Instructions for Setting up a Digital Signature for RFV e-form
INTRODUCTION

A **Digital Signature** is a mathematical product which will allow us to demonstrate the authenticity of a message or an electronic document. A digital signature provides the receiver with the certainty that:

- the message was really created by who claims to be the sender, and
- it was not modified during its transmission.

Technically speaking it is a cryptographic tool that associates and incorporates someone’s (or some computer’s) identity to any given message or document.

The digital signature, sort of speaking, is like our own hand-written signature. It will:

1. Allow us to accredit our identity. A valid signature on a document implies that such document can be attributed without any doubt to us.

2. Imply that we will never be able to deny that such document has been signed by us. We cannot repudiate it.

3. Allow us to confirm its integrity. Any modification produced on the document from the moment of its signature to the moment it arrives to its intended recipient will affect the status of the signature making it unrecognizable and, therefore, not valid.

**What do you need to digitally sign a document or to check the authenticity of any digitally signed document received?**

- **Software.**- For any hand-written signature you need a writing tool (a pencil, a pen, etc.) in order to be able to exercise the action of actually signing. In the case of the digital signature you’ll also need a tool although, in this case, it will be software-based tool.

Again, we can establish a comparison between the hand-writing signature and the digital signature when it comes to check its veracity. In the case of the hand-writing signature we can exercise such a check by ourselves with the help of a copy of the signature that we may have in another document or in our own mind. With the digital signature, due to its special characteristics, we will need a software-based program.

Currently, we are using *Acrobat Reader version 9 or higher* to sign electronic copies of a document and/or to check the veracity of its digital signature. In case you don’t have it installed in your computer you can download it, free of charge, from Adobe’s official web site: [http://www.adobe.com/es/products/reader/](http://www.adobe.com/es/products/reader/)
**A digital identity (Digital ID):** On one side, the Digital ID is necessary for the sender’s to sign a document. On the other side, it will allow the receiver to properly identify the sender. The generation of the Digital ID is also possible with *Acrobat Reader version 9 or higher.*

Technically speaking, a Digital ID (Public Key Cryptography) is formed by two different keys. One of the keys is the Public Key stored in a certificate that can be shared with other users. The other one is the Private Key that must not be shared with anybody.

- The Private Key is secret and must be under the sole custody of its owner. This key is the one that will be used to sign electronic documents and messages.

- The Public Key (certificate) can be known by anyone. It will allow the receiver to check the digital signature of the sender. In other words, with this certificate the receiver will be able to identify who has sent the message and to confirm that it has not been altered during its transmission.
CREATE A DIGITAL ID WITH ACROBAT READER X

To create a Digital ID with Acrobat Reader X, please, follow the next steps:

1) Click on “Edit” > “Protection” > “Security Settings”:

![Image of Acrobat Reader X interface showing Security Settings]

All fields must be completed and the form communicated via Government-to-Government

REQUEST FOR VISIT

TO:

(Country / international organisation name)

2. TYPE OF INFORMATION / MATERIAL OR SITE ACCESS

- [ ] CONFIDENTIAL or above
- [ ] Access to security areas without access to classified information / material

Only if required by the laws / regulations of the countries involved

- [ ] Unclassified / RESTRICTED

3. SUMMARY

No. of sites: 1
No. of visitors: 1

4. ADMINISTRATIVE DATA:

<table>
<thead>
<tr>
<th>Requestor:</th>
<th>NSA/DSA RFV Reference No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>To:</td>
<td>Date (dd/mm/yyyy):</td>
</tr>
</tbody>
</table>
2) Then, select “Digital IDs” and press “Add ID”: 

![Image of a screenshot showing the 'Add ID' option in a digital ID management interface. The interface includes fields for selecting the type of digital ID and administrative data such as Requestor and To fields with placeholders. The screenshot also shows a pop-up window for managing digital IDs with options like 'Manage My Digital IDs' and 'Set Default' among others.]
3) After that, select “A new digital ID I want to create now” and press “Next”:
4) Next, select “New PKCS#12 digital ID file” and press “Next”: 
5) Then, please fill up the following fields and, once you have finished, press “Next”:

i) Name:

ii) Organizational Unit:

iii) Organization Name:

iv) Email Address:

v) Country / Region:

vi) Key Algorithm: 1024-bit RSA.

vii) Use digital ID for: Digital Signatures and Data Encryption.
6) After that, please specify the following:
   i) The location where you want to store the Digital ID (it is a .pfx file).
   ii) The password (necessary for using that Digital ID). This password must contain, at least, 6 characters although we recommend, for security reasons, that it contains, at least, 8 characters mixing up uppercase and lowercase letters, digits and symbols.
   iii) Press “Finish”.

![Image of a digital ID store form with fields for location, password, and administrative data]
7) Once finished, you should see the following window as it appears in the image below:
EXPORT A PUBLIC KEY (CERTIFICATE) FROM OUR DIGITAL ID

Exporting a certificate from our Digital ID will allow other users, to whom you decide to share it with, to identify all those documents that you have signed with it.

Technically speaking, a digital certificate is an electronic file that associates a given public key with the identity of its owner (and its Digital ID). Additionally, apart from the public key and the identity of its owner, a digital certificate may contain other information in order to, for example, set the public key’s conditions of use, the dates of validity of the certificate, etc.

To export a certificate from your Digital ID using Acrobat Reader 9.0, please follow the next steps:

1) Click on “Edit” > “Protection” > “Security Settings”:

![Image of a document interface with a request for visit form]
2) After that, select “Digital IDs” and choose “Export”:
3) Then, select “Save the data to a file” and press “Next”: 
4) Now, store your Digital ID certificate in the field that you choose. It is advisable to store it as "*.cer". You will find it in the “Type” box as it is shown in the image below:
5) Once you have pressed “Save”, the following message should appear in your screen:

This means that the certificate of your Digital ID has been successfully exported. After that, you’ll notice that there is a new file in the location you selected previously with the following appearance:

![CertExchangeDulce.cer](image)
CONFIGURE ACROBAT READER X FOR THE VALIDATION OF THE DIGITAL SIGNATURE

Now, we will describe the procedure for the installation of public certificates from trusted Digital IDs in the Acrobat Reader X software installed in your computer. In other words, you are going to configure Acrobat Reader so it can recognize the signatures of the documents you may receive and you will also be able to confirm the identity of the sender and the integrity of the document.

1) Click on “Edit” > “Protection” > “Manage Trusted Identities”:
2) Then, select “Add contacts”: 
3) After that, press “Browse” and search the certificate you want to install in the location where you have stored it (it may have different extensions: “.fdf”, “.p7c”, “.p7b”, “.crt”, although the most common one is “.cer”)

![Image of a form titled REQUEST FOR VISIT with fields for Type of Visit Request, No. of sites, No. of visitors, Administrative Data, and a certificate search dialog box. The form is filled out with entries like One-time, Recurring, Emergency, Amendment, 1 for No. of sites and No. of visitors, and blank fields for Requestor, NSA/DSA RFV Reference No., and Date (dd/mm/yyyy).]
4) The certificate will appear in the upper field ("Contacts") of the window, as it is shown in the image below. After that, press “Import”.
5) Then, a window will appear informing you that the certificate and its contact have been correctly imported.
6) Once you press “OK” the contact should appear in your screen as follows:
7) The certificate is already installed. However, you still have to configure the identities to which Adobe Reader will trust. Before using any contact and his certificate, it is necessary to indicate to the program that the certificate that you have already installed is trustful. To this aim you will have to do the following:

8) Select which contact you would like Acrobat Reader to recognize as trustful and then press “Details”:
9) Then, select the certificate you would like to mark as trustful and press “Edit Trust”:
10) After that, please click on “Use this certificate as a trusted root” and press “OK”:
11) Next, click on “OK” located inside the *Edit Contact* box.
12) And, last but not least, press “Close” located inside the Manage Trusted Identities box: