```
<ConstraintsParameters Name="QES AdESQC TL based" xmlns=
"http://dss.esig.europa.eu/validation/policy">
    <Description>Validate electronic signatures and indicates whether they are
Advanced electronic Signatures (AdES), AdES supported by a Qualified Certificate
(AdES/QC) or a
        Qualified electronic Signature (QES). All certificates and their related
chains supporting the signatures are validated against the EU Member State Trusted
Lists (this includes
        signer's certificate and certificates used to validate certificate validity
status services - CRLs, OCSP, and time-stamps).
    </Description>
    <ContainerConstraints>
        <AcceptableContainerTypes Level="FAIL">
            <Id>ASiC-S</Id>
            <Id>ASiC-E</Id>
        </AcceptableContainerTypes>
<!--        <ZipCommentPresent Level="WARN" /> -->
<!--        <AcceptableZipComment Level="WARN"> -->
<!--            <Id>mimetype=application/vnd.etsi.asic-s+zip</Id> -->
<!--            <Id>mimetype=application/vnd.etsi.asic-e+zip</Id> -->
<!--        </AcceptableZipComment> -->
        <MimeTypeFilePresent Level="FAIL" />
        <AcceptableMimeTypeFileContent Level="WARN">
            <Id>application/vnd.etsi.asic-s+zip</Id>
            <Id>application/vnd.etsi.asic-e+zip</Id>
        </AcceptableMimeTypeFileContent>
        <ManifestFilePresent Level="FAIL" />
        <AllFilesSigned Level="WARN" />
    </ContainerConstraints>
    <SignatureConstraints>
        <AcceptablePolicies Level="FAIL">
            <Id>ANY_POLICY</Id>
            <Id>NO_POLICY</Id>
        </AcceptablePolicies>
        <PolicyAvailable Level="FAIL" />
        <PolicyHashMatch Level="FAIL" />
        <AcceptableFormats Level="FAIL">
            <Id>*</Id>
        </AcceptableFormats>
        <BasicSignatureConstraints>
            <ReferenceDataExistence Level="FAIL" />
            <ReferenceDataIntact Level="FAIL" />
            <SignatureIntact Level="FAIL" />
            <ProspectiveCertificateChain Level="FAIL" />
<!--            <TrustedServiceTypeIdentifier Level="WARN"> -->
<!--                <Id>http://uri.etsi.org/TrstSvc/Svctype/CA/QC</Id> -->
<!--            </TrustedServiceTypeIdentifier> -->
<!--            <TrustedServiceStatus Level="FAIL"> -->
<!--
<Id>http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision</Id> -->
```

```
<!--
<Id>http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/accredited</Id> -->
<!--
<Id>http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/supervisionincessation</Id> -->
<!--                <Id>http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted</Id>
-->
<!--
<Id>http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn</Id> -->
<!--            </TrustedServiceStatus> -->
            <SigningCertificate>
                <Recognition Level="FAIL" />
                <Signature Level="FAIL" />
                <NotExpired Level="FAIL" />
                <AuthorityInfoAccessPresent Level="WARN" />
                <RevocationInfoAccessPresent Level="WARN" />
                <RevocationDataAvailable Level="FAIL" />
                <RevocationDataNextUpdatePresent Level="WARN" />
                <RevocationDataFreshness Level="WARN" />
                <KeyUsage Level="WARN">
                    <Id>nonRepudiation</Id>
                </KeyUsage>
                <SerialNumberPresent Level="WARN" />
                <NotRevoked Level="FAIL" />
                <NotOnHold Level="FAIL" />
                <NotSelfSigned Level="WARN" />
<!--                <Qualification Level="WARN" /> -->
<!--                <SupportedByQSCD Level="WARN" /> -->
<!--                <IssuedToNaturalPerson Level="INFORM" /> -->
<!--                <IssuedToLegalPerson Level="INFORM" /> -->
                <UsePseudonym Level="INFORM" />
                <Cryptographic Level="FAIL">
                    <AcceptableEncryptionAlgo>
                        <Algo>RSA</Algo>
                        <Algo>DSA</Algo>
                        <Algo>ECDSA</Algo>
                    </AcceptableEncryptionAlgo>
                    <MiniPublicKeySize>
                        <Algo Size="128">DSA</Algo>
                        <Algo Size="1024">RSA</Algo>
                        <Algo Size="192">ECDSA</Algo>
                    </MiniPublicKeySize>
                    <AcceptableDigestAlgo>
                        <Algo>SHA1</Algo>
                        <Algo>SHA224</Algo>
                        <Algo>SHA256</Algo>
                        <Algo>SHA384</Algo>
                        <Algo>SHA512</Algo>
                        <Algo>SHA3-224</Algo>
                        <Algo>SHA3-256</Algo>
                        <Algo>SHA3-384</Algo>
                        <Algo>SHA3-512</Algo>
```

```xml
                    <Algo>RIPEMD160</Algo>
                </AcceptableDigestAlgo>
            </Cryptographic>
        </SigningCertificate>
        <CACertificate>
            <Signature Level="FAIL" />
            <NotExpired Level="FAIL" />
            <RevocationDataAvailable Level="FAIL" />
            <RevocationDataNextUpdatePresent Level="WARN" />
            <RevocationDataFreshness Level="WARN" />
            <NotRevoked Level="FAIL" />
            <NotOnHold Level="FAIL" />
            <Cryptographic Level="FAIL">
                <AcceptableEncryptionAlgo>
                    <Algo>RSA</Algo>
                    <Algo>DSA</Algo>
                    <Algo>ECDSA</Algo>
                </AcceptableEncryptionAlgo>
                <MiniPublicKeySize>
                    <Algo Size="128">DSA</Algo>
                    <Algo Size="1024">RSA</Algo>
                    <Algo Size="192">ECDSA</Algo>
                </MiniPublicKeySize>
                <AcceptableDigestAlgo>
                    <Algo>SHA1</Algo>
                    <Algo>SHA224</Algo>
                    <Algo>SHA256</Algo>
                    <Algo>SHA384</Algo>
                    <Algo>SHA512</Algo>
                    <Algo>SHA3-224</Algo>
                    <Algo>SHA3-256</Algo>
                    <Algo>SHA3-384</Algo>
                    <Algo>SHA3-512</Algo>
                    <Algo>RIPEMD160</Algo>
                </AcceptableDigestAlgo>
            </Cryptographic>
        </CACertificate>
        <Cryptographic Level="FAIL">
            <AcceptableEncryptionAlgo>
                <Algo>RSA</Algo>
                <Algo>DSA</Algo>
                <Algo>ECDSA</Algo>
            </AcceptableEncryptionAlgo>
            <MiniPublicKeySize>
                <Algo Size="128">DSA</Algo>
                <Algo Size="1024">RSA</Algo>
                <Algo Size="192">ECDSA</Algo>
            </MiniPublicKeySize>
            <AcceptableDigestAlgo>
                <Algo>SHA1</Algo>
                <Algo>SHA224</Algo>
```

```
                    <Algo>SHA256</Algo>
                    <Algo>SHA384</Algo>
                    <Algo>SHA512</Algo>
                        <Algo>SHA3-224</Algo>
                        <Algo>SHA3-256</Algo>
                        <Algo>SHA3-384</Algo>
                        <Algo>SHA3-512</Algo>
                    <Algo>RIPEMD160</Algo>
                </AcceptableDigestAlgo>
            </Cryptographic>
        </BasicSignatureConstraints>
        <SignedAttributes>
            <SigningCertificatePresent Level="FAIL" />
            <SigningCertificateSigned Level="FAIL" />
            <CertDigestPresent Level="FAIL" />
            <CertDigestMatch Level="FAIL" />
            <IssuerSerialMatch Level="WARN" />
            <SigningTime Level="FAIL" />
<!--        <ContentType Level="FAIL" value="1.2.840.113549.1.7.1" />
            <ContentHints Level="FAIL" value="*" />
            <CommitmentTypeIndication Level="FAIL">
                <Id>1.2.840.113549.1.9.16.6.1</Id>
                <Id>1.2.840.113549.1.9.16.6.4</Id>
                <Id>1.2.840.113549.1.9.16.6.5</Id>
                <Id>1.2.840.113549.1.9.16.6.6</Id>
            </CommitmentTypeIndication>
            <SignerLocation Level="FAIL" />
            <ContentTimeStamp Level="FAIL" /> -->
        </SignedAttributes>
        <UnsignedAttributes>
<!--        <CounterSignature Level="IGNORE" /> check presence -->
        </UnsignedAttributes>
    </SignatureConstraints>
    <Timestamp>
        <TimestampDelay Level="FAIL" Unit="DAYS" Value="0" />
        <MessageImprintDataFound Level="FAIL" />
        <MessageImprintDataIntact Level="FAIL" />
        <RevocationTimeAgainstBestSignatureTime Level="FAIL" />
        <BestSignatureTimeBeforeIssuanceDateOfSigningCertificate Level="FAIL" />
        <SigningCertificateValidityAtBestSignatureTime Level="FAIL" />
        <AlgorithmReliableAtBestSignatureTime Level="FAIL" />
        <Coherence Level="WARN" />
        <BasicSignatureConstraints>
            <ReferenceDataExistence Level="FAIL" />
            <ReferenceDataIntact Level="FAIL" />
            <SignatureIntact Level="FAIL" />
            <ProspectiveCertificateChain Level="WARN" />
            <SigningCertificate>
                <Recognition Level="FAIL" />
                <Signature Level="FAIL" />
                <NotExpired Level="FAIL" />
                <RevocationDataAvailable Level="FAIL" />
                <RevocationDataNextUpdatePresent Level="WARN" />
                <RevocationDataFreshness Level="WARN" />
                <NotRevoked Level="FAIL" />
                <NotOnHold Level="FAIL" />
                <NotSelfSigned Level="WARN" />
                <Cryptographic Level="FAIL">
                    <AcceptableEncryptionAlgo>
                        <Algo>RSA</Algo>
                        <Algo>DSA</Algo>
                        <Algo>ECDSA</Algo>
                    </AcceptableEncryptionAlgo>
                    <MiniPublicKeySize>
                        <Algo Size="128">DSA</Algo>
                        <Algo Size="1024">RSA</Algo>
                        <Algo Size="192">ECDSA</Algo>
                    </MiniPublicKeySize>
                    <AcceptableDigestAlgo>
                        <Algo>SHA1</Algo>
                        <Algo>SHA224</Algo>
                        <Algo>SHA256</Algo>
                        <Algo>SHA384</Algo>
                        <Algo>SHA512</Algo>
                        <Algo>SHA3-224</Algo>
                        <Algo>SHA3-256</Algo>
                        <Algo>SHA3-384</Algo>
                        <Algo>SHA3-512</Algo>
                        <Algo>RIPEMD160</Algo>
                    </AcceptableDigestAlgo>
                </Cryptographic>
            </SigningCertificate>
            <CACertificate>
                <Signature Level="FAIL" />
                <NotExpired Level="FAIL" />
                <RevocationDataAvailable Level="WARN" />
                <RevocationDataNextUpdatePresent Level="WARN" />
                <RevocationDataFreshness Level="WARN" />
                <NotRevoked Level="FAIL" />
                <NotOnHold Level="FAIL" />
                <Cryptographic Level="FAIL">
                    <AcceptableEncryptionAlgo>
                        <Algo>RSA</Algo>
                        <Algo>DSA</Algo>
                        <Algo>ECDSA</Algo>
                    </AcceptableEncryptionAlgo>
                    <MiniPublicKeySize>
                        <Algo Size="128">DSA</Algo>
                        <Algo Size="1024">RSA</Algo>
                        <Algo Size="192">ECDSA</Algo>
                    </MiniPublicKeySize>
                    <AcceptableDigestAlgo>
```

```
                        <Algo>SHA1</Algo>
                        <Algo>SHA224</Algo>
                        <Algo>SHA256</Algo>
                        <Algo>SHA384</Algo>
                        <Algo>SHA512</Algo>
                        <Algo>SHA3-224</Algo>
                        <Algo>SHA3-256</Algo>
                        <Algo>SHA3-384</Algo>
                        <Algo>SHA3-512</Algo>
                        <Algo>RIPEMD160</Algo>
                    </AcceptableDigestAlgo>
                </Cryptographic>
            </CACertificate>
            <Cryptographic Level="FAIL">
                <AcceptableEncryptionAlgo>
                    <Algo>RSA</Algo>
                    <Algo>DSA</Algo>
                    <Algo>ECDSA</Algo>
                </AcceptableEncryptionAlgo>
                <MiniPublicKeySize>
                    <Algo Size="128">DSA</Algo>
                    <Algo Size="1024">RSA</Algo>
                    <Algo Size="192">ECDSA</Algo>
                </MiniPublicKeySize>
                <AcceptableDigestAlgo>
                    <Algo>SHA1</Algo>
                    <Algo>SHA224</Algo>
                    <Algo>SHA256</Algo>
                    <Algo>SHA384</Algo>
                    <Algo>SHA512</Algo>
                    <Algo>SHA3-224</Algo>
                    <Algo>SHA3-256</Algo>
                    <Algo>SHA3-384</Algo>
                    <Algo>SHA3-512</Algo>
                    <Algo>RIPEMD160</Algo>
                </AcceptableDigestAlgo>
            </Cryptographic>
        </BasicSignatureConstraints>
    </Timestamp>
    <Revocation>
        <RevocationFreshness Level="FAIL" Unit="DAYS" Value="0" />
        <BasicSignatureConstraints>
            <ReferenceDataExistence Level="FAIL" />
            <ReferenceDataIntact Level="FAIL" />
            <SignatureIntact Level="FAIL" />
            <ProspectiveCertificateChain Level="WARN" />
            <SigningCertificate>
                <Recognition Level="FAIL" />
                <Signature Level="FAIL" />
                <NotExpired Level="FAIL" />
                <RevocationDataAvailable Level="FAIL" />
                <RevocationDataNextUpdatePresent Level="WARN" />
                <RevocationDataFreshness Level="WARN" />
                <NotRevoked Level="FAIL" />
                <NotOnHold Level="FAIL" />
                <Cryptographic Level="WARN">
                    <AcceptableEncryptionAlgo>
                        <Algo>RSA</Algo>
                        <Algo>DSA</Algo>
                        <Algo>ECDSA</Algo>
                    </AcceptableEncryptionAlgo>
                    <MiniPublicKeySize>
                        <Algo Size="128">DSA</Algo>
                        <Algo Size="1024">RSA</Algo>
                        <Algo Size="192">ECDSA</Algo>
                    </MiniPublicKeySize>
                    <AcceptableDigestAlgo>
                        <Algo>SHA1</Algo>
                        <Algo>SHA224</Algo>
                        <Algo>SHA256</Algo>
                        <Algo>SHA384</Algo>
                        <Algo>SHA512</Algo>
                        <Algo>SHA3-224</Algo>
                        <Algo>SHA3-256</Algo>
                        <Algo>SHA3-384</Algo>
                        <Algo>SHA3-512</Algo>
                        <Algo>RIPEMD160</Algo>
                    </AcceptableDigestAlgo>
                </Cryptographic>
            </SigningCertificate>
            <CACertificate>
                <Signature Level="FAIL" />
                <NotExpired Level="FAIL" />
                <RevocationDataAvailable Level="WARN" />
                <RevocationDataNextUpdatePresent Level="WARN" />
                <RevocationDataFreshness Level="WARN" />
                <NotRevoked Level="FAIL" />
                <NotOnHold Level="FAIL" />
                <Cryptographic Level="FAIL">
                    <AcceptableEncryptionAlgo>
                        <Algo>RSA</Algo>
                        <Algo>DSA</Algo>
                        <Algo>ECDSA</Algo>
                    </AcceptableEncryptionAlgo>
                    <MiniPublicKeySize>
                        <Algo Size="128">DSA</Algo>
                        <Algo Size="1024">RSA</Algo>
                        <Algo Size="192">ECDSA</Algo>
                    </MiniPublicKeySize>
                    <AcceptableDigestAlgo>
                        <Algo>SHA1</Algo>
                        <Algo>SHA224</Algo>
                        <Algo>SHA256</Algo>
                        <Algo>SHA384</Algo>
                        <Algo>SHA512</Algo>
                        <Algo>SHA3-224</Algo>
                        <Algo>SHA3-256</Algo>
                        <Algo>SHA3-384</Algo>
                        <Algo>SHA3-512</Algo>
                        <Algo>RIPEMD160</Algo>
                    </AcceptableDigestAlgo>
                </Cryptographic>
            </CACertificate>
            <Cryptographic Level="FAIL">
                <AcceptableEncryptionAlgo>
                    <Algo>RSA</Algo>
                    <Algo>DSA</Algo>
                    <Algo>ECDSA</Algo>
                </AcceptableEncryptionAlgo>
                <MiniPublicKeySize>
                    <Algo Size="128">DSA</Algo>
                    <Algo Size="1024">RSA</Algo>
                    <Algo Size="192">ECDSA</Algo>
                </MiniPublicKeySize>
                <AcceptableDigestAlgo>
                    <Algo>SHA1</Algo>
                    <Algo>SHA224</Algo>
                    <Algo>SHA256</Algo>
                    <Algo>SHA384</Algo>
                    <Algo>SHA512</Algo>
                    <Algo>SHA3-224</Algo>
                    <Algo>SHA3-256</Algo>
                    <Algo>SHA3-384</Algo>
                    <Algo>SHA3-512</Algo>
                    <Algo>RIPEMD160</Algo>
                </AcceptableDigestAlgo>
            </Cryptographic>
        </BasicSignatureConstraints>
    </Revocation>
    <Cryptographic />
    <!-- <Cryptographic> <AlgoExpirationDate Format="yyyy-MM-dd"> <Algo Date="2017-02-
24">SHA1</Algo> <Algo Date="2035-02-24">SHA224</Algo> <Algo Date="2035-02-
24">SHA256</Algo> <Algo
        Date="2035-02-24">SHA384</Algo> <Algo Date="2035-02-24">SHA512</Algo> <Algo
Date="2017-02-24">RIPEMD160</Algo> <Algo Date="2017-02-24">DSA128</Algo> <Algo
Date="2015-02-24">RSA1024</Algo>
        <Algo Date="2015-02-24">RSA1536</Algo> <Algo Date="2020-02-24">RSA2048</Algo>
<Algo Date="2020-02-24">RSA3072</Algo> <Algo Date="2035-02-24">RSA4096</Algo> <Algo
Date="2035-02-24">ECDSA192</Algo>
        <Algo Date="2035-02-24">ECDSA256</Algo> </AlgoExpirationDate> </Cryptographic>
-->

    <!-- eIDAS REGL 910/EU/2014 -->
```

```xml
    <eIDAS>
        <TLFreshness Level="WARN" Unit="HOURS" Value="6" />
        <TLNotExpired Level="FAIL" />
        <TLWellSigned Level="WARN" />
        <TLVersion Level="FAIL" value="5" />
        <TLConsistency Level="FAIL" />
    </eIDAS>
</ConstraintsParameters>
```