



Connecting Europe Facility  
eSignature Building Block

# Validation of Qualified Electronic Signatures

10 January 2018

**Olivier Barette**

Nowina Solutions *on behalf of* the European Commission

# Connecting Europe Facility (CEF) in a nutshell

Funding for the  
EUROPEAN COMMISSION

**Services** offered by the  
European Commission

Justice



**eJustice Portal**

Consumer  
Protection



**ODR**

Information  
Society



**Open Data**

Internal  
Market



**BRIS**

Social  
Security



**EESSI, etc.**

**Building Blocks**



**IDENTIFY**  
with eID



**SIGN**  
with eSignature



**INVOICE**  
with eInvoicing



**EXCHANGE**  
with eDelivery



**TRANSLATE**  
with eTranslation

Funding for the  
MEMBER STATES

**Grants** - Projects in  
the Member States



Typically 'deployment' projects at national level  
(up to 75% of eligible cost)

---

# Agenda

1 The eIDAS Regulation

2 ETSI standards

3 Implementation in DSS open-source library

**1**



# The eIDAS Regulation

# eIDAS Regulation

## Regulation (EU) N° **910/2014**

- Adoption: July 2014
- Application: July 2016

## eIDAS date of entry into force

- Brussels time, CET : 1 July 2016 00:00
- UTC : **2016-06-30 22:00:00**



---

## Article 32

### Requirements for the validation of qualified electronic signatures

1. The process for the validation of a qualified electronic signature shall confirm the validity of a qualified electronic signature provided that:
  - (a) the certificate that supports the signature was, **at the time of signing**, a qualified certificate for electronic signature complying with Annex I;
  - (b) the qualified certificate was **issued** by a qualified trust service provider and was valid at the time of signing;
  - ...
  - (h) the requirements provided for in **Article 26** were met at the time of signing.
2. ...

---

# Annex I

## Qualified certificates for electronic signatures

(b) ...

(g) the advanced electronic signature or advanced electronic seal of the issuing qualified trust service provider;

(h) the location where the certificate supporting the advanced electronic signature or advanced electronic seal referred to in point (g) is available free of charge;

(i) the location of the services that can be used to enquire about the validity status of the qualified certificate;

(j) ...

# 2



## ETSI standards





---

# ETSI standards for AdES / QES

## Trusted Lists

- **TS 119 612**

## Certificate profiles

- **EN 319 412-1 : Overview**
- **EN 319 412-2 : Natural persons**
- **(EN 319 412-3 : Legal persons)**
- **(EN 319 412-4 : Web Site Auth)**
- **EN 319 412-5 : QCStatements**

## Signature creation / validation

- **EN 319 102-1 & EN 319 102-2**
- **EN 319 122 (CAAdES)**
- **EN 319 132 (XAdES)**
- **EN 319 142 (PAdES)**
- **EN 319 162 (ASiC)**

## Signature validation policy for European qualified electronic signatures/seals using trusted lists

- **TS 119 172-4**

# 3

---

## Implementation in DSS

[ec.europa.eu/cefdigital/eSignature](https://ec.europa.eu/cefdigital/eSignature)



---

# Objectives of DSS

1

**Compliance with  
eIDAS and the  
ETSI standards**

2

**DSS deals with the  
signatures, so you  
can deal with the  
business**

3

**Non-competition  
with the market**

---

# Pre-processing steps for QES validation in DSS

- LOTL and TLs loading and validation
  - Signature: **Pivot** LOTLs
  - NextUpdate & "Freshness"
- Select Trust Services with type = CA/QC
  - **Pre**-eIDAS: undersupervision / supervisionin cessation / accredited
  - **Post**-eIDAS: granted
- Trust Service **consistency** checks
  - QCStatement vs NotQualified
  - QSCD vs NoQSCD
  - eSeal / WSA /... vs Pre eIDAS
  - Additional Service Info vs Service Qualifier
- Certificate content vs Trust Service **consistency** checks
  - Certificate type vs Additional Service Info

# QES validation in DSS

AdES ?	Qualified Cert ?	Cert type ?	QSCD ?	Conclusion
<p style="text-align: center;"> <span style="background-color: #d4edda; padding: 2px;">VALID</span>                      /  <span style="background-color: #fff3cd; padding: 2px;">INDETERMINATE</span> </p>	QC	eSig	QSCD	QESig
			NotQSCD	AdESig-QC
		eSeal	QSCD	QESeal
			NotQSCD	AdESeal-QC
	Not QC	eSig	QSCD	AdESig
			NotQSCD	AdESig
		eSeal	QSCD	AdESeal
			NotQSCD	AdESeal
INVALID				

# Qualified Certificate ?

Dates : signing time + cert issuance time

				CA/QC Trust Service		
				No catching Qualifier	Qualifier NotQualified	Qualifier QcStatement
Certificate	Pre-eIDAS	QCStatement	qc-compliant		Overrule	
		PolicyId	qcp-public		Overrule	
			qcp-public-with-sscd		Overrule	
		None			Overrule	
	Post-eIDAS	QCStatement	qc-compliant		Overrule	
			None			Overrule

Color legend:

QC	Not QC
----	--------

# Certificate type ?

Date : signing time

			CA/QC Trust Service			
			No catching Qualifier QCForXX	Qualifier QCForEsig	Qualifier QCForEseal	Qualifier QCForWSA
Certificate	Pre-eIDAS	QCType not defined				
	Post-eIDAS	QCType not defined			Overrule	Overrule
		QCType = eSign			Overrule	Overrule
		QcType = eSeal		Overrule		
		QcType = WSA		Overrule		

Color legend:

<i>eSig</i>	<i>eSeal</i>	WSA	<i>Not allowed</i>
-------------	--------------	-----	--------------------

# QSCD ?

Prerequisite : QC certificate (cert + TL)

Date : signing time

				CA/QC Trust Service		
				No catching Qualifier	Qualifier QCNoSSCD/QCNoQSCD	Qualifier QCWithQSCD / QCWithSSCD / QCQSCDManagedOnBehalf
Certificate	Pre-eIDAS	PolicyId	qcp-public-with-sscd		Overrule	
			qcp-legal-qscd		Overrule	
			qcp-natural-qscd		Overrule	
		QCStatement	qc-sscd		Overrule	
			Nothing			Overrule
	Post-eIDAS	QCStatement	qc-sscd		Overrule	
			Nothing			Overrule

Color legend:

QSCD	Not QSCD
------	----------



---

## Lessons learned from QES validation implementation in DSS

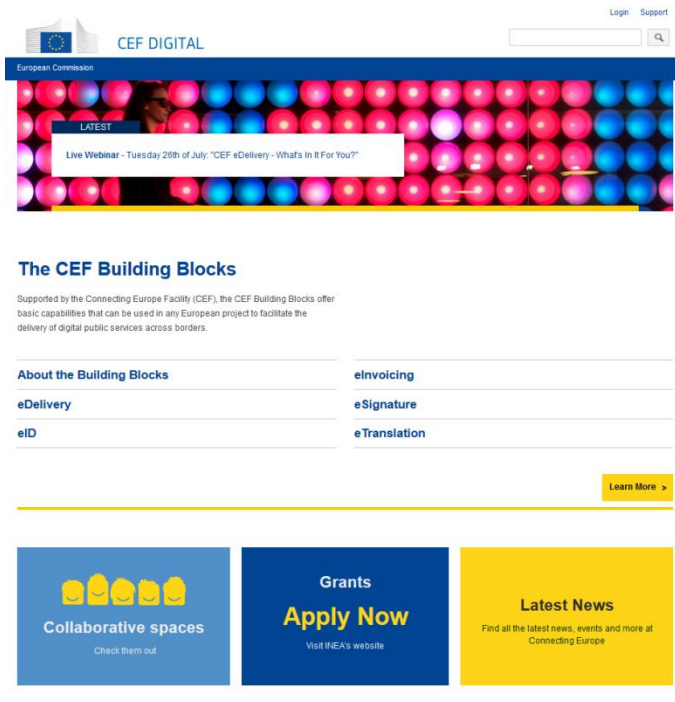
- eIDAS **entry** into force = UTC 2016-06-30 22:00:00
- **Pivot** LOTL: detection, integration
- QC status vs. QTSP status: **not immutable**
- **2 moments** in time to be considered:
  - time of signing
  - time of issuance
- ETSI EN **319 102-1** for Article 26. Independent of the EU context (Qualified,...)
- **Pre-processing** steps before validation, and **implications** if it fails
- QcType: **WSA** considered as eSeal

---

# Suggestions

- Public **access** to ETSI TS 119 172-4 ?
- ETSI QES validation **plugtests** ?
- Implementation of ETSI EN 319 102-2 (presentation of the **results**)

# Find out more on CEF Digital eSignature



The screenshot shows the CEF Digital website homepage. At the top, there is a navigation bar with the European Commission logo, the text 'CEF DIGITAL', and links for 'Login' and 'Support'. Below this is a search bar. The main content area features a large banner with a grid of colorful spheres (red, blue, yellow) and a 'LATEST' section with a 'Live Webinar - Tuesday 20th of July: "CEF eDelivery - Whats in It For You?"' announcement. Below the banner is a section titled 'The CEF Building Blocks' with a brief description: 'Supported by the Connecting Europe Facility (CEF), the CEF Building Blocks offer basic capabilities that can be used in any European project to facilitate the delivery of digital public services across borders.' This section contains a grid of links: 'About the Building Blocks', 'eInvoicing', 'eDelivery', 'eSignature', 'eID', and 'eTranslation'. A 'Learn More >' button is located at the bottom right of this section. Below the grid are three colored boxes: a blue box for 'Collaborative spaces' with a 'Check them out' link, a dark blue box for 'Grants Apply Now' with a 'Visit INEA's website' link, and a yellow box for 'Latest News' with a 'Find all the latest news, events and more at Connecting Europe' link.



[ec.europa.eu/cefdigital/eSignature](https://ec.europa.eu/cefdigital/eSignature)

## DIGIT

Directorate-General for Informatics

## DG CONNECT

Directorate-General for Communications  
Networks, Content and Technology

## Contact us



[Michael.de-Boer@ec.europa.eu](mailto:Michael.de-Boer@ec.europa.eu)

[CEF-ESIGNATURE-SUPPORT@ec.europa.eu](mailto:CEF-ESIGNATURE-SUPPORT@ec.europa.eu)

© European Union, 2017. All rights reserved. Certain parts are licensed under conditions to the EU. Reproduction is authorized provided the source is acknowledged.