# Provider's (manufacturer's) declaration of the QES application to declare meeting the requirements in QES creation, verification and validation under Regulation (EU) No 910/2014

The form contains an overview of features of application for qualified electronic signature /seal (QES), declared by the application's manufacturer and their correctness can be confirmed by the certification body.
The form is signed/sealed by the provider (manufacturer) of the application and as the certification is voluntary, the form can be signed/sealed also by the certification body. The certification body is the conformity assessment body defined in Article 3 of the Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market. The certification of the application is carried out in accordance with Articles 27, 37, 32 a 40 of the Regulation (EU) No 910/2014 mutatis mutandis regarding the requirements for usage of QSCD (the requirements are consequence of certification according to Article 30 (3) of the Regulation (EU) No 910/2014).
The supervision body for the trust services may publish the declaration of the manufacturer of QES application on its website. Together with declaration the supervision body may also publish document with findings of non-conformity with the legislative requirements. These findings were acquired during supervision activities of trust services and the supervision body may have reviewed these findings in cooperation with the certification body.
QES application has to create, verify and provide the result of the QES validation process only if the format of the signature/seal is one of the formats stated in the Annex of the Commission Implementing Decision (EU) 2015/1506 of 8 September 2015 laying down specifications relating to formats of advanced electronic signatures and advanced seals to be recognized by public sector bodies pursuant to Articles 27(5) and 37(5) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market; hereinafter referred to as „Decision (EU) 2015/1506“). Mapping of the legislative requirements defined in the Regulation (EU) No 910/2014 into technical processes is defined in the document of the supervision body "Supervision Scheme" until implementation acts to some Articles of the Regulation (EU) No 910/2014 will be issued.
During the validation process QES application has to review at least all the points of the procedure for the creation of the QES validation report defined in the Supervision Scheme according to Article 33 of the Regulation (EU) No 910/2014 defining qualified validation service for qualified electronic signatures.
Annex to this declaration of the provider (manufacturer) of the QES application may contain also declaration as a form in accordance with Annex A to ISO 14533 for the respective QES format.

| The provider (manufacturer) | Certified by |
|---|---|

# 1 Application for QES

**Data on provider (manufacturer)**

Business name: _____

Company Registration Number: _____

Address: _____

Website address: _____

**Data on application**

Application name: _____

Version: _____

Requirements (OS, …): _____

Website of installation package: _____

SHA256 hash of installation package: _____

Main application module: _____

SHA256 hash of main module: _____

Name and SHA256 hash of other application modules if not validated by a main application module:

# 2 QES formats supported by application

## 2.1 Application creates or validates QES

(Creates/Validates)

2.1.1 ☐/☐ **CMS AdES** - Basic profile of CAdES ETSI TS 103173 v.2.2.1
(see http://www.etsi.org/deliver/etsi_ts/103100_103199/103173/02.02.01_60/ts_103173v020201p.pdf )

2.1.2 ☐/☐ **PDF AdES** - Basic profile of PAdES ETSI TS 103172 v.2.2.2
(see http://www.etsi.org/deliver/etsi_ts/103100_103199/103172/02.02.02_60/ts_103172v020202p.pdf )

2.1.3 ☐/☐ **XML AdES** - Basic profile of XAdES ETSI TS 103171 v.2.1.1
(see http://www.etsi.org/deliver/etsi_ts/103100_103199/103171/02.01.01_60/ts_103171v020101p.pdf )

2.1.4 ☐/☐ **ASiC** - Basic profile of signing container in ASiC format ETSI TS 103174 v.2.2.1
(see http://www.etsi.org/deliver/etsi_ts/103100_103199/103174/02.02.01_60/ts_103174v020201p.pdf )

5 ☐ It prevents QES validation if the signature contains Manifest in XML AdES, because Manifest enables **not to validate** the hash value of the electronic document, thus putting the signature (seal) format using the Manifest, according to Articles 27(1) and (2) and 37(1) and (2) of the Regulation (EU) No 910/2014, into the category of methods for alternative formats, when it is necessary to offer other Member States the validation possibilities of advanced electronic signature (seal) which will be, where possible, suitable for automated processing, thus making the signature not complying with the Annex of the Decision (EU) 2015/1506.

6 ☐ If Manifest or other methods for alternative formats in accordance with Articles 27(1) and (2) and 37(1) and (2) of the Regulation (EU) No 910/2014 (only if the signature is not QES when the qualified certificate does not contain QSCD identification - OID 0.4.0.1862.1.4) are used in XML AdES and the application distinguishes specific rules from the signature or from the signed data, for example for Manifest usage or other method for alternative formats, the validation will be carried out under these specific rules, otherwise the impossibility of validation will be declared.

## 2.2 Application creates or validates QES conformity with (B) level:

(Creates/Validates)

1 ☐/☐ CAdES – EPES (internal SP)
2 ☐/☐ CAdES – (external SP)
3 ☐/☐ XAdES – EPES (internal SP)
4 ☐/☐ XAdES – (external SP)
5 ☐/☐ PAdES – EPES (internal SP)
6 ☐/☐ PAdES – (external SP)
7 ☐/☐ PAdES – DTS (external SP)
8 ☐/☐ ASiC-S CAdES
9 ☐/☐ ASiC-S XAdES
10 ☐/☐ ASiC-S Time-stamp token (external SP)
11 ☐/☐ ASiC-E CAdES
12 ☐/☐ ASiC-E XAdES
13 ☐/☐ ASiC-E Time-stamp (external SP)

## 2.3 Application creates or validates QES conformity of QES with (T or LT) level

(Creates/Validates)

1 ☐/☐ CAdES – T (IETF RFC 3161)
2 ☐/☐ CAdES – T (IETF RFC 6960 STS over OCSP)
3 ☐/☐ CAdES – LT
4 ☐/☐ XAdES – T (IETF RFC 3161)
5 ☐/☐ XAdES – T (IETF RFC 6960 STS over OCSP)
6 ☐/☐ XAdES – LT
7 ☐/☐ PAdES – T (IETF RFC 3161)
8 ☐/☐ PAdES – T (IETF RFC 6960 STS over OCSP)
9 ☐/☐ PAdES – LT

## 2.4 Application creates or validates QES conformity with (LTA *) level

(Creates/ Validates)

1 ☐/☐ CAdES – LTA * (according to ETSI EN)
2 ☐/☐ XAdES – LTA * (according to ETSI EN)
3 ☐/☐ PAdES – LTA * (according to ETSI EN)

Abbreviations and notes:

| | |
|---|---|
| SP | Signature Policy (SP) according to Article 11(1), item m) of the Act No 272/2016 Coll. on trust services for electronic transactions in the internal market and on the amendment and supplementing of certain acts (Act on Trust Services) is published on the NSA website (in ASN.1 format in DER coding). |
| EPES | Application works with ASN.1 SP, to which the reference is included in QES, in the item secured by signature, containing SP identification. |
| external SP | If QES does not contain EPES or SP has expired, the application will get SP for validation from a list of SPs published by the NSA, valid at the time when the validated object was provably created (e. g. in accordance with LTA time stamp). |
| STS | Signature Time Stamp whose profile is defined by the document Supervision Scheme. |
| AdES-T | QES contains (qualified electronic) signature time stamp. |
| AdES-DTS | Time Stamp of the document – defined in PDF standard ISO 32000. |
| AdES-LT | Contains T + CRL or OCSP responses to verify the certificates' validity. |
| AdES-LTA | QES contains the information for the Long-Term validation and for ensuring the Availability and integrity. |

* AdES-LTA format is not, due to its deficiencies, required in the Annex of the Commission Implementing Decision (EU) 2015/1506 but its latest version can be used as one of the alternatives in "Qualified preservation service for qualified electronic signatures (seals)" profiled in Chapter 5.4 in the document Supervision Scheme according to current ETSI EN format for CAdES, XAdES and PAdES.

## 2.5 Supported non-mandatory attributes, elements or items protected by QES

(CMS attributes are identified with id- at the beginning) - (XML elements are without id- at the beginning):
(Creates/Validates)

1 ☐/☐ (id-aa-contentHint)
2 ☐/☐ (id-aa-ets-signerLocation)
3 ☐/☐ (id-aa-ets-commitmentType)
4 ☐/☐ (DataObjektFormat)
5 ☐/☐ (SignatureProductionPlace)
6 ☐/☐ (CommitmentTypeIndication)

(Creates/ Validates - PDF entries in a signature dictionary ISO 32000-1/2)

7 ☐/☐ (Location)
8 ☐/☐ (Reason)

## 2.6 Explanations or additional information on the above mentioned points:

## 2.7 Application supports these algorithms and parameters

Secure algorithms for machine processing are published in signature policies on the NSA website. Recommendations according to SOGIS Agreed Cryptographic Mechanisms (see http://sogis.org/uk/supporting_doc_en.html). Algorithms:

1 ☐ sha-256 OID 2.16.840.1.101.3.4.2.1
2 ☐ sha-384 OID 2.16.840.1.101.3.4.2.2
3 ☐ sha-512 OID 2.16.840.1.101.3.4.2.3
4 ☐ sha512-256 OID 2.16.840.1.101.3.4.2.6
5 ☐ sha3-256 OID 2.16.840.1.101.3.4.2.8
6 ☐ sha3-384 OID 2.16.840.1.101.3.4.2.9
7 ☐ sha3-512 OID 2.16.840.1.101.3.4.2.10
8 ☐ dsaWithSha256 OID 2.16.840.1.101.3.4.3.2
9 ☐ dsa-with-sha384 OID 2.16.840.1.101.3.4.3.3
10 ☐ dsa-with-sha512 OID 2.16.840.1.101.3.4.3.4
11 ☐ dsa-with-sha3-256 OID 2.16.840.1.101.3.4.3.6
12 ☐ dsa-with-sha3-384 OID 2.16.840.1.101.3.4.3.7
13 ☐ dsa-with-sha3-512 OID 2.16.840.1.101.3.4.3.8
14 ☐ ecdsaWithSHA256 OID 1.2.840.10045.4.3.2
15 ☐ ecdsaWithSHA384 OID 1.2.840.10045.4.3.3
16 ☐ ecdsaWithSHA512 OID 1.2.840.10045.4.3.4
17 ☐ ecdsa-with-sha3-256 OID 2.16.840.1.101.3.4.3.10
18 ☐ ecdsa-with-sha3-384 OID 2.16.840.1.101.3.4.3.11
19 ☐ ecdsa-with-sha3-512 OID 2.16.840.1.101.3.4.3.12
20 ☐ sha256WithRSAEncryption OID 1.2.840.113549.1.1.11
21 ☐ sha384WithRSAEncryption OID 1.2.840.113549.1.1.12
22 ☐ sha512WithRSAEncryption OID 1.2.840.113549.1.1.13
23 ☐ rsaPSS OID 1.2.840.113549.1.1.10
24 ☐ rsaEncryption OID 1.2.840.113549.1.1.1
25 ☐ ecPublicKey OID 1.2.840.10045.2.1
26 ☐ pkcs1-v1_5 is used only for validation of RSA signatures or seals and not for creation of new signatures
27 ☐ rsassa-pkcs1-v1_5-with-sha3-256 OID 2.16.840.1.101.3.4.3.14
28 ☐ rsassa-pkcs1-v1_5-with-sha3-384 OID 2.16.840.1.101.3.4.3.15
29 ☐ rsassa-pkcs1-v1_5-with-sha3-512 OID 2.16.840.1.101.3.4.3.16

Parameters:

RSA key size _____ minimum, _____ maximum.

DSA key size _____ minimum, _____ maximum.

ECDSA key size _____ minimum, _____ maximum.

Elliptic Curve Domain Parameter Identifiers: Brainpool (RFC5639), NIST (FIPS186-4, Appendix D.1.2), FR (JORF)

30 ☐ brainpoolP256r1OID 1.3.36.3.3.2.8.1.1.7
31 ☐ brainpoolP384r1OID 1.3.36.3.3.2.8.1.1.11
32 ☐ brainpoolP512r1OID 1.3.36.3.3.2.8.1.1.13
33 ☐ nistp256 OID 1.2.840.10045.3.1.7
34 ☐ nistp384 OID 1.3.132.0.34
35 ☐ nistp521 OID 1.3.132.0.35
36 ☐ FRP256v1 OID 1.2.250.1.223.101.256.1

Name and OID of other supported algorithms and parameters:

# 3 User interface

☐3.1 User interface of the application is protected against the change of display settings in the system (colour, size of windows and fonts, transparency, names and size of buttons).

☐ 3.2 The application is to be used only in secure environment under the full control of the user; it is not protected against attacks on operation system (a change of font, password capture, foisting a fake value on QSCD to create QES or several fake QESs).

☐ 3.3 A change of system fonts may cause different display of the content being signed when signing on different computers and may cause different display in signature validation on different computers.

☐ 3.4 The application communicates with QSCD via secure channel that prevents modification or change of data intended for QES creation.

☐ 3.5 The application supports secure PIN entry for QSCD via a keyboard on a reader which will prevent password capture (e.g. PC/SC v2 with Secure PIN Entry (part 10)).

☐ 3.6 The application will notify of danger of secure password entering on a keyboard, if secure password entering is not supported by the key-board (3.5).

☐ 3.7 The application contains a store of trusted certificates and their parameters for validation of certification path.

☐ 3.8 A store of trusted certificates is protected against unauthorized change.

If yes – A store of trusted certificates is protected by:

☐ signature of validator ☐ signature of authority (Admin) ☐ signature of TL

☐ other way:

| |
|---|
| |

☐ 3.9 Application is protected against the change of its code.

If yes – Form of protection against the change of code is:

☐ Component hashes signed by the application are validated at the application launch.

☐ Component hashes are signed and validated at the application launch in OS.

☐ Component hashes can be validated also by external application.

URL application _____

☐ A list of hash values of components for external validation by external application is published.

URL application _____

☐ Otherwise:

3.10 Explanations or additional information on the above mentioned points

# 4. Verification of certificate validity in QES creation, verification and validation

☐ 4.1 Before signing (sealing) it is enabled to display a certificate of a signatory.
☐ 4.2 Before signing (sealing) the validity of a signatory's certificate is verified.
☐ Verification of expiration of a signatory's (seal creator's) certificate.

Verification by ☐ CRL or ☐ OCSP.

4.3 Verification of the certificate validity is ensured by:
☐ CRL ☐ OCSP ☐ Indirect CRL ☐ OCSP authorized in TL
☐ OCSP with controlled positive response (*certHash)*

4.4 The application has implemented the following procedure for the certification path validation [1]:

☐ 4.4.1. The application validates and verifies the validity of a qualified certificate on the basis of a trusted list e.g. http://ep.nbu.gov.sk/kca/tsl/tsl.xml, which contains "trust anchors" with parameters defined in the text of Decision (EU) 2015/1505, for example a trust service with the qualified status may be used only for validation and verification of end user certificates (End Entity) and certificates belonging to this service (issues the certificate to itself – the same organisation).

☐ 4.4.2. The application checks the up-to-date status of a trusted list according to the time of the NSA seal http://ep.nbu.gov.sk/kca/tsl/tsl.xml.p7s.

☐ 4.4.3. According to Chapter 10.3 (Certification path processing procedure - Path processing variables) of ITU-T Rec. X.509 standard or ISO/IEC 9594-8 the application will read initial variable values to check the certification path from TL elements defined in additional XSD which is documented on the NSA website in the document http://ep.nbu.gov.sk/kca/tsl/tlX509XMLSchemaDocumentation.pdf for TL. The elements are following: *PrivateKeyUsagePeriod* which enables to shorten the usage period of a key pair of a trust service for issuing objects (e.g. certificates) against the time interval indicated in the certificate of a trust service with the longest validity period during the qualified status of a trust service, *TLPathLenConstraint*, *TLServiceIdentifier*, *ExplicitAcceptablePolicySet*, *TrustAnchor* and *URLContentTypeAndAuthorizedServiceList*. Based on these data the application will use standard validations according to Chapter 10.3 of ITU-T Rec. X.509 to prevent for example incorrect verification via cross-certificates or to enable an automated verification by other authorized qualified trust service in accordance with Article 4 of the Act No 272/2016 Coll.

☐ 4.4.4. Based on explicit list of certificate policy OIDs the application requires their presence in all certificates of the certification path[2].

☐ 4.4.5. If the validation of certificate policies is required in the certificate extension *policyConstraints* via *policyMapping*, the application will validate certificate policies on the basis of *policyConstraints*, *certificatePolicy* and *policyMapping*.

[1] Procedure according to "SS of Articles 32 and 40 of Regulation (EU) No 910/2014" in the document Supervision Scheme

[2] NSA RCA Certificate Policy OID 1.3.158.36061701.0.0.0.1.2.2

☐ 4.5 The application identifies type of qualified certificate (for signature, for seal or for web) in accordance with the rules specified in the document Supervision Scheme in Chapter 5.2 (SS of Annexes I, III and IV of Regulation (EU) No 910/2014).

☐ 4.6 The application identifies type of signature/seal (Is it qualified?) in accordance with the rules specified in the document Supervision Scheme in Chapter 5.2 (SS of Annexes I, III and IV of Regulation (EU) No 910/2014).

☐ 4.7 It is possible to insert a reference to a signature policy into items protected by QES.
If yes, ☐ the rules from the signature policy are used in signature creation.

☐ 4.8 The application enables to display the content of the signature policy transformed to human readable form.

☐ 4.9 Validation is carried out according to signature policy whose identifier is a part of the signature (protected by QES).

☐ 4.10 Validation of signature is carried out according to signature policy chosen by the validator if the identifier of the signature policy is not a part of the signature.

☐ 4.11 The application enables to insert a time stamp in signature creation procedure.

☐ 4.12 The application enables to insert a time stamp in signature validation procedure.

☐ 4.13 The application validates inserted time stamp in signature validation procedure.

☐ 4.14 The application before inserting a time stamp of LTA conformity level completes signature and signatures of the previous time stamps (with suitable CRL or OCSP) for their verification.

☐ 4.15 The application verifies the last time stamp of LTA level (with current CRL or OCSP).

4.16 Explanations or additional information on the above mentioned points:

# 5 Secure browser

☐ 5.1 Unambiguous determination of the signed/sealed document format is ensured by the application when signing and validating the document by data which are protected by signature. It will be, as a minimum, in accordance with the Supervision Scheme in chapter "SS of Articles 26 and 36 of Regulation (EU) No 910/2014" for item d) of Articles 26 and 36 of the Regulation (EU) No 910/2014.

Protection of the format of the document being signed is ensured by:

☐ MIME ***Content-Type*** value included in the *contentHint* signed CAdES attribute in *contentDescription* field as one-line string.

Example: `Content-Type: text/plain; charset=UTF-8; name="Document.txt"`

☐ MIME ***Content-Type*** value included in one-line in XAdES *Description* element in *DataObjectFormat* element.

Example: `Content-Type: text/plain; charset=UTF-8; name="Document.txt"`

☐ MIME ***MimeType*** in XAdES *MimeType* element in *DataObjectFormat* element.

Example: `<xades:MimeType>application/pdf</xades:MimeType>`

☐ MIME ***Content-Type*** value containing only MIME type and parameters included in the component "file comment" of "4.3.12 Central directory structure" in signed ZIP file. ETSI EN 319 162-1, Clause 4.3.2 and Annex B.1.3

Example: `mimetype=text/plain; charset=UTF-8`

☐ Other:

| |
|---|
| |

☐ 5.2 The application signs/validates and displays document formats listed in Articles 57a to 57d of Decree No 55/2014 Coll. according to Annex No 12 to Decree No 55/2014 Coll. in secure browser in all versions of the application equally.

Values for identification of the signed electronic document format

| **Signed electronic document according to** | **Identifier in the form of file extension** | **Identifier in the form of "Content-type" component in electronic signature** |
|---|---|---|
| § 57a items a) and b) of the first point | ☐ .pdf | application/pdf |
| § 57a item b) of the second point | ☐ .txt | text/plain; charset=UTF-8 |
| § 57a item b) of the third point | ☐ .png | image/png |
| § 57a item c) | ☐ .xml | application/vnd.gov.sk.xmldatacontainer+xml; charset=UTF-8 |

Values for identification of the signing container format

| Signature container | Identifier in the form of file extension | Identifier in the form of "Content-type" component in electronic signature |
|---|---|---|
| § 57b item a) | ☐ .asics, .scs | application/vnd.etsi.asic-s+zip |
| § 57b item a), signed ZIP ETSI EN 319 162-1, 4.3.2, B.1.3 | ☐ .zip | application/zip |
| § 57b item a), extended signature container | ☐ .asice, .sce | application/vnd.etsi.asic-e+zip |

☐ 5.3 It will enable to display a notice window when signing/validating and displaying other document format than the one indicated in Article 57a items a) to c) and in Article 57b item a) of Decree No 55/2014 Coll..

☐ 5.4 The application, in addition to the previous formats, signs/validates and displays the following document formats. The document formats are indicated in the form (identifier in the form of file extension, identifier in the form of "Content-type" component in electronic signature):

5.5 Explanations or additional information on the above mentioned points:

# 6 Additional information

6.1 The application can be used only when meeting the following limitations:

6.2 Supported certified QSCD for qualified electronic signature/seal creation according to restrictions stemming from certification:

6.3 Annexes: (e.g. in the form of http address of the annex, hash SHA256 of the annex):

6.4 Other annexes: