CEF eSignature

esig-validation-tests

Version 1.0

User guide

Reference documents:

Reference	Document	Date	Version
QES V-A	Qualified electronic signature (QES) validation algorithm	07/2018	0.2
ETSI 119 001	ESI: Definitions and abbreviations	03/2016	1.2.1
ETSI TS 103 171	XAdES Baseline profile	03/2018	2.1.1

TABLE OF CONTENTS

PURPOSE AND APPROACH OF THE DOCUMENT

In order to help third parties to validate their implementation of eIDAS requirements regarding electronic signature, the CEF eSignature building block is proposing to publish validation test cases.

As a first step, the focus is on the validation of qualified electronic signatures (QES) according to the *guidelines* "Qualified electronic signature (QES) validation algorithm" document [QES V-A] and following the standard [ETSI TS 103 171] (https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/e-Signature+standards).

As a next step, the focus will be to implement more QES test cases as well as AdES ones (according to ETSI EN 319 102-1).

The structure of the document is the following:

First the presentation of the test cases, then a presentation of the web application itself, finally an explanation on how to use and integrate the test cases in a third-party solution.

The targeted audience of the present document are the eSignature solution implementers already aware of the QES validation algorithm and previously quoted standards.

1. QES TEST CASES

A qualified electronic signature is an advanced electronic signature which is additionally:

- Created by a private key that is protected by a qualified signature creation device;

- And is based on a qualified certificate for electronic signatures.

Qualified certificates for electronic signatures are provided by (public and private) providers which have been granted a qualified status by a national competent authority as indicated in the national 'trusted lists' of the EU Member State.

Taking this into account and based on the validation algorithm guidelines [QES V-A], a list of tests cases has been identified to allow eSignature solution implementers to validate their solutions.

For each of those test cases, a signed document, a trusted list including a related trust service and a root of trust (a LOTL together with its LOT-signing certificates) are needed.

The identified test cases differ by the variation on the content of the certificates (e.g. qualification statement), the trust service entries content, and the quality of the trusted list (e.g. availability, signature, …).

An overview of the list of test cases is shown in the figure below. The actual list can be downloaded from the web application itself.

Conclusion	Test case description		sigCert (signing certificate content)				TL (trusted list content)					Fake LOTL / TL entries			
	Processing the TLs											LOTL-2			
AdESig w/ warning		2.1.1	TL signature is not authorized, TL is ignored	QC	eSig	QSCD		catching	CA/QC	eSig			TL-21	TSP-2.1	TS-2.1.1	SDI-2.1.1
AdESig w/ warning		2.1.2	TL signature crypto failure, TL is ignored	QC	eSig	QSCD		catching	CA/QC	eSig			TL-22	TSP-2.1	TS-2.1.2	SDI-2.1.2
QESig w/ warning		2.1.3	TL has expired (NextUpdate)	QC	eSig	QSCD		catching	CA/QC	eSig			TL-23	TSP-2.1	TS-2.1.3	SDI-2.1.3
AdESig w/ warning		2.1.4	TL is temporarily unavailable, use version in cache	QC	eSig	QSCD		catching	CA/QC	eSig			TL-24	TSP-2.1	TS-2.1.4	SDI-2.1.4
												LOTL-3			
	Matching SDI + StifaSil + status												TL-3		
	3.1	0 matching service												TSP-3.1	
AdESig		3.1.1	No matching SDI	QC	eSig	QSCD		not catching	CA/QC	eSig					TS-3.1.1	SDI-3.1.1
AdESig		3.1.2	No matching CA/QC	QC	eSig	QSCD		catching	CA/PKC	eSig					TS-3.1.2	SDI-3.1.2
AdESig		3.1.3	No matching Sie:aSI	QC	eSig	QSCD		catching	CA/QC	eSeal					TS-3.1.3	SDI-3.1.3
AdESig		3.1.4	Withdrawn	QC	eSig	QSCD		catching	CA/QC withdrawn	eSig					TS-3.1.4	SDI-3.1.4
AdESig		3.1.5	Supervision ceased/..., before eIDAS	QC	eSig	QSCD		catching	CA/QC superv. ceased						TS-3.1.5	SDI-3.1.5
AdESig		3.1.6	Accreditation revoked/..., before eIDAS	QC	eSig	QSCD		catching	CA/QC accred. revoked						TS-3.1.6	SDI-3.1.6
	3.2	1 matching service												TSP-3.2	
QESig		3.2.1	Standard case	QC	eSig	QSCD		catching	CA/QC	eSig					TS-3.2.1	SDI-3.2.1
								catching	CA/QC	eSeal					TS-3.2.1	SDI-3.2.1
QESig w/ warning		3.2.2	No matching TSP Name / trade name	QC	eSig	QSCD		catching	CA/QC	eSig					TS-3.2.2	SDI-3.2.2
	3.3	Incoherences in TL												TSP-3.3	
error		3.3.1	Several entries matching (simple case)	QC	eSig	QSCD		catching	CA/QC	eSig					TS-3.3.1	SDI-3.3.1
								catching	CA/QC	eSig					TS-3.3.1	
	QC / notQC												TL-4		
	4.1	notQC based on sigCert content												TSP-4.1	
AdESig		4.1.1	sigCert not declared as QC		eSig	QSCD		catching	CA/QC	eSig					TS-4.1.1	SDI-4.1.1
QESig		4.1.2	Cert policy before eIDAS		eSig	QSCD	QCP+	catching	CA/QC	eSig					TS-4.1.2	SDI-4.1.2
QESig		4.1.3	Cert policy before eIDAS		eSig	QSCD	QCP	catching	CA/QC	eSig					TS-4.1.3	SDI-4.1.3
AdESig-QC		4.1.4	Cert policy before eIDAS		eSig		QCP	catching	CA/QC	eSig					TS-4.1.4	SDI-4.1.4
AdESig		4.1.5	Cert policy after eIDAS		eSig		QCP	catching	CA/QC	eSig					TS-4.1.5	SDI-4.1.5
AdESig		4.1.6	Cert policy after eIDAS		eSig		qcp_n_qcsd	catching	CA/QC	eSig					TS-4.1.6	SDI-4.1.6
QESig		4.1.7	Cert policy before eIDAS, QCP and QCP+		eSig		QCP, QCP+	catching	CA/QC	eSig					TS-4.1.7	SDI-4.1.7
	4.2	Overrule to notQC by Sie:Q in TL												TSP-4.2	
AdESeal		4.2.1	Catching	QC	eSeal			catching	CA/QC	eSeal	catching, NotQualified	All -> nonRepudiation true			TS-4.2.1	SDI-4.2.1
AdESig-QC		4.2.2	Not catching because of type	QC	eSig			catching	CA/QC	eSeal	catching, NotQualified	All -> digitalSignature true			TS-4.2.2	SDI-4.2.2
								catching	CA/QC	eSig					TS-4.2.2	SDI-4.2.2
AdESig-QC		4.2.3	Not catching because of criteria	QC	eSig			catching	CA/QC	eSig	not catching, NotQualified	All -> nonRepudiation true; keyEncipherment true			TS-4.2.3	SDI-4.2.3
	4.3	Overrule to QC by Sie:Q in TL												TSP-4.3	
AdESig-QC		4.3.1	Catching, although sigCert content is notQC		eSig			catching	CA/QC	eSig	catching, QcStatement	AtLeastOne -> keyCertSign true / decipherOnly true			TS-4.3.1	SDI-4.3.1
AdESeal		4.3.2	Not catching because of type		eSeal			catching	CA/QC	eSig	catching, QcStatement	none -> digitalSignature true; keyCertSign true			TS-4.3.2	SDI-4.3.2
AdESeal		4.3.3	Not catching because of criteria		eSeal			catching	CA/QC	eSeal	not catching, QcStatement	All -> nonRepudiation false; digitalSignature false			TS-4.3.3	SDI-4.3.3

Figure 1A: QES test cases – List of identified test cases

2. WEB APPLICATION

2.1. Overview

Figure 2A: esig-validation-tests – home page

The web application esig-validation-tests is composed of a home page, two main views (1 & 2), documentations files that can be downloaded (3) and useful links (4).

Documentation is composed of:

- User guide: The present document

- QES test cases: The list of identified test cases for QES validation

2.2. Trusted lists

According to the algorithm described in [QES V-A] and in order to simulate the existence of qualified trust services, esig-validation-tests has to provide "fake" LOTLs and "fake" TLs.

Because some test cases require dedicated LOTLs, more than one LOTL are generated for the purpose of esig-validation-tests.

The LOTLs and the TLs are **hosted** by the application and should not be downloaded to be hosted locally. This is due to the sheer structure of LOTLs and TLs that contain absolute URLS to each other.

From the "Trusted Lists" web page, the LOTLs and TLs can be browsed and shown below (hyperlinks):

Figure 2B: Trusted lists page – LOTLs and TLs

2.3. Test cases packages

On the "Test cases packages" web page, the test cases are displayed according to the structure of the *QES test cases* document [Figure 1A]. There are three levels of aggregation of test cases:

- LOTL

    ⇨ The test cases are grouped by LOTL in order to facilitate the integration and to minimize the configuration required for running the tests.

    o Category

        ▪ Sub-category

    ⇨ The test cases are classified in categories and sub-categories which refer to the certificates content/trust services implementation identified in the *QES test cases* document.

The *test cases packages* can be downloaded by LOTL (1) or in full (2).

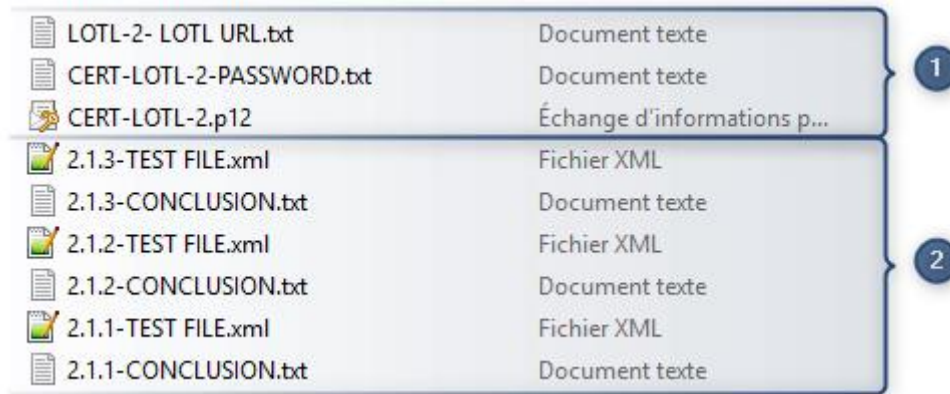

Figure 2C: Test cases page – package download

The test cases and related elements (LOTLs, TLs and LOTL-signing keystores) may expire as they contain dates (start date, notBefore date, notAfter date…). In order to avoid expiration of test cases, they are automatically renewed at the end of each week.

3. TEST CASES PACKAGE AND INTEGRATION

3.1. LOTL test cases package

A **LOTL** *test cases package* include the LOTL configuration files, the *signed test files* and the QES validation conclusions, as illustrated on the following screenshot of the "LOTL-2" *test cases package*:

LOTL-2- LOTL URL.txt	Document texte
CERT-LOTL-2-PASSWORD.txt	Document texte
CERT-LOTL-2.p12	Échange d'informations p...
2.1.3-TEST FILE.xml	Fichier XML
2.1.3-CONCLUSION.txt	Document texte
2.1.2-TEST FILE.xml	Fichier XML
2.1.2-CONCLUSION.txt	Document texte
2.1.1-TEST FILE.xml	Fichier XML
2.1.1-CONCLUSION.txt	Document texte

Figure 3A: LOTL-2 Content of the package

The filenames follow a naming convention based on `%LOTL_ID%` and `%TEST_CASE_ID%`:

LOTL Configuration files names are structured as follows:

- The LOTL URL

  Name   `%LOTL_ID%`- LOTL URL.txt

- The LOTL-signing keystore that contains the certificate used to sign the LOTL

  Name   CERT-`%LOTL_ID%`.p12

- The LOTL-signing keystore password that contains the password to read and access the keystore

  Name   `%LOTL_ID%` - LOTL URL.txt

The *signed test files* and the *esig validation conclusions* filenames are structured as follows:

- The *signed test files*

  Name   `%TEST_CASE_ID%`-TEST FILE.xml

- The *esig validation conclusions*

  Name   `%TEST_CASE_ID%`-CONCLUSION.txt

3.2. FULL test cases package

The FULL *test cases package* includes all the LOTL *test cases packages* in a unique zip file. The content of each LOTL *test cases package* is as described in the previous section.

3.3. Integration

As a third party, you need to:

- Download a test cases package**.**

- Retrieve the LOTL configuration files and configure the eSignature validation solution with them:

     o Set the LOTL location in the eSignature validation solution to be the URL contained in the `%LOTL_ID%`- LOTL URL.txt file.

     o Set the LOTL-signing certificate in the eSignature validation solution to be the one present in the LOTL-signing keystore.

- Retrieve the list of signed test files and esig validation conclusions.

- Run the eSignature validation solution on the corresponding signed test files and compare the outcome with the expected result provided in the esig validation conclusions.

4. USEFUL LINKS AND CONTACTS

CEF eSignature building block: https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eSignature

Digital Signature Service (DSS):
https://ec.europa.eu/cefdigital/wiki/pages/viewpage.action?pageId=46992515

Trusted list Browser (TL-Browser): https://webgate.ec.europa.eu/tl-browser/#/

CEF eSignature Support Team: CEF-eSignature-support@ec.europa.eu