

Mi i

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

INTRODUCTION..... 3

CREATE A DIGITAL ID WITH ACROBAT READER X 5

EXPORT A PUBLIC KEY (CERTIFICATE) FROM OUR DIGITAL ID..... 12

**CONFIGURE ACROBAT READER X FOR THE VALIDATION OF THE DIGITAL SIGNATURE
..... 17**

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/>

- **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 ADOBE READER X

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

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

The screenshot shows the Adobe Reader X interface with the 'Security Settings' menu open. The main document is a 'REQUEST FOR VISIT' form. The form is divided into several sections:

- Header:** "All fields must be completed and the form communicated via Government-to-Government"
- Title:** "REQUEST FOR VISIT" (highlighted in yellow)
- TO:** [Redacted] (Country / international organisation name)
- 1. REASONS:** (partially obscured by the menu)
- 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:**
 - Requestor: [Redacted]
 - NSA/DSA RFV Reference No.: [Redacted]
 - To: [Redacted]
 - Date (dd/mm/yyyy): [Redacted]

2) Then, select “Digital IDs” and press “Add ID”:

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

Security Settings

Digital IDs (highlighted)

Directory Servers

Time Stamp Servers

Add ID (highlighted)

Usage Options

Certificate Details

Export

Refresh

Remove ID

Name

Issuer

Storage Mechanism

1. TYPE OF V...

One-time

Recurring

Emergenc

Amendme

MANAGE MY DIGITAL IDS

This is a list of the **digital IDs** that are available for your use on this computer. Digital IDs are *private* and should not be shared. They are used when you create a digital signature or when you decrypt documents that are encrypted for you using *Certificate Security*.

Each digital ID has a corresponding *public* certificate which contains identifying information about you and which you can share with others. This certificate is used by others to encrypt documents for you, or to validate your digital signatures. Select one of the entries above and click *Certificate Details* to view information from your certificate. Use *Export* to share your certificate with others.

Use *Set Default* to set or clear which digital ID is used by default when you sign or encrypt documents. Use *Add ID* to add a new digital ID or to find an existing digital ID and add it to this view. Use *Remove ID* to permanently remove a digital ID from this list and wherever it is stored.

4. ADMINISTRATIVE DATA:

Requestor:

NSA/DSA RFV Reference No.

To:

Date (dd/mm/yyyy):

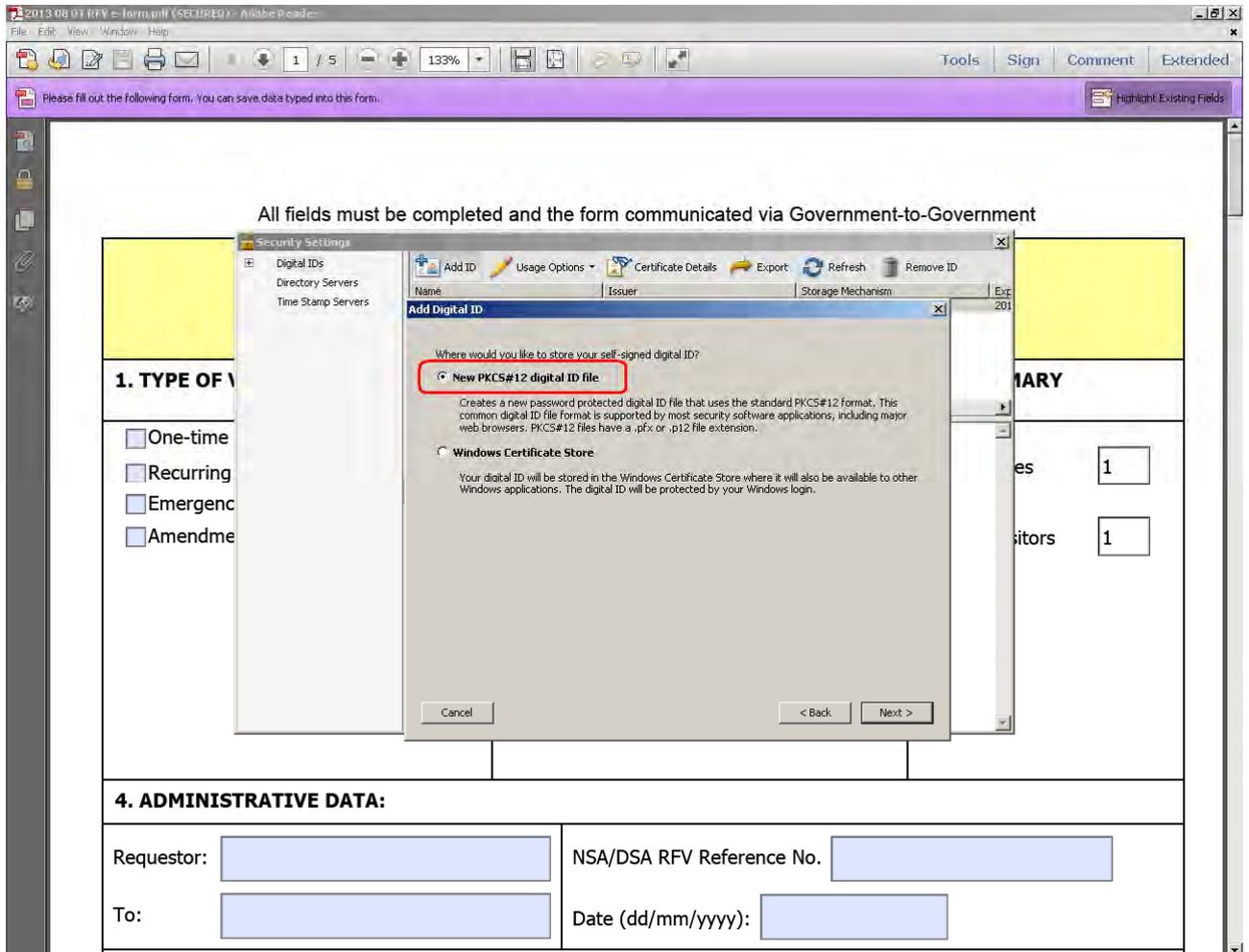
es

sitors

3) After that, select “A new digital ID I want to create now” and press “Next”:

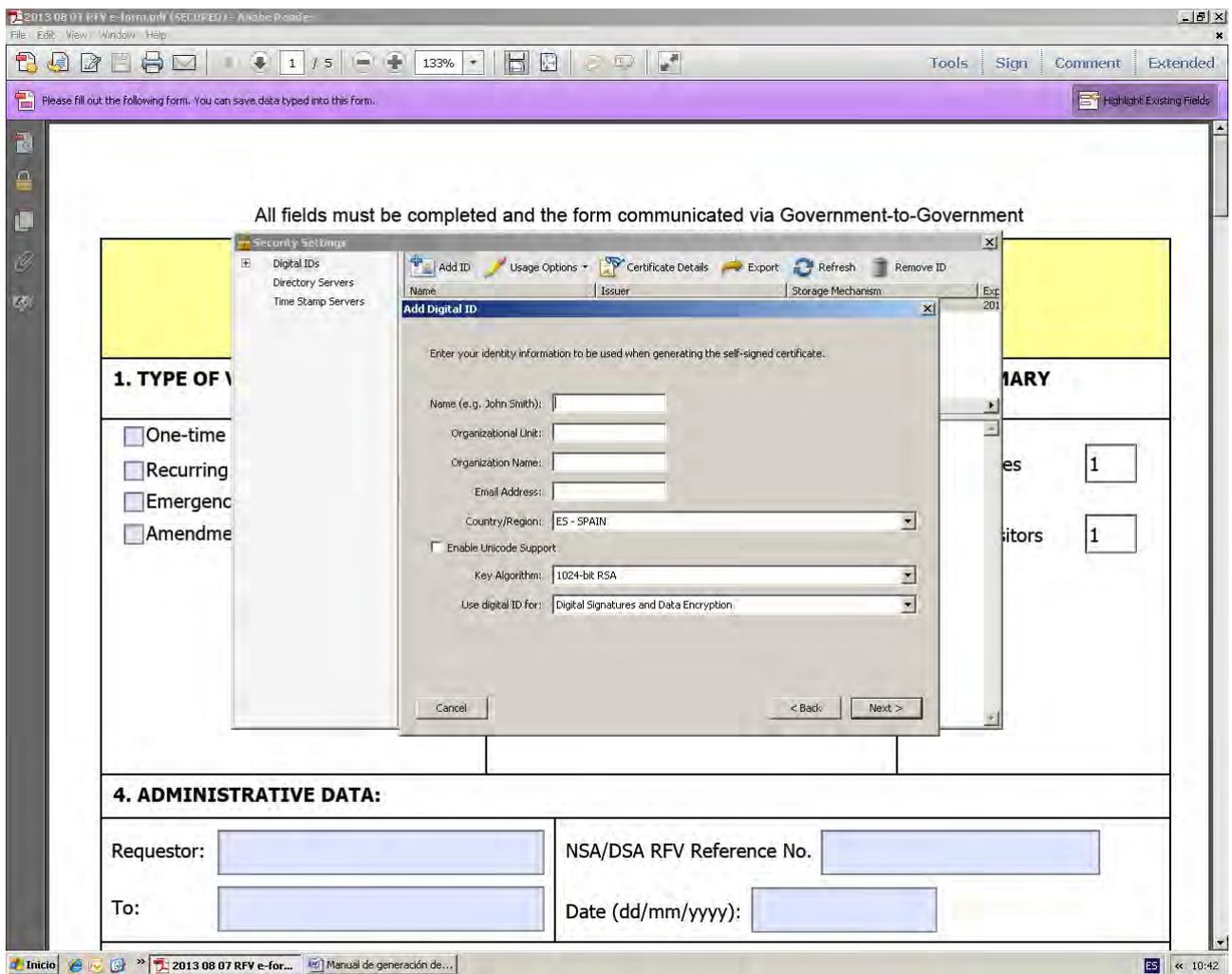
The screenshot shows a PDF form titled "2013 08 07 RFV e-form.pdf (SECURED)" in Adobe Reader. A dialog box titled "Add Digital ID" is open, prompting the user to "Add or create a digital ID to sign and encrypt documents." The dialog box has three radio button options under "My existing digital ID from:": "A file", "A roaming digital ID accessed via a server", and "A new digital ID I want to create now". The third option is selected and highlighted with a red rectangular box. The background form is partially visible, showing a header "All fields must be completed and the form communicated via Government-to-Government" and several sections: "1. TYPE OF V..." with checkboxes for "One-time", "Recurring", "Emergency", and "Amendme"; "4. ADMINISTRATIVE DATA:" with fields for "Requestor:", "To:", "NSA/DSA RFV Reference No.", and "Date (dd/mm/yyyy)"; and a "SUMMARY" section with input fields for "es" and "itors", both containing the number "1".

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”.

The screenshot shows a PDF form titled "2013 08 07 RFV e-form.pdf (SECURED)" in Adobe Reader. A dialog box titled "Add Digital ID" is open, prompting the user to enter a file location and password. The dialog box contains the following fields:

- File Name:** A text input field containing a file path: "C:\Documents and Settings\All Users\Desktop\program\Adobe\Acrobat\10.0\Fielddata". A "Browse..." button is next to it.
- Password:** A text input field containing "*****". Below it is a strength indicator showing three green bars and the word "Strong".
- Confirm Password:** A text input field containing "*****".

At the bottom of the dialog box, there are three buttons: "Cancel", "< Back", and "Finish". The "Finish" button is highlighted with a red box.

The background form has a purple header bar with the text "Please fill out the following form. You can save data typed into this form." and a "Highlight Existing Fields" button. The form content includes:

- A title: "All fields must be completed and the form communicated via Government-to-Government".
- A sidebar on the left with a tree view containing "Digital IDs", "Directory Servers", and "Time Stamp Servers".
- A section titled "1. TYPE OF V" with four radio button options: "One-time", "Recurring", "Emergency", and "Amendme".
- A section titled "4. ADMINISTRATIVE DATA:" with two columns of input fields:
 - Left column: "Requestor:" and "To:" followed by empty text boxes.
 - Right column: "NSA/DSA RFV Reference No." and "Date (dd/mm/yyyy):" followed by empty text boxes.

7) Once finished, you should see the following window as it appears in the image below:

The screenshot shows a PDF form in Adobe Reader. The main form has a purple header with the text "Please fill out the following form. You can save data typed into this form." and a "Highlight Existing Fields" button. The form content includes:

- A title: "All fields must be completed and the form communicated via Government-to-Government".
- A "Security Settings" window with a table of digital IDs:

Name	Issuer	Storage Mechanism	Exp
Dulce <aslc@areatec.com>	Dulce <aslc@areatec.com>	Digital ID File	201

Below the table, a blue-bordered box contains the following details:

Dulce
ONS
Issued by: Dulce
ONS
Valid from: 2013/09/05 11:44:44 +02'00'
Valid to: 2018/09/05 11:44:44 +02'00'
Intended usage: Sign transaction, Encrypt document

The main form also includes:

- 1. TYPE OF V** (partially visible)
- Radio buttons for: One-time, Recurring, Emergenc, Amendme.
- 4. ADMINISTRATIVE DATA:**
- Requestor: [text box]
- To: [text box]
- NSA/DSA RFV Reference No. [text box]
- Date (dd/mm/yyyy): [text box]

On the right side, there are input fields for "es" (value 1) and "itors" (value 1).

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”:

The screenshot shows the Adobe Reader interface with the 'Security Settings' menu open. The main window displays a 'REQUEST FOR VISIT' form. The form is divided into several sections:

- Header:** "All fields must be completed and the form communicated via Government-to-Government"
- Section 1:** "REQUEST FOR VISIT" with a "TO:" field containing a redacted name and the instruction "(Country / international organisation name)".
- Section 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
- Section 3: SUMMARY**
 - No. of sites:
 - No. of visitors:
- Section 4: ADMINISTRATIVE DATA:**
 - Requestor:
 - NSA/DSA RFV Reference No.:
 - To:
 - Date (dd/mm/yyyy):

2) After that, select “Digital IDs” and choose “Export”:

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

Security Settings

- Digital IDs
- Directory Servers
- Time Stamp Servers

1. TYPE OF V...

- One-time
- Recurring
- Emergenc
- Amendme

Name	Issuer	Storage Mechanism	Exp
Dulce <casic@areatec.com>	Dulce <casic@areatec.com>	Digital ID File	201

Export Refresh Remove ID

Dulce
ONS
Issued by: Dulce
ONS
Valid from: 2013/09/05 11:44:44 +02'00'
Valid to: 2018/09/05 11:44:44 +02'00'
Intended usage: Sign transaction, Encrypt document

4. ADMINISTRATIVE DATA:

Requestor: NSA/DSA RFV Reference No.

To: Date (dd/mm/yyyy):

SUMMARY

es

sitors

3) Then, select “Save the data to a file” and press “Next”:

The screenshot shows a web browser window displaying a form titled "2013 08 01 RFV e-form.pdf (SECURED) - Adobe Reader". The form has a purple header with the instruction "Please fill out the following form. You can save data typed into this form." and a "Highlight Existing Fields" button. The main content area is titled "All fields must be completed and the form communicated via Government-to-Government".

Overlaid on the form is a "Security Settings" window showing a list of digital IDs. Below it, a "Data Exchange File - Export Options" dialog box is open, displaying the following text:

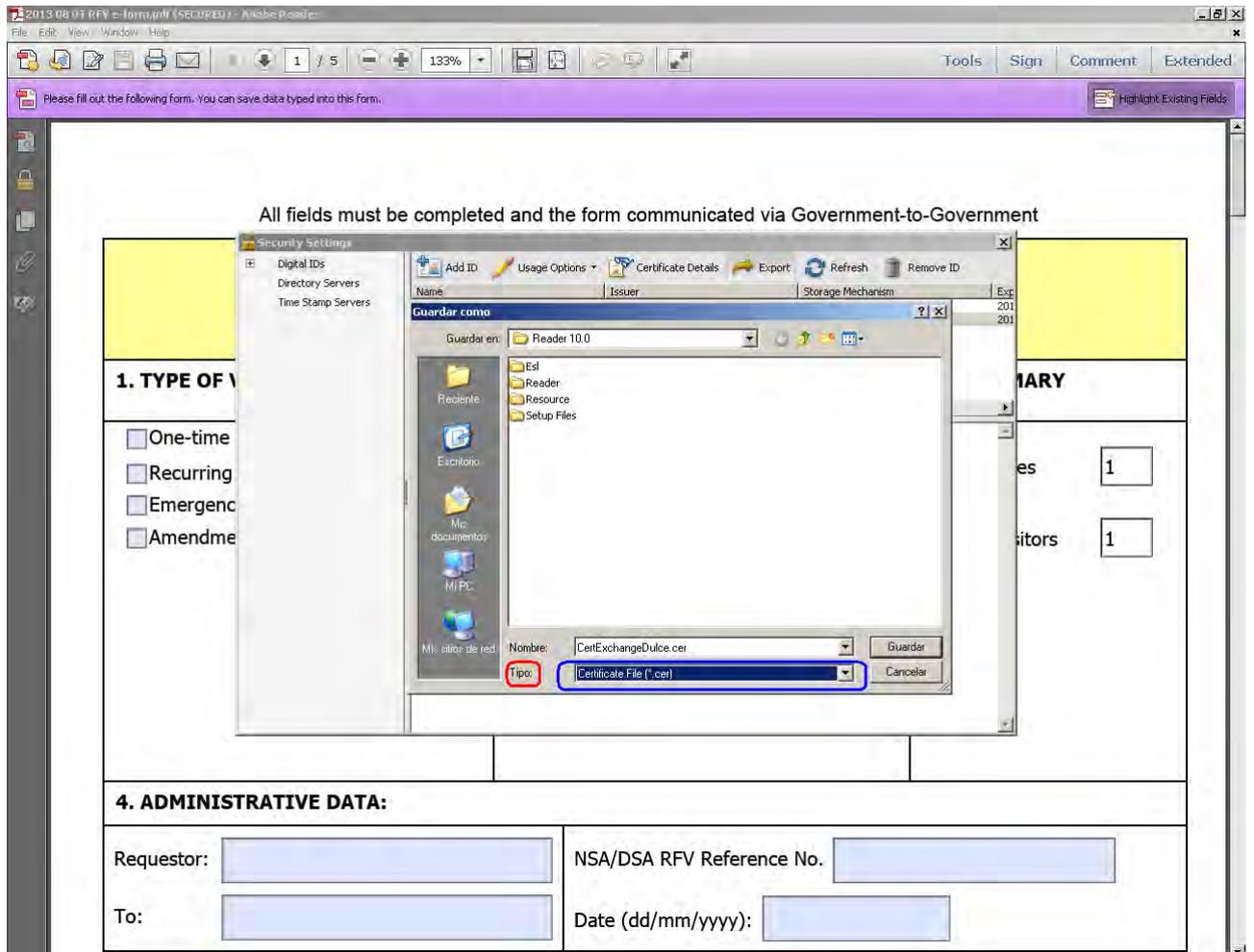
You have chosen to export the following data:
My Certificate(s)
Certificates are exported to allow the recipients to validate signatures created by you and to encrypt documents for you. Exporting your certificate does not export your private key.

Export Options
Select whether you want to save the data to a file or share it via email:
 Email the data to someone
 Save the data to a file

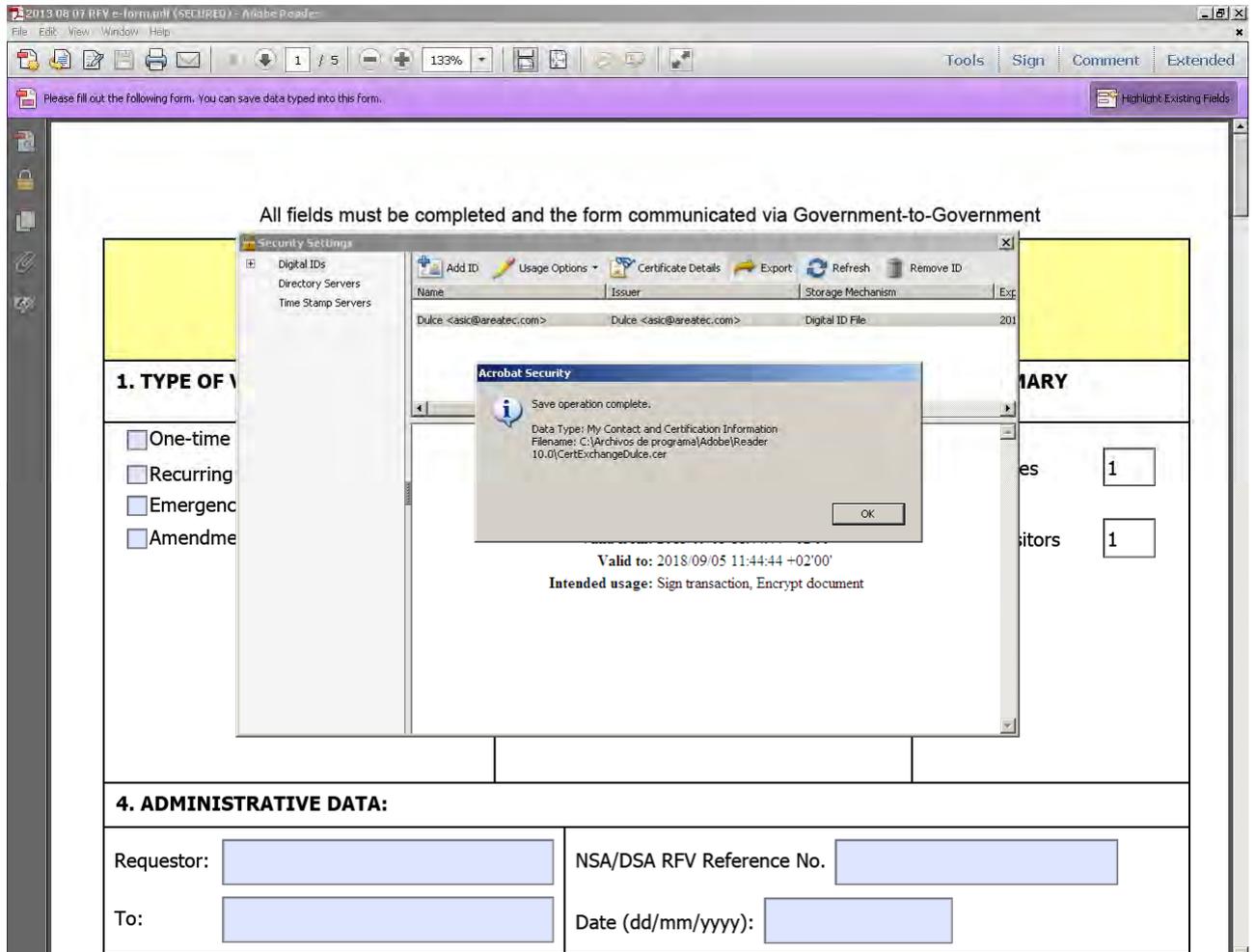
The "Save the data to a file" option is highlighted with a red circle. The dialog box has "Next" and "Cancel" buttons.

The form itself is divided into sections. Section 1, "1. TYPE OF V...", has four radio button options: "One-time", "Recurring", "Emergency", and "Amendme". Section 4, "4. ADMINISTRATIVE DATA:", contains four input fields: "Requestor:", "NSA/DSA RFV Reference No.", "To:", and "Date (dd/mm/yyyy):".

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:



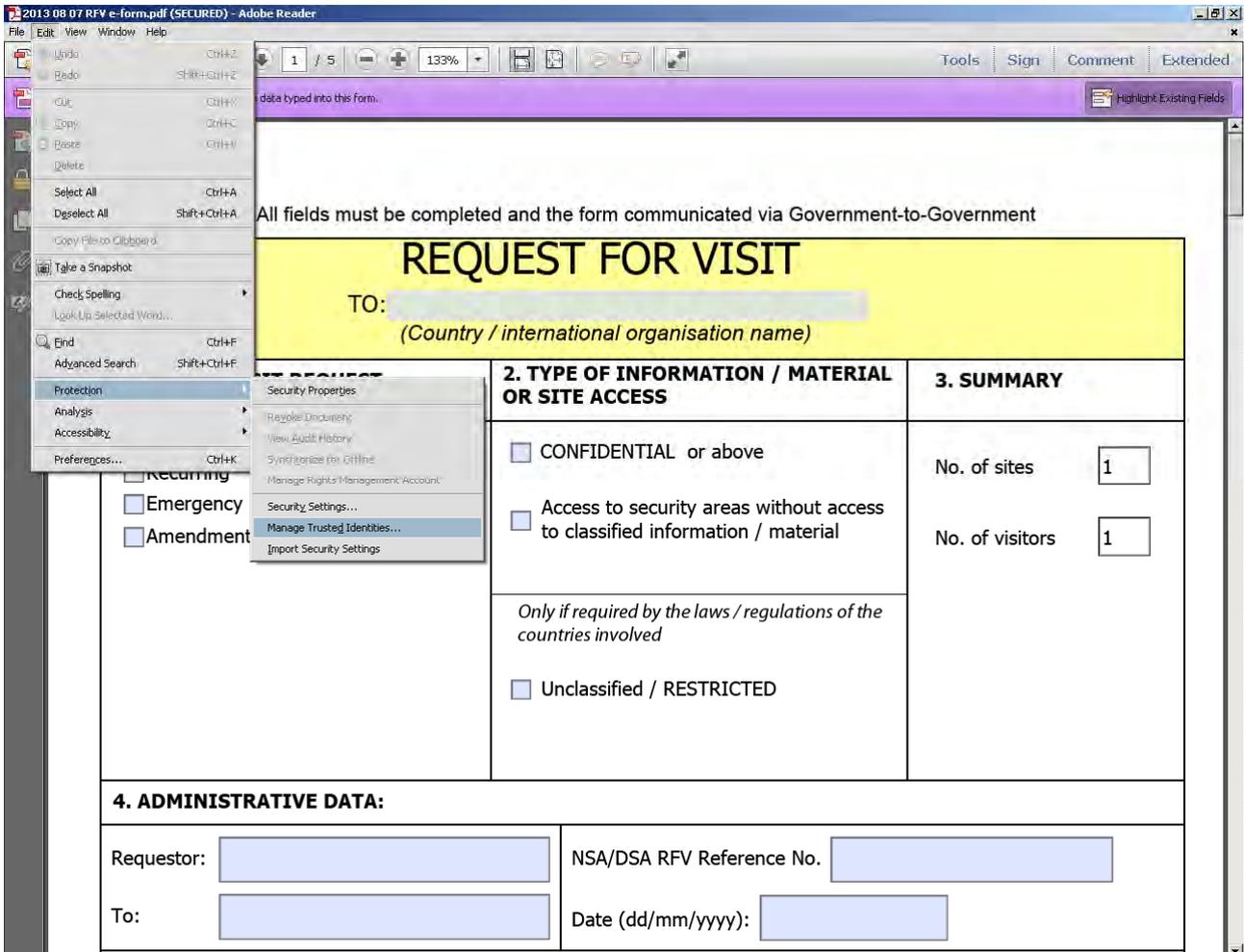
This means that the certificate of your Digital ID has been successfully exported. After that, you'll notice that there is a new file in the location you selected previously with the following appearance:



CONFIGURE ADOBE 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”:

The screenshot shows a web browser window displaying a form titled "REQUEST FOR VISIT". The form is divided into several sections:

- 1. TYPE OF VISIT REQUEST:** Includes checkboxes for "One-time", "Recurring", "Emergency", and "Amendment".
- 3. SUMMARY:** Includes input fields for "No. of sites" (value: 1) and "No. of visitors" (value: 1).
- 4. ADMINISTRATIVE DATA:** Includes input fields for "Requestor:", "To:", "NSA/DSA RFV Reference No.", and "Date (dd/mm/yyyy)".

A "Manage Trusted Identities" dialog box is overlaid on the form. It has a "Display:" dropdown menu set to "Contacts". The "Add Contacts..." button is highlighted with a red rectangle. Other buttons in the dialog include "Request Contact...", "Details...", "Export...", "Delete", "New Group...", "Help", and "Close".

At the bottom of the dialog box, there is a checkbox labeled "Unclassified / RESTRICTED".

- 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”)

The screenshot shows a web browser window with the title "2013 08 07 RFV e-form.pdf (SECURED) - Adobe Reader". The browser's address bar shows "Please fill out the following form. You can save data typed into this form." The main content area displays a form titled "REQUEST FOR VISIT" with a yellow header. The form is divided into several sections:

- 1. TYPE OF VISIT REQUEST:** Contains four radio button options: "One-time", "Recurring", "Emergency", and "Amendment".
- 3. SUMMARY:** Contains two input fields: "No. of sites" with the value "1" and "No. of visitors" with the value "1".
- 4. ADMINISTRATIVE DATA:** Contains four input fields: "Requestor:", "NSA/DSA RFV Reference No.", "To:", and "Date (dd/mm/yyyy):".

A dialog box titled "Choose Contacts to Import" is overlaid on the form. It contains two sections: "Contacts" and "Certificates". The "Contacts" section has a table with columns "Name" and "Email", and buttons "Remove", "Browse ..." (highlighted with a red box), and "Search ...". The "Certificates" section has a table with columns "Subject", "Issuer", and "Expires", and buttons "Details ..." and "Trust ...". The dialog box also has "Help", "Import", and "Cancel" buttons at the bottom.

- 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”.

The screenshot shows a web browser window displaying a form titled "REQUEST FOR VISIT". The form is divided into several sections:

- 1. TYPE OF VISIT REQUEST:** Includes radio buttons for "One-time", "Recurring", "Emergency", and "Amendment".
- 3. SUMMARY:** Includes input fields for "No. of sites" (value: 1) and "No. of visitors" (value: 1).
- 4. ADMINISTRATIVE DATA:** Includes input fields for "Requestor:", "To:", "NSA/DSA RFV Reference No.", and "Date (dd/mm/yyyy)".

A dialog box titled "Choose Contacts to Import" is overlaid on the form. It contains a table of contacts with columns for "Name" and "Email". One contact is listed: "Dulce" with email "asik@areatec.com". The "Import" button at the bottom of the dialog is highlighted with a red box.

5) Then, a window will appear informing you that the certificate and its contact have been correctly imported.

2013 06 07 RFV e-form.pdf (SECURED) - Adobe Reader

File Edit View Window Help

Tools Sign Comment Extended

Please fill out the following form. You can save data typed into this form. Highlight Existing Fields

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

REQUEST FOR VISIT

1. TYPE OF VISIT REQUEST

One-time

Recurring

Emergency

Amendment

Unclassified / RESTRICTED

3. SUMMARY

No. of sites

No. of visitors

4. ADMINISTRATIVE DATA:

Requestor: <input type="text"/>	NSA/DSA RFV Reference No. <input type="text"/>
To: <input type="text"/>	Date (dd/mm/yyyy): <input type="text"/>

6) Once you press “OK” the contact should appear in your screen as follows:

The screenshot shows a web browser window with the title "2013 08 07 RFV e-form.pdf (SECURED) - Adobe Reader". The browser's address bar shows "1 / 5" and "133%". The page content includes a purple header with the text "Please fill out the following form. You can save data typed into this form." and a "Highlight Existing Fields" button. The main content area has a yellow header with the text "All fields must be completed and the form communicated via Government-to-Government" and a large yellow box with the title "REQUEST FOR VISIT".

The form is divided into several sections:

- 1. TYPE OF VISIT REQUEST:** Contains four radio button options: "One-time", "Recurring", "Emergency", and "Amendment".
- 3. SUMMARY:** Contains two input fields: "No. of sites" with the value "1" and "No. of visitors" with the value "1".
- 4. ADMINISTRATIVE DATA:** Contains four input fields: "Requestor:", "NSA/DSA RFV Reference No.", "To:", and "Date (dd/mm/yyyy):".

A "Manage Trusted Identities" dialog box is open in the center of the screen. It has a "Display:" dropdown menu set to "Contacts". Below the dropdown is a list of contacts, with "Dulce" selected and highlighted by a blue box. To the right of the list are buttons for "Add Contacts...", "Request Contact...", "Details...", "Export...", "Delete", and "New Group...". At the bottom of the dialog are "Help" and "Close" buttons.

- 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”:

The screenshot shows the Adobe Reader interface with a PDF form titled "REQUEST FOR VISIT". The form is divided into several sections:

- 1. TYPE OF VISIT REQUEST:** Includes checkboxes for "One-time", "Recurring", "Emergency", and "Amendment".
- 3. SUMMARY:** Includes input fields for "No. of sites" (value: 1) and "No. of visitors" (value: 1).
- 4. ADMINISTRATIVE DATA:** Includes fields for "Requestor:", "NSA/DSA RFV Reference No.", "To:", and "Date (dd/mm/yyyy)".

A "Manage Trusted Identities" dialog box is open over the form. It shows a list of contacts with "Dulce" selected. The "Details..." button in the dialog is highlighted with a red rectangle. The dialog also includes buttons for "Add Contacts...", "Request Contact...", "Export...", "Delete", "New Group...", "Help", and "Close".

9) Then, select the certificate you would like to mark as trustful and press “Edit Trust”:

The screenshot shows a web browser window displaying a secured PDF form titled "2013 08 07 RFV e-Form.pdf (SECURED) - Adobe Reader". The form is titled "REQUEST FOR VISIT" and contains the following sections:

- 1. TYPE OF VISIT REQUEST:** Includes radio buttons for "One-time", "Recurring", "Emergency", and "Amendment".
- 3. SUMMARY:** Includes input fields for "No. of sites" (value: 1) and "No. of visitors" (value: 1).
- 4. ADMINISTRATIVE DATA:** Includes input fields for "Requestor:", "NSA/DSA RFV Reference No.", "To:", and "Date (dd/mm/yyyy):".

A "Manage Trusted Identities" dialog box is open over the form. It displays a table of certificates:

Name	Issuer	Expires
Dulce <...>	Dulce <as...>	2018.09....

The "Edit Trust..." button in the dialog is highlighted with a red box. The dialog also includes buttons for "Associate Certificates...", "Remove Association", "Show Certificate...", "OK", and "Cancel".

10) After that, please click on “Use this certificate as a trusted root” and press “OK”:

The image shows a screenshot of a PDF form titled "2013 08 07 REV e-form.pdf (SECURED) - Adobe Reader". The form is partially filled out, and an "Import Contact Settings" dialog box is open in the center. The dialog box displays the following information:

- Certificate Details:**
 - Subject: Dulce <asic@areatec.com>
 - Issuer: Dulce <asic@areatec.com>
 - Usage: Sign transaction, Encrypt document
 - Expiration: 05/09/2018 9:44:44
- Trust:** Policy Restrictions
- Policy Restrictions:**
 - A certificate used to sign a document must either be designated as a trust anchor or chain up to a trust anchor in order for signature validation to succeed. Revocation checking is not performed on or above a trust anchor.
 - Use this certificate as a trusted root
 - If signature validation succeeds, trust this certificate for:
 - Signed documents or data
 - Certified documents
 - Dynamic content
 - Embedded high privilege JavaScript
 - Privileged system operations (networking, printing, file access, etc.)

The background form has the following sections:

- 1. TYPE OF VISIT REQUEST:** Includes radio buttons for One-time, Recurring, Emergency, and Amendment.
- 3. SUMMARY:** Includes input fields for "No. of sites" (value: 1) and "No. of visitors" (value: 1).
- 4. ADMINISTRATIVE DATA:** Includes input fields for "Requestor:", "To:", "NSA/DSA RFV Reference No.", and "Date (dd/mm/yyyy)".

The "OK" button in the dialog box is highlighted with a red rectangle.

11) Next, click on “OK” located inside the *Edit Contact* box.

2013 08 07 RFV e-Form.pdf (SECURED) - Adobe Reader

File Edit View Window Help

Tools Sign Comment Extended

Please fill out the following form. You can save data typed into this form. Highlight Existing Fields

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

REQUEST FOR VISIT

1. TYPE OF VISIT REQUEST

One-time

Recurring

Emergency

Amendment

Unclassified / RESTRICTED

3. SUMMARY

No. of sites

No. of visitors

4. ADMINISTRATIVE DATA:

Requestor: <input style="width: 100%;" type="text"/>	NSA/DSA RFV Reference No. <input style="width: 100%;" type="text"/>
To: <input style="width: 100%;" type="text"/>	Date (dd/mm/yyyy): <input style="width: 100%;" type="text"/>

Manage Trusted Identities

Display: Contact

Edit Contact

Contact Name: Dulce

Email Address: asic@areatec.com

Contact Information:

Name	Issuer	Expires
Dulce <...>	Dulce <as...>	2018/09/...

12) And, last but not least, press “Close” located inside the *Manage Trusted Identities* box:

The screenshot shows a web browser window with a document titled "2013 08 07 RFV e-form.pdf (SECURED) - Adobe Reader". The browser's address bar shows "1 / 5" and "133%". The page content includes a header "All fields must be completed and the form communicated via Government-to-Government" and a main heading "REQUEST FOR VISIT".

The form is divided into several sections:

- 1. TYPE OF VISIT REQUEST:** Includes radio buttons for "One-time", "Recurring", "Emergency", and "Amendment".
- 3. SUMMARY:** Includes input fields for "No. of sites" (value: 1) and "No. of visitors" (value: 1).
- 4. ADMINISTRATIVE DATA:** Includes input fields for "Requestor:", "To:", "NSA/DSA RFV Reference No.", and "Date (dd/mm/yyyy)".

A "Manage Trusted Identities" dialog box is open in the center, showing a list of contacts with "Dulce" selected. The dialog box has a "Close" button highlighted with a blue rectangle.