EUROPEAN COMMISSION
DIRECTORATE-GENERAL
INFORMATICS
Directorate A - Corporate IT Solutions & Services
Corporate Infrastructure Solutions for Information Systems (LUX)

Generic PDF signature specification

Date:	10.10.2012
Version:	0.102
Authors:	DIGIT.A.3
Reference Number:	DIGIT A/3 D/(2012) xxxx

European Commission, L-2920 Luxembourg. Telephone: (352) 43 01-1.
Office: DRB C3/071. Telephone: direct line +352 4301 33207. Fax: +352 4301 34311.

E-mail: philippe.schneider@.ec.europa.eu

Document History

Version	Date	Modified Pages
0.100	26.09.2012	Initial Draft (by RV)
0.101	05.10.2012	Revision (by RV)
0.102	10.10.2012	Revision (by RV)

European Commission, L-2920 Luxembourg. Telephone: (352) 43 01-1.
Office: DRB_D3/071. Telephone: direct line +352 4301 33207. Fax: +352 4301 34311.

E-mail: Philippe.schneider@ec.europa.eu

TABLE OF CONTENT

European Commission, L-2920 Luxembourg. Telephone: (352) 43 01-1.
Office: DRB C3/071. Telephone: direct line +352 4301 33207. Fax: +352 4301 34311.

E-mail: philippe.schneider@ec.europa.eu

European Commission, L-2920 Luxembourg. Telephone: (352) 43 01-1.
Office: DRB C3/071. Telephone: direct line +352 4301 33207. Fax: +352 4301 34311.

E-mail: philippe.schneider@.ec.europa.eu

1. GENERAL

This document is about the specification of the Generic PDF Signature Creation and Validation Services for qualified electronic signatures (QES), advanced electronic signatures based on a qualified certificate (AdES/QC), and Commission-internal signatures (AdES/EC). This prototype should demonstrate the electronic signature technology currently available regarding interoperable signatures as specified in directive 2011/130/EU. Even more, it should be useable by people who are not familiar with the advanced concepts of electronic signature. It should also be a way of teaching people the motives of the different signature types and policies.

2. REQUIREMENTS

(1) Qualified certificates on SSCD issued by the official Commission provider FNMT should be supported

(2) Qualified certificates other than those issued by FNMT should be supported. The provider must provide certificate access via MSCAPI

(3) For signature creation the signed document should be published regardless wether extension was successful or not

(4) Access to the application should be restrictable. This should be done using ECAS, the European Commission Authentication Service.

(5) PDF documents should be signed by PAdES.

(6) The application should be a JAVA application that runs on any servlet container.

(7) The application should be conformant to Commission Decision 2011/130/EU regarding interoperable signatures.

(8) The application should be useable by people not familiar with the advanced concepts of electronic signature. Furthermore it should be a way of teaching people the motives of the different signature types and policies.

(9) The application should guide the user to the correct policy by being as lenient as possible.

(10) The user should have an overview over the page hierarchy.

(11) Signature creation and validation should be two separate pages because they are two different processes

(12) Signature creation and validation should have a layout as similar as possible so that the user has no problems using the one service when he has used the other service before.

(13) It should be possible to open the file to be signed and the signed file from the browser

(14) The file to be signed should be protected against tampering

(15) A description of advanced signature concepts should be available to the user

3. LAYOUT

This section describes the layout choices that were made for the validation and signature creation services. The aim is to have the same look-and-feel for both services where possible. Where needed, the sections below should explain when the two services differ in their common basis.

Figure 1 shows the Generic PDF Signature Creation page. Figure 2 shows the Generic PDF Signature Validation page.

European Commission, L-2920 Luxembourg. Telephone: (352) 43 01-1.
Office: DRB_D3/071. Telephone: direct line +352 4301 33207. Fax: +352 4301 34311.

E-mail: Philippe.schneider@ec.europa.eu

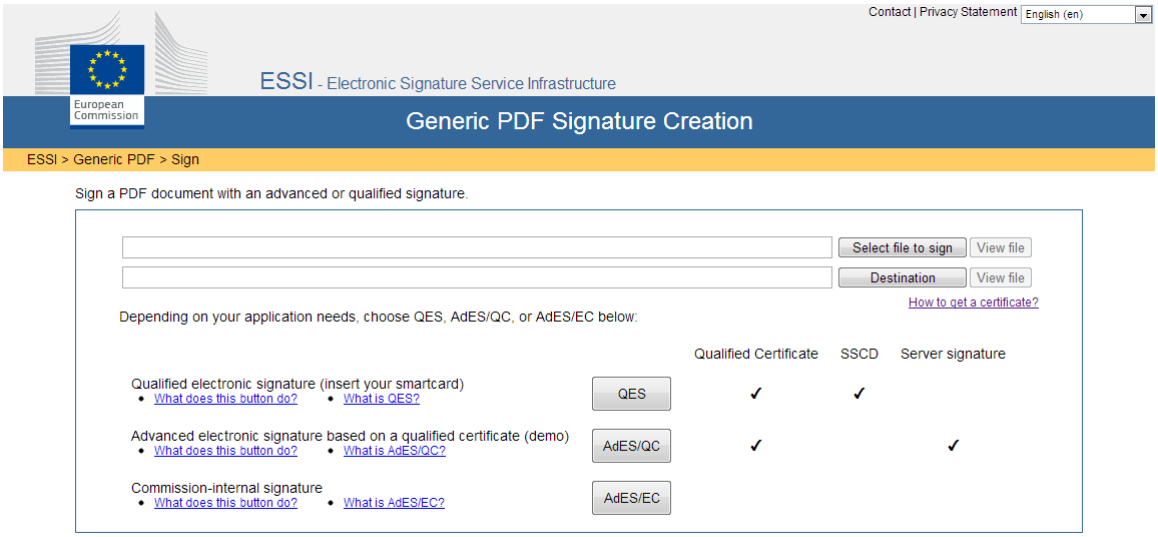


Figure 1: Generic PDF Signature Creation page

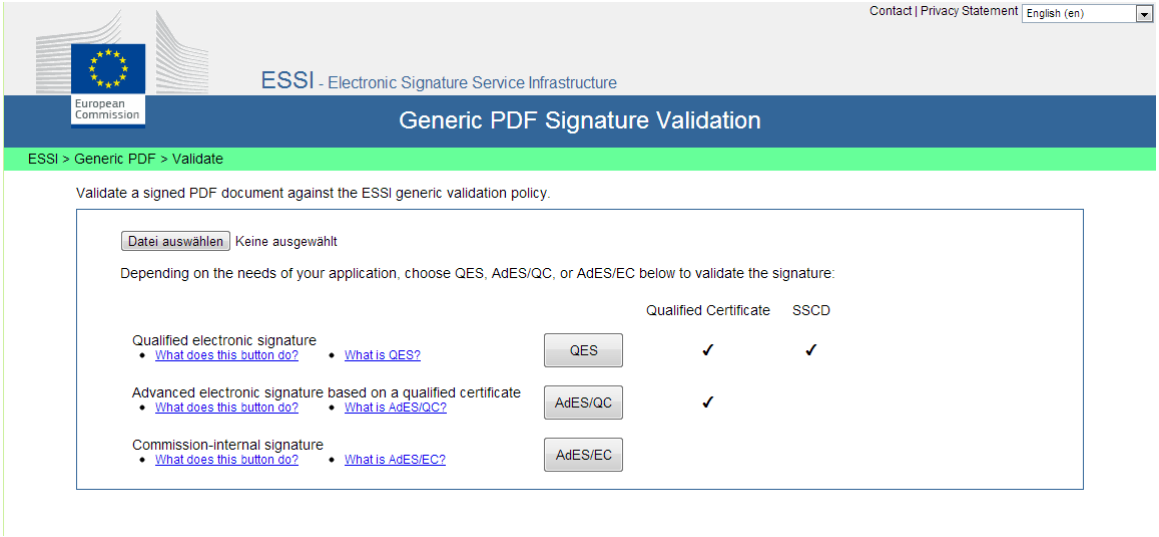


Figure 2: Generic PDF Signature Validation page

?Mark title, breadcrumbs, etc (using boxes and numbers) to be able to refer to them later or cut out title, breadcrumbs, etc and insert in later sections

3.1. Title

Since signature creation and validation are both about generic PDF signature they should share the same title (with the respective service type appended which would be "signature creation"/"validation") appended (as seen in Figure 1and Figure 2):

"Generic PDF Signature creation/validation"

3.2. Breadcrumbs

Breadcrumbs typically appear horizontally across the top of a web page, often below title bars or headers. They provide links back to each previous page the user navigated through to get to the

European Commission, L-2920 Luxembourg. Telephone: (352) 43 01-1.
Office: DRB C3/071. Telephone: direct line +352 4301 33207. Fax: +352 4301 34311.

E-mail: philippe.schneider@ec.europa.eu

current page or the parent pages of the current one. Breadcrumbs provide a trail for the user to follow back to the starting or entry point.

Breadcrumbs are used in the generic PDF signature application to implement requirement (10). They look like the following:

ESSI > Generic PDF > Sign/Validate

- ESSI: This is the entry point for the application. It links to the ESSI MyIntracomm page (http://myintracomm.ec.europa.eu/corp/digit/ENU/isp_service_catalogue/Pages/essi_new.aspx).
- Generic PDF: This is an overview page that describes both services and where the user can navigate either to Generic PDF signature creation or validation.
- Sign/Validate: These are the actual pages where the user can create and validate signatures.

3.3. Application body

The application body is where the user chooses a document to be signed or validated and selects wich kind of signature or validation he wants. Both pages should be as similar as possible so that a user which has used one of the services is able to use the other service without problems.

Differences:

- Destination file chooser: The signature creation page has an additional file chooser that provides the location where the resulting signed document should be stored. This is not needed for signature validation.
- Server signature column: This column only exists on the signature creation page to inform the user if the service creates the signature locally or on a remote server. Using signature validation both local and remote signatures can be verified. Please note that depending on the service type the signature may not be validated successfully (e.g. currently the server signature is not a personal signature whose signing certificate does not reside on an SSCD).

3.4. File viewing

Implementing requirement (13) it is possible to view the file to be signed and the signed file by clicking the “View file” button next to the respective file chooser. For the file to be signed a protection against tampering was implemented as described in section 5.1.

3.1. “What does this button do?” links

Those links should provide a detailed explanation of the behavior of each button. The explanation should describe the signature creation and validation logic, including the fallback logic that directs the user towards the correct policy to use. It should furthermore describe the button behavior and point to regulations/directives/policies it is based on as far as this is not done by the “What is ..?” link. Those explanations are specified in section 6.

3.2. “What is ..?” links

The explanation should cover those advanced concepts of electronic signature and should point to regulations/directives/policies regarding those concepts.

4. FUNCTIONAL OVERVIEW

This section gives a functional overview of the Generic PDF signature application. A more detailed technical overview is presented in section 5.

4.1. Validation services

A set of Serenity validation services, that implement the so-called R policies, which are described in the three section below, are used both for signature creation and signature validation. This set of services enables the application to distinguish between QES, AdES/QC and AdES/EC signatures.

For signature creation the services are used in the following way. After a signature is created locally the document is sent to the server. This serves two purposes:

1. The signature is validated. This is how the generic PDF application can verify that the signature is really the kind of signature that the user requested, although the extension algorithm offers some leniency as described in detail in section 6.2.

2. A qualified timestamp is added to the signature. A qualified timestamp is a timestamp that is signed electronically by a trusted authority. A trust path is established through the use of TSLs[1]. [not yet for EC-internal] A qualified timestamp is not to be mistaken for the signing time attribute inside the signature mandated by 2011/130/EU. The signing time attribute can be specified by the client, e.g. by using the local system time. As the signing time can be set to an arbitrary value it cannot be guaranteed that the document was really signed at that point in time.

4.1.1. Service types

QSig_P

OID: 1.3.130.999.3

QSig_P is used to validate and extend QES signatures. It uses TSLs for signature and timestamp verification. It is required that the signing certificate is a qualified certificate and that it resides on an SSCD (Secure Signature Creation Device).

QCert_P

OID: 1.3.130.999.4

QCert_P is almost equivalent to QSig_P with the exception that the signing certificate does not need to be on an SSCD.

ECINT_P

OID: 1.3.130.999.7

The ECINT_P policy is used to validate and extend Commission-internal signatures. The signatures are extended using a trusted Timestamping authority.

4.2. Signature creation

Figure 3 below shows the process of signature creation for the three services QES, AdES/QC, and AdES/EC. This flowchart illustrates the common core regarding the both local signature creation services QES and AdES/EC as marked by the box. The signing processes differ in the discovery of the signing certificates (see section 5.2), the result depending on the service the user has chosen and the actual extension algorithm. But even the extension algorithms have a common core as described in section 4.2.1.

[1] As defined in the Annex of the Corrigendum to Commission Decision 2009/767/EC

European Commission, L-2920 Luxembourg. Telephone: (352) 43 01-1.
Office: DRB C3/071. Telephone: direct line +352 4301 33207. Fax: +352 4301 34311.

E-mail: philippe.schneider@ec.europa.eu

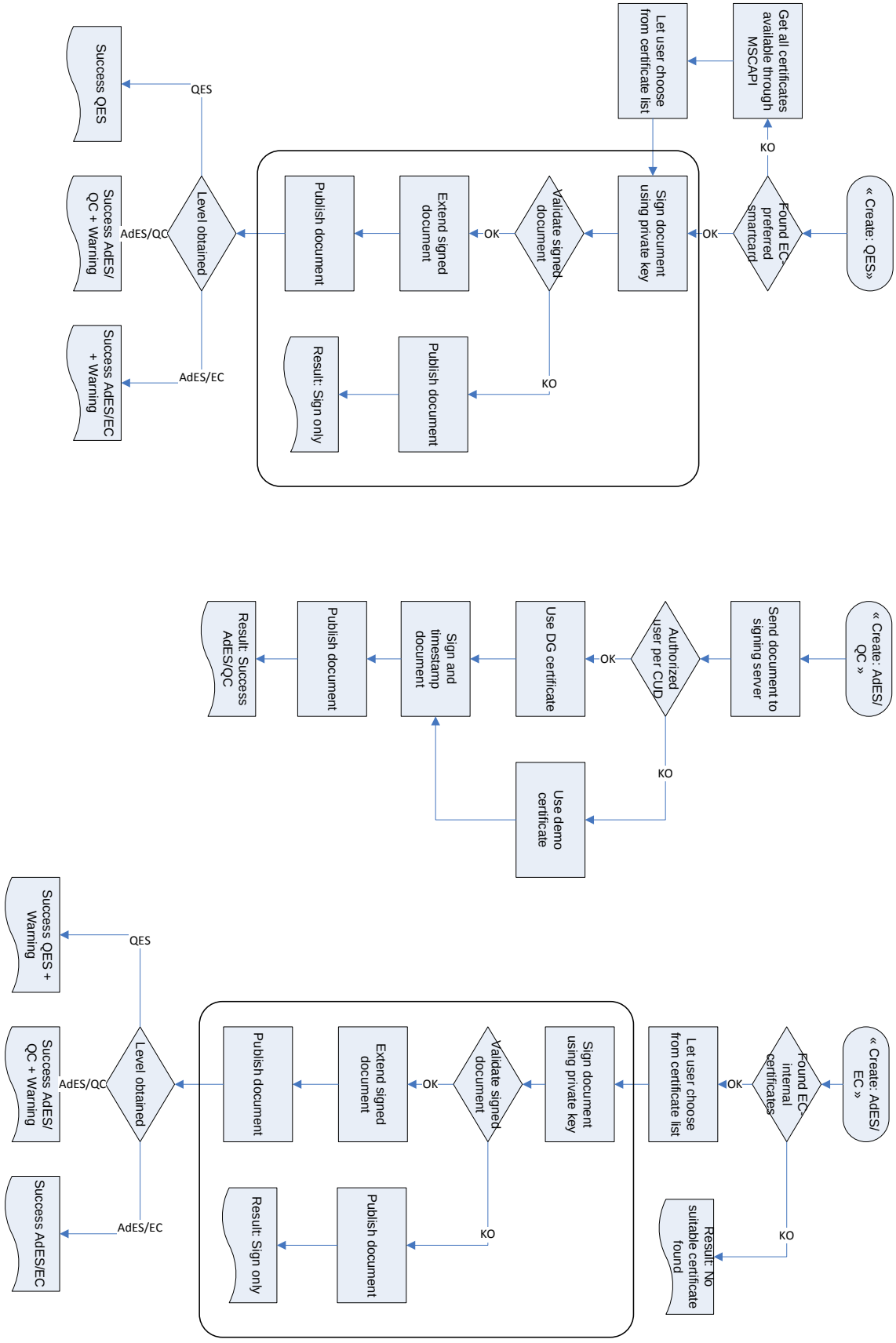


Figure 3: Signature creation

European Commission, L-2920 Luxembourg. Telephone: (352) 43 01-1.
Office: DRB C3/071. Telephone: direct line +352 4301 33207. Fax: +352 4301 34311.

E-mail: philippe.schneider@ec.europa.eu

Message definitions

- *Success:* Your PDF document was just signed. The signature is a *<signature type long> (<signature type short>).* Signature details can be viewed with an adequate PDF viewer but adequate validation can only be obtained from a service implementing the ESSI R policy like the generic ESSI Validation service.
- *Warning*: Warning: You requested *<signature type short>* but *<error message>*, thus it is not *<signature type short>*.
- *Sign only:* Your document was just signed but not extended. Reason: *<reason>*

4.2.1. Signature extension

As shown in Figure 4 both local signature extension processes share the same core that is QSig and QCert validation and extension. While for QES QSig Validation is the primary validation service, for AdES/EC it is used as a fallback in case ECINT validation failed.

The flowchart does not include AdES/QC extension because the timestamp is added during signature creation, while for QES and AdES/EC the timestamp is added after signature creation by extending the signature.

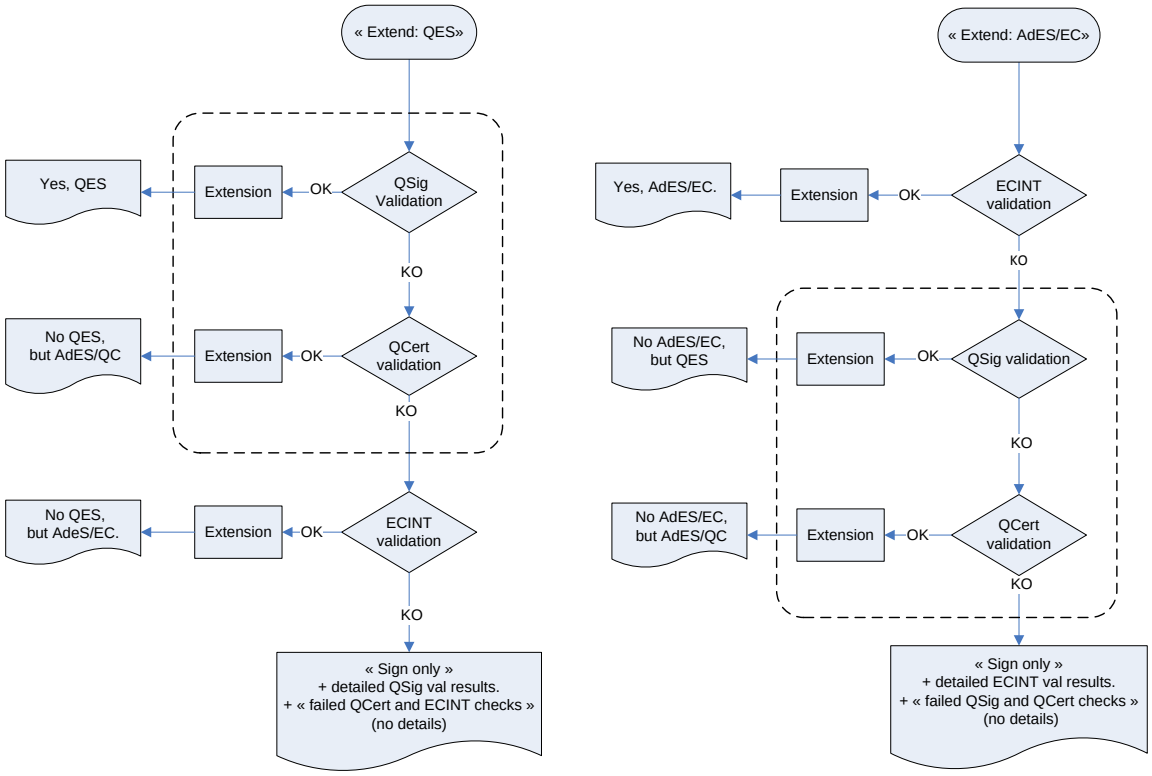


Figure 4: Local signature extension

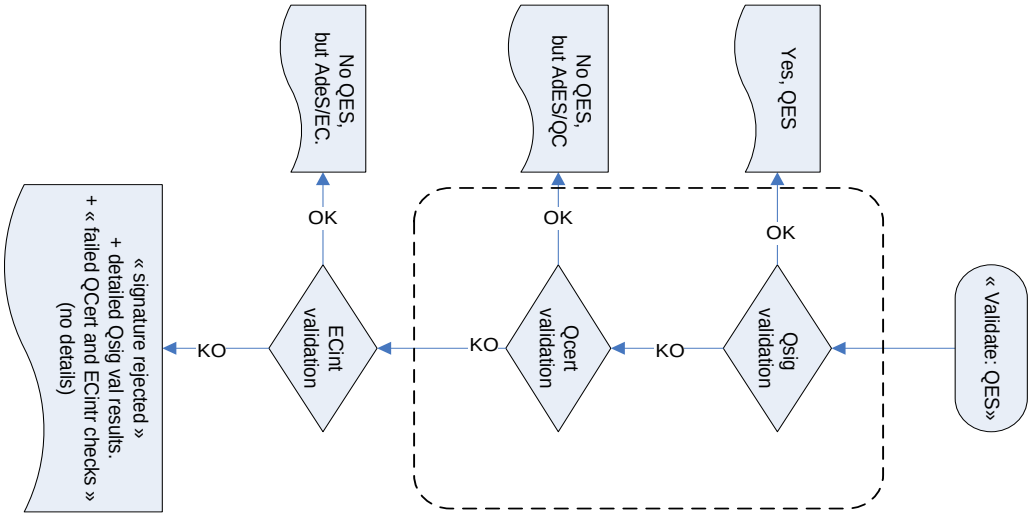
4.3. Signature validation

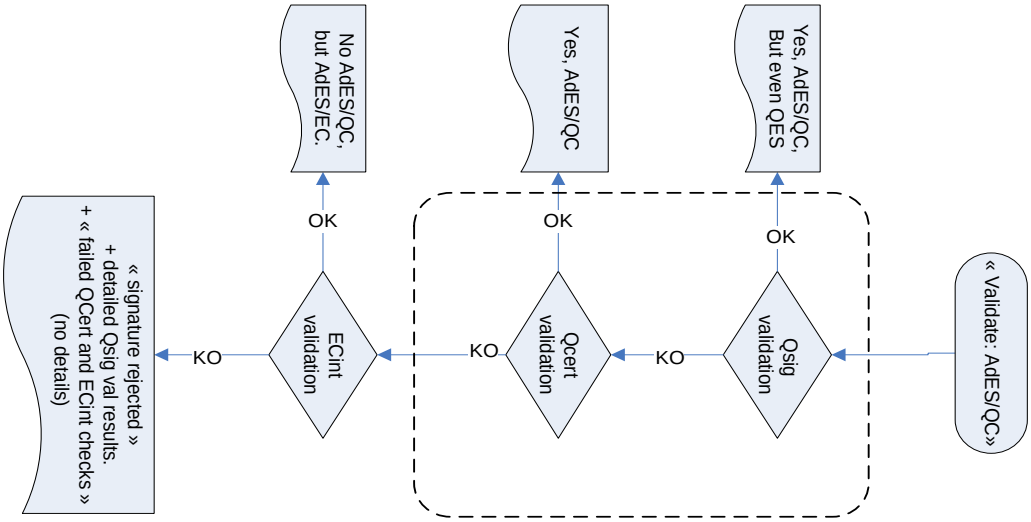
As shown in Figure 5 all three validation services share the same validation core which is in fact very similar to the extension core. As with extension the AdES/EC service only uses Qsig validation as a fallback in case the primary ECINT validation fails.

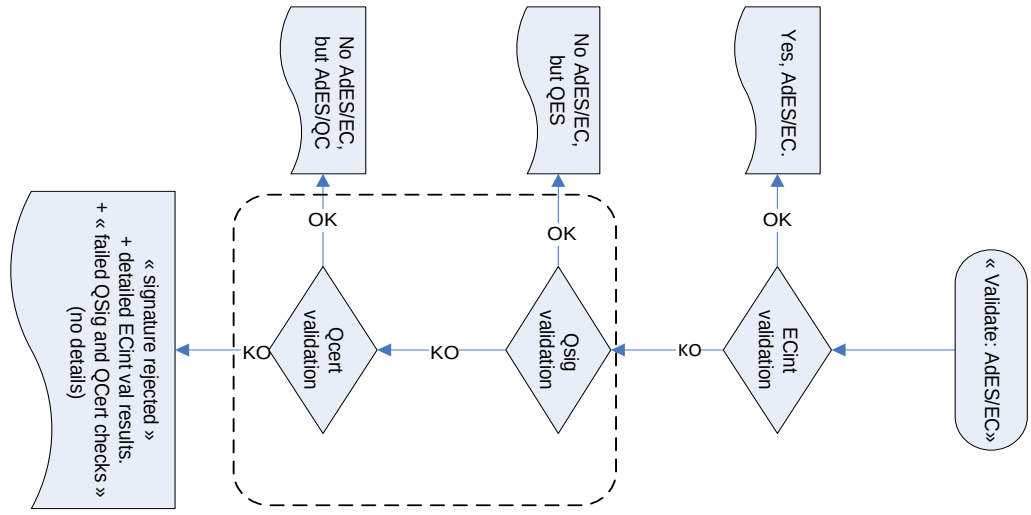
AdES/QC uses QSig as primary validation service, as does QES. This is because if QES validates successfully AdES/QC should also validate successfully because the both services are almost the same as described in section 4.1.1.

European Commission, L-2920 Luxembourg. Telephone: (352) 43 01-1.
Office: DRB C3/071. Telephone: direct line +352 4301 33207. Fax: +352 4301 34311.

E-mail: philippe.schneider@ec.europa.eu







European Commission, L-2920 Luxembourg. Telephone: (352) 43 01-1.
Office: DRB C3/071. Telephone: direct line +352 4301 33207. Fax: +352 4301 34311.

E-mail: philippe.schneider@.ec.europa.eu

Figure 5: Signature validation

Message definitions

Yes <*target signing type*>*:* The signature was successfully validated as a <*target signing type*>.

No <*target signing type*>, but <*resulting signing type*>*:* Although the signature could not be validated as <*target signing type*> it was successfully validated as <*resulting signing type*>.

<< *signature rejected* >>*:* The signature could not be validated as a <*target signing type*>. Reason: <*reason*>. Furthermore <*other signing types*> validation also failed.

5. TECHNICAL OVERVIEW

This section gives a more in-depth overview over the more technical details of the Generic PDF Signature application.

5.1. Local signature creation

Local signature creation makes use of a Java applet because otherwise files on the file system could not be accessed through the browser other than file upload to a server. Using an applet benefits the application in multiple ways:

- Protection against tempering (see section 5.1 below)
- Viewing the file to be signed and the signed file (see section 3.4)
- Writing the resulting signed file to disk (requirement (3))

5.2. Remote signature extension

Signature extension is done on a remote server running Cryptolog Serenity…

5.1. Protection against tampering

To protect the file to be signed against tampering as required by requirement (14), the file is hashed when it is chosen using the file chooser and the resulting hash value is stored. Everytime the file is viewed or the signature process is started the file is read from the file system and hashed again. This resulting hash is than compared to the hash stored previously when the file was first chosen. If the hashes differ this means that the file has been modified (or deleted, moved, replaced). A security message (cf section 7) warns the user of the modification.

5.2. Certificate discovery

Certificate discovery differs for the three services since the requirements on the certificates differ for each service.

5.2.1. Signing APIs

Different API's are used for the different signing types as shown in Table 1**Error! Reference source not found.**. The default signing API for QES is the FNMT PKCS#11 API implementation. This is because FNMT is the official Commission provider for qualified certificates (cf. requirement (1)) that reside on an SSCD which make qualified electronic signatures possible.

But since the user should not be limited to FNMT certificates (cf. requirement (2)), thus as fallback MSCAPI is provided. MSCAPI is supported by all popular smartcard providers on Windows operating system.

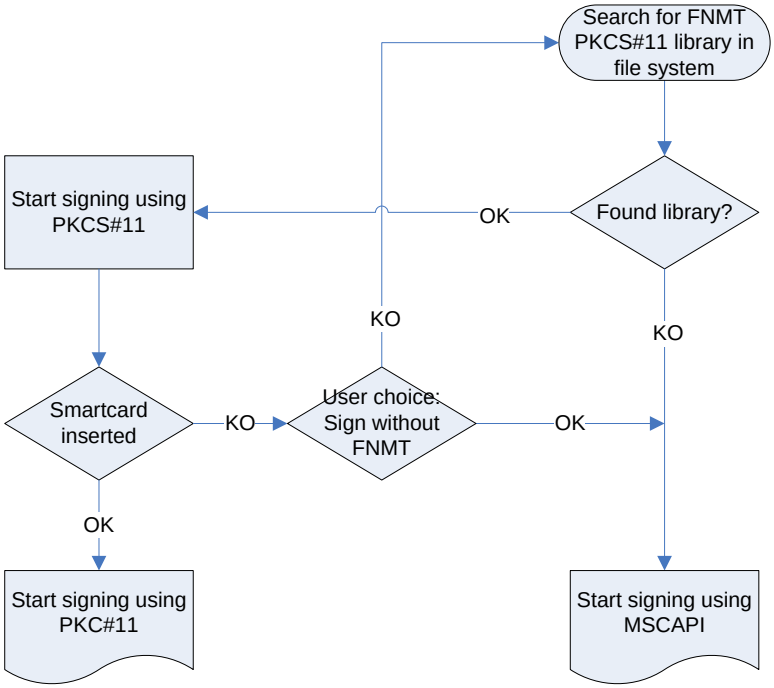
European Commission, L-2920 Luxembourg. Telephone: (352) 43 01-1.
Office: DRB C3/071. Telephone: direct line +352 4301 33207. Fax: +352 4301 34311.

E-mail: philippe.schneider@ec.europa.eu

QES	AdES/QC	AdES/EC
FNMT PKCS#11, fallback MSCAPI	MSS	MSCAPI

Table 1: Signing API used by the respective services

5.2.1.1. QES



- Filters

5.2.1.2. AdES/QC

Since the signing certificate is not stored locally but on a server no local signing API is used.

5.2.1.3. AdES/EC

AdES/EC only uses MSCAPI as signing API.

5.2.2. Local signing certificate filters

When more than one certificate exists and is found suitable for signing, a certificate choosing dialog appears. For every signing certificate the distinguished name and the issuer of the certificate are displayed. The user can then choose the certificate he wants to use for signing. Depending on the requested signature, different filters are applied that filter out unsuitable certificates. Table 2**Error! Reference source not found.** displays which filters are applied for which signature type.

QES	AdES/QC	AdES/EC
Validity date, duplicates, key-usage non-repudiation	No filters because AdES/QC certificate is provided on a server	Validity date, duplicates, key-usage non-repudiation, Issuer CommisSign

Table 2: Local signing certificate filters for signature creation

European Commission, L-2920 Luxembourg. Telephone: (352) 43 01-1.
Office: DRB C3/071. Telephone: direct line +352 4301 33207. Fax: +352 4301 34311.

E-mail: philippe.schneider@ec.europa.eu

- Validity date: Only show certificates whose “Not after” date is after the current point in time which is the local computer’s system time.
- Duplicates: In CUTE the list of available signing certificates is represented through their whole certificate chain. The list of signing certificates that may be used for signing is compiled from those chains. Since multiple certificate chains can have the same signing certificates, the signing certificate list may contain duplicates. Duplicate signing certificates are filtered from this list if the filter is active. The chains are filtered by which one comes first.
- Key-usage non-repudiation: Only certificates having the key-usage non-repudiation are allowed.
- Issuer: Only certificates that have one of the specified issuers are shown.

5.2.3. Remote certificate filters

	QES	AdES/QC	AdES/EC
ETSI policy	SSCD, qualified certificate	<No extension>	Issuer (CommisSign)
Serenity policy	TSL	<No extension>	

- SSCD: Only certificates that reside on a SSCD (certificate policy) are allowed.
- Qualified certificate: The signing certificate must be qualified
- TSL: The certificate chain of the signing certificate is validated up to a trusted root that is present in the Trusted List for the country of the Certification Service Provider that issued the signing certificate.
- Issuer: Only certificates that have one of the specified issuers are shown.

6. USER DOCUMENTATION

Requirement (15).

6.1. Signature creation

6.1.1. QES

This service creates a qualified electronic signature (QES). Per default this is done by using an FNMT smartcard, because FNMT is the official provider for qualified certificates on an SSCD for the European Commission. To not limit users to FNMT, a fallback mechanism using MSCAPI is provided, which is supported by all popular smartcard providers. After the signing, which is transparent to the user, a qualified timestamp is added by extending the signature.

- Show/link to signature creation comparison flowchart
- Show/link to signature extension flowchart
- Link to filter description

European Commission, L-2920 Luxembourg. Telephone: (352) 43 01-1.
Office: DRB C3/071. Telephone: direct line +352 4301 33207. Fax: +352 4301 34311.

E-mail: philippe.schneider@.ec.europa.eu

6.1.2. AdES/QC

This service creates an advanced electronic signature based on a qualified certificate (AdES/QC) that resides on a server (server signature). The demo nature of the certificate is identified by the CN "ESSI AP TEST" of the certificate DN. Currently it is not possible to use a Directorate-General provided certificate through the browser, but it could be added as a future option if on popular demand. After the signing, transparent to the user, a qualified timestamp is added by extending the signature.

- Show/link to signature creation comparison flowchart

6.1.3. AdES/EC

This service creates a Commission-internal certificate. Commission-internal certificates non-qualified certificates issued by CommisSign. After the signing, transparent to the user, a qualified timestamp is addedby extending the signature.

- Show/link to signature creation comparison flowchart
- Show/link to signature extension flowchart
- Link to filter description

6.2. Signature validation

6.2.1. QES

For every signature of a PDF document: Validate if the signature is a qualified electronic signature (QES). If the signature validation fails because the signing certificate was not on a SSCD, AdES/QC validation is used as a fallback. In all other cases AdES/EC validation is used as a fallback.

- Show/link to signature validation comparison flowchart

6.2.2. AdES/QC

For every signature of a PDF document: Validate if the signature is an advanced electronic signature based on a qualified certificate. In addition to a successful validation an additional validation is executed. This validation checks if the signature is also a qualified electronic signature which is the equivivalent to a handwritten signature. If the initial validation fails an AdES/EC validation is executed.

- Show/link to signature validation comparison flowchart

6.2.3. AdES/EC

For every signature of a PDF document: Validate if the signature is a Commission-internal signature. If the signature could not be validated.

- Show/link to signature validation comparison flowchart

European Commission, L-2920 Luxembourg. Telephone: (352) 43 01-1.
Office: DRB C3/071. Telephone: direct line +352 4301 33207. Fax: +352 4301 34311.

E-mail: philippe.schneider@ec.europa.eu

7. GUI SUPPORT OF END USER CATEGORIZATION

7.1. Syntax error messages

Syntax error messages correspond to errors due to wrong handling of the application or incomplete preparation by the user.

- Please select a PDF document first → No PDF document for signing has been chosen yet
- Please select a destination first → The destination for the resulting signed document was not chosen yet
- Please insert your smartcard and try again
- No suitable certificate for signing found
- Wrong PIN entered
- The signing operation was cancelled by the user→ The user pressed "Cancel" on the PIN entry dialog

7.2. Policy error messages

If Serenity encounters an error during validation it sends back an error code. A resource file provides a mapping between these error codes and the error description which is forwarded to the user

Most common messages:

- No suitable X509 path found → A trust chain could not be established
- SSCD error → The private key is not residing on an SSCD
- Certificate not qualified → The signing certificate is not qualified

7.3. Security messages

- The file was modified since it has been selected → See section 5.1 Protection against tampering.

European Commission, L-2920 Luxembourg. Telephone: (352) 43 01-1.
Office: DRB C3/071. Telephone: direct line +352 4301 33207. Fax: +352 4301 34311.

E-mail: philippe.schneider@.ec.europa.eu