Certificate Id=
"021EC5069EB8A903BD62B6769EDDFE439DFA90A720C9A362D5FE76B9C31D0302">
            <SubjectDistinguishedName Format="CANONICAL"
>2.5.4.5=#130b38373035333032363231,2.5.4.42=#130b456c696e65204765726461,2.5.4.4=#130
d56616e205261656d646f6e636b,cn=E van R (signature),c=be</SubjectDistinguishedName>
            <SubjectDistinguishedName Format="RFC2253"
>2.5.4.5=#130b38373035333032363231,2.5.4.42=#130b456c696e65204765726461,2.5.4.4=#130
d56616e205261656d646f6e636b,CN=E Van R (Signature),C=BE</SubjectDistinguishedName>
            <IssuerDistinguishedName Format="CANONICAL"
>2.5.4.5=#130632303137313130,cn=citizen
ca,o=http://repository.eid.belgium.be/,c=be</IssuerDistinguishedName>
            <IssuerDistinguishedName Format="RFC2253"
>2.5.4.5=#130632303137313130,CN=Citizen
CA,O=http://repository.eid.belgium.be/,C=BE</IssuerDistinguishedName>
            <SerialNumber>21267647932559290630671294378886251870</SerialNumber>
            <CommonName>E Van R (Signature)</CommonName>
            <CountryName>BE</CountryName>
            <GivenName>E G</GivenName>
            <Surname>Van R</Surname>
            <AuthorityInformationAccessUrls>
                <Url>http://certs.eid.belgium.be/belgiumrs4.crt</Url>
            </AuthorityInformationAccessUrls>
            <CRLDistributionPoints>
                <Url>http://crl.eid.belgium.be/eidc201710.crl</Url>
            </CRLDistributionPoints>
            <OCSPAccessUrls>
                <Url>http://ocsp.eid.belgium.be/2</Url>
            </OCSPAccessUrls>
            <DigestAlgoAndValues>
                <DigestAlgoAndValue>
                    <DigestMethod>SHA256</DigestMethod>
                    <DigestValue>
Ah7FBp64qQO9YrZ2nt3+Q536kKcgyaNi1f52ucMdAwI=</DigestValue>
                </DigestAlgoAndValue>
                <DigestAlgoAndValue>
                    <DigestMethod>SHA1</DigestMethod>
                    <DigestValue>WWUnOSgChkevrP7omdQeS/plaNQ=</DigestValue>
                </DigestAlgoAndValue>
            </DigestAlgoAndValues>
            <NotAfter>2027-03-13T23:59:59</NotAfter>
            <NotBefore>2017-05-15T16:19:53</NotBefore>
            <PublicKeySize>2048</PublicKeySize>
            <PublicKeyEncryptionAlgo>RSA</PublicKeyEncryptionAlgo>
            <KeyUsageBits>
```

```
                <KeyUsage>nonRepudiation</KeyUsage>
            </KeyUsageBits>
            <ExtendedKeyUsages/>
            <IdPkixOcspNoCheck>false</IdPkixOcspNoCheck>
            <BasicSignature>
                <EncryptionAlgoUsedToSignThisToken>
RSA</EncryptionAlgoUsedToSignThisToken>
                <KeyLengthUsedToSignThisToken>4096</KeyLengthUsedToSignThisToken>
                <DigestAlgoUsedToSignThisToken>SHA256</DigestAlgoUsedToSignThisToken>
                <ReferenceDataFound>true</ReferenceDataFound>
                <ReferenceDataIntact>true</ReferenceDataIntact>
                <SignatureIntact>true</SignatureIntact>
                <SignatureValid>true</SignatureValid>
            </BasicSignature>
            <SigningCertificate Id=
"80AC352930875BA0AFE7F70DD389130C8E1E7BEFFDC96477356AD2A9E003AD2B"/>
            <CertificateChain>
                <ChainItem Id=
"80AC352930875BA0AFE7F70DD389130C8E1E7BEFFDC96477356AD2A9E003AD2B">
                    <Source>UNKNOWN</Source>
                </ChainItem>
                <ChainItem Id=
"702DD5C1A093CF0A9D71FADD9BF9A7C5857D89FB73B716E867228B3C2BEB968F">
                    <Source>TRUSTED_LIST</Source>
                </ChainItem>
            </CertificateChain>
            <Trusted>false</Trusted>
            <SelfSigned>false</SelfSigned>
            <CertificatePolicies>
                <certificatePolicy cpsUrl="http://repository.eid.belgium.be"
>2.16.56.12.1.1.2.1</certificatePolicy>
            </CertificatePolicies>
            <QCStatementIds>
                <oid Description="qc-compliance">0.4.0.1862.1.1</oid>
                <oid Description="qc-sscd">0.4.0.1862.1.4</oid>
            </QCStatementIds>
            <QCTypes/>
            <TrustedServiceProviders>
                <TrustedServiceProvider>
                    <TSPName>Certipost n.v./s.a.</TSPName>
                    <TSPRegistrationIdentifier>VATBE-
0475396406</TSPRegistrationIdentifier>
                    <CountryCode>BE</CountryCode>
                    <TrustedServices>
                        <TrustedService>
                            <ServiceName>CN=Belgium Root CA4, C=BE</ServiceName>
                            <ServiceType>
http://uri.etsi.org/TrstSvc/Svctype/CA/QC</ServiceType>

<Status>http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted</Status>
                            <StartDate>2016-06-30T22:00:00</StartDate>
                            <CapturedQualifiers>

<Qualifier>http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCQSCDStatusAsInCert</Qu
alifier>
                            </CapturedQualifiers>
                            <AdditionalServiceInfoUris>

<URI>http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/RootCA-QC</URI>

<URI>http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures</URI>
                            </AdditionalServiceInfoUris>
                        </TrustedService>
                    </TrustedServices>
                </TrustedServiceProvider>
            </TrustedServiceProviders>
            <Revocations>
                <Revocation Id=
"021ec5069eb8a903bd62b6769eddfe439dfa90a720c9a362d5fe76b9c31d0302bfc08d553a774d1f440ab
36525a3290e2cc23b46d0ac954ea4d8201faff0d91a">
                    <Origin>SIGNATURE</Origin>
                    <Source>OCSPToken</Source>
                    <Status>true</Status>
                    <ProductionDate>2017-10-27T11:55:08</ProductionDate>
                    <ThisUpdate>2017-10-27T11:55:08</ThisUpdate>
                    <NextUpdate>2017-10-27T11:56:08</NextUpdate>
                    <DigestAlgoAndValues>
                        <DigestAlgoAndValue>
                            <DigestMethod>SHA256</DigestMethod>
                            <DigestValue>
v8CNVTp3TR9ECrNlJaMpDizCO0bQrJVOpNggH6/w2Ro=</DigestValue>
                        </DigestAlgoAndValue>
                        <DigestAlgoAndValue>
                            <DigestMethod>SHA1</DigestMethod>
                            <DigestValue>MRhWbZTCsnogtBv4KZ5GzE2imWA=</DigestValue>
                        </DigestAlgoAndValue>
                    </DigestAlgoAndValues>
                    <BasicSignature>
                        <EncryptionAlgoUsedToSignThisToken>
RSA</EncryptionAlgoUsedToSignThisToken>
                        <KeyLengthUsedToSignThisToken>
2048</KeyLengthUsedToSignThisToken>
                        <DigestAlgoUsedToSignThisToken>
SHA256</DigestAlgoUsedToSignThisToken>
                        <ReferenceDataFound>true</ReferenceDataFound>
                        <ReferenceDataIntact>true</ReferenceDataIntact>
                        <SignatureIntact>true</SignatureIntact>
                        <SignatureValid>true</SignatureValid>
                    </BasicSignature>
                    <SigningCertificate Id=
"CB217219BADFC13B4FEA3EFA43882E9FECE49E542DCDBA83428DC6854499A35F"/>
                    <CertificateChain>
```

```
                        <ChainItem Id=
"CB217219BADFC13B4FEA3EFA43882E9FECE49E542DCDBA83428DC6854499A35F">
                            <Source>OCSP_RESPONSE</Source>
                        </ChainItem>
                        <ChainItem Id=
"80AC352930875BA0AFE7F70DD389130C8E1E7BEFFDC96477356AD2A9E003AD2B">
                            <Source>UNKNOWN</Source>
                        </ChainItem>
                        <ChainItem Id=
"702DD5C1A093CF0A9D71FADD9BF9A7C5857D89FB73B716E867228B3C2BEB968F">
                            <Source>TRUSTED_LIST</Source>
                        </ChainItem>
                    </CertificateChain>
                    <Info/>
                </Revocation>
            </Revocations>
            <Info>
                <Message Id="0">No CRL info found !</Message>
            </Info>
        </Certificate>
        <Certificate Id=
"80AC352930875BA0AFE7F70DD389130C8E1E7BEFFDC96477356AD2A9E003AD2B">
            ...
        </Certificate>
        <Certificate Id=
"702DD5C1A093CF0A9D71FADD9BF9A7C5857D89FB73B716E867228B3C2BEB968F">
            ...
        </Certificate>
        <Certificate Id=
"EE3C22E06087BFEC213709AD3E7F2DDA9CE9D19CE238DCA81A6433E9070A9FBE">
            ...
        </Certificate>
        <Certificate Id=
"CB217219BADFC13B4FEA3EFA43882E9FECE49E542DCDBA83428DC6854499A35F">
            ...
        </Certificate>
    </UsedCertificates>
    <TrustedLists>
        <TrustedList>
            <CountryCode>BE</CountryCode>
            <Url>https://tsl.belgium.be/tsl-be.xml</Url>
            <SequenceNumber>36</SequenceNumber>
            <Version>5</Version>
            <LastLoading>2018-02-23T05:15:00</LastLoading>
            <IssueDate>2018-02-08T00:00:00</IssueDate>
            <NextUpdate>2018-07-30T00:00:00</NextUpdate>
            <WellSigned>true</WellSigned>
        </TrustedList>
    </TrustedLists>
    <ListOfTrustedLists>
        <CountryCode>EU</CountryCode>
        <Url>https://ec.europa.eu/information_society/policy/esignature/trusted-list/tl-mp.xml</Url>
        <SequenceNumber>200</SequenceNumber>
        <Version>5</Version>
        <LastLoading>2018-02-23T05:15:00</LastLoading>
        <IssueDate>2018-02-19T13:00:00</IssueDate>
        <NextUpdate>2018-08-19T00:00:00</NextUpdate>
        <WellSigned>true</WellSigned>
    </ListOfTrustedLists>
</DiagnosticData>
```