



# TECHNICAL ANNEX TO

## AGREEMENT BETWEEN EUROCONTROL AND THE “CRCO EXTRANET FOR AIRSPACE USERS (“CEFA”) USERS

### **4- Protection of data**

#### **4.1 Principles**

CEFA uses an Advanced Electronic Signature (AES) for signing invoices and related documents. It is by nature a closed user group domain.

Electronic signatures do not affect any substantive rights or obligations of the parties. A contract or other documents relating to a transaction may not be denied legal effect, validity, or enforceability solely because it is in electronic form.

The sole purpose of the electronic signature is to assist the recipient of the documents in checking the authenticity and integrity of the document and in verifying the identity of the emitter. The successful verification of the electronic signature is only one element contributing in asserting the authenticity and validity of the document. It is the responsibility of the recipient to use other methods of additional controls that are considered standard or best practices in commercial relations.

Any claim or enquiry based on an electronically signed document shall not be accepted after 6 months from the end of validity of the certificate used for signing the document, with the exception of a possible early cancellation of a certificate.

#### **4.2 Use of electronic signature**

Some of the electronic documents issued through CEFA are “Billing documents”. These documents are PDF files. All these files are digitally ‘signed’. The digital signature is compliant with standard PDF signature interchange standard, which can be verified by Acrobat reader 8.1 or above, or by compatible handler directly.

When digitally signing these PDF files, Eurocontrol CRCO is using their own private certificate key and GlobalSign as Certification Authority.

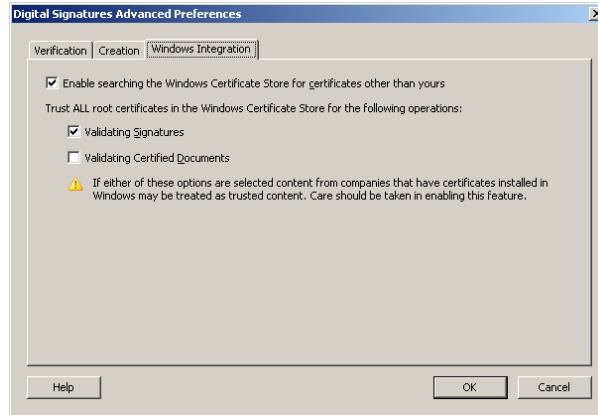
The certificate gives an intuitive way to authenticate and verify the origin of these PDF files. The advantage of PDF signature is that the user can verify the signature.




## TECHNICAL ANNEX TO

### AGREEMENT BETWEEN EUROCONTROL AND THE “CRCO EXTRANET FOR AIRSPACE USERS (“CEFA”) USERS

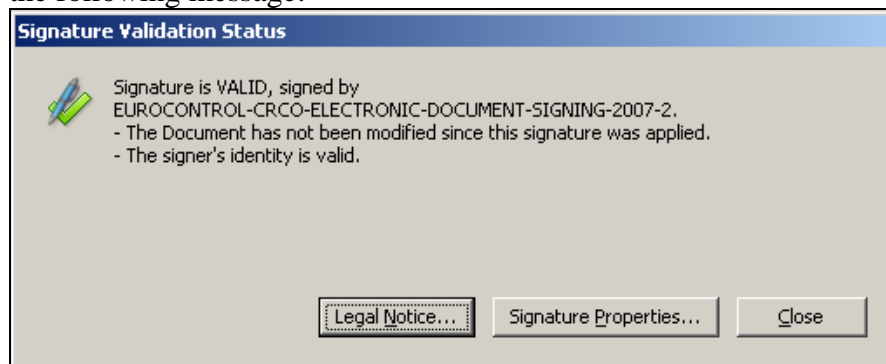
3. Click > Advanced Preferences and in the Windows Integration tab, click the option “Enable searching the Windows Certificate Store for Certificates other than yours’ and click the option *Validating signatures* under *Trust all root certificates* in the Windows Certificates.







#### **B. Validate the signature**

1. Open the PDF containing the signature, and click the Signatures button  on the left to open the Signatures panel.
2. Select the “Eurocontrol-CRCO” signature in the Signatures panel, and then choose *Validate Signature* from the Options menu. By doing this operation, Acrobat Reader is going to validate the ‘Eurocontrol CRCO....’ certificate by contacting a function of the Fedict website – Belgium E-Government Portal, <http://ocsp.pki.belgium.be>.



The Signature Validation Status describes the validity of the signature. You should have the following message:



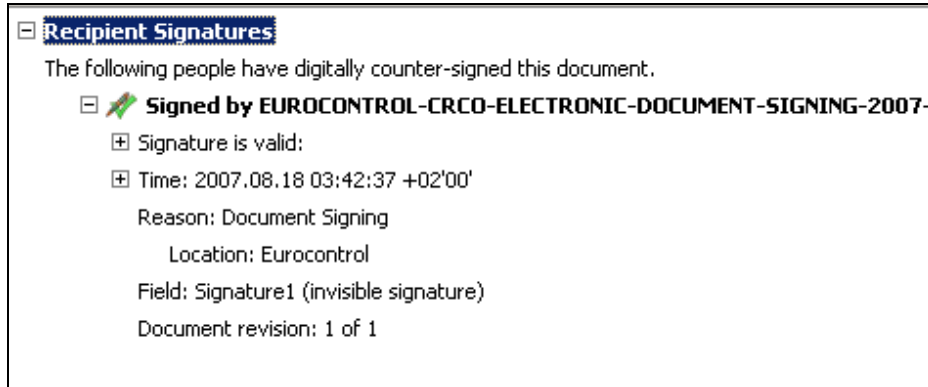
- The check mark icon  indicates that the signature is **valid**.
- The red x icon  indicates that the signature is **invalid**.
- The caution triangle icon  indicates that the **document was modified after** the signature was added.
- The question mark icon  indicates that the signature couldn't be validated because the signer's certificate **isn't in your list of trusted identities.** ( see chapter A. Point 3.)

# TECHNICAL ANNEX TO

## AGREEMENT BETWEEN EUROCONTROL AND THE “CRCO EXTRANET FOR AIRSPACE USERS (“CEFA”) USERS

If the signature status is unknown or unverified, validate the signature manually to determine the problem’s cause and possible solution. If the signature status is invalid, indicated by the red x icon  or the caution icon  **contact EUROCONTROL CRCO about the problem.**

3. On the left panel, as shown hereunder, the document version must be 1 of 1. This supports the fact that the document was not modified after the signature.



4. Click Signature Properties and then click Show Certificate to view the details of the certificate. The “Eurocontrol-CRCO ...”certificate must present a full certification path having the certificate Global Sign Root CA as Certification Authority.

