

02.12.2021

Electronic certificate issuance application for Bank of Spain user institutions (Version 02).

Registration number: I.E.2019.03

Control Sheet

Title	User's Manual for the Electronic Certificate Issuance Application for Bank of Spain User Institutions
Code	DCPAUTE
Version	02
Date	02/12/2021

Version Control

Version	Date	Reason for the change
01	26/09/2019	Version one
02	02/12/2021	Modification of screens flow in the record and signature of a certificate request.

Internal Distribution List	
Paper/Digital	Recipient

CONTENTS

1	Introduction	4
2	Application technical requirements	5
2.1	Authentication requirements.	5
2.2	Client end technology requirements	5
2.2.1	Compatible browser	5
2.2.2	Trust in the PKIBDE certification hierarchy	5
2.2.3	Installation of the electronic signature component	5
2.2.4	Trusted URL settings for different browsers	7
3	Description of the application	12
3.1	Home page	12
3.2	Installation of certificates from Certification Authorities	12
3.3	Consult your institution's data	12
3.4	Consult and generate certificate applications	12
3.4.1	Details of the certificate request	13
3.4.2	Record of a certificate request	14
3.4.3	Downloading a certificate	17
3.5	Manage your institution's certificate	18
3.5.1	Details of the certificate	19
3.5.2	Revoking a certificate	20
3.5.3	Renewing a certificate	20
4	Error and warning messages	21
4.1	System Error	21
4.2	Application under maintenance	21
4.3	Messages on home page	22
4.4	Messages while downloading the certificate	22
4.5	Messages in the record of a request	22
4.6	Messages during the signing of the request	23
4.7	Messages in the renewal of a certificate	23

1 Introduction

This document describes the use of the DCP application, which enables the management of electronic certificates issued by the BKI of the Bank of Spain (hereinafter, PKIBDE) by means of external entities.

The application allows to undertake the proceedings detailed as follow:

- Check electronic certificate data and pending requests.
- Request new electronic certificates.
- Renew certificates about to expire.
- Revoke certificates relevant to the entity.

Certificates obtained via this application are known as generic components for external entities (the certification policy for which may be found in the website policy section <https://pki.bde.es>) and they may be used to electronically exchange information via the corporate applications BdE makes available to the entities.

2 Application technical requirements

2.1 Authentication requirements.

Access to application is verified by means of electronic certificates. Particularly, electronic certificates of any of the two types established below are admitted:

- Electronic certificate of legal entity or legal entity representative issued by a Trusted Service Provider. Users can check the list of supported TSPs in the list available at <https://pki.bde.es/pkibde/es/menu/certacceptados/>.
- Generic certificate of IT components for external entities issued by PKIBDE.
- The Tax ID Number (NIF) or the Business Identifier Code (BIC8) included in the certificate and used to access will be used as the entity's identification code. Please note that, therefore, if the entity changes the NIF or has several different NIFs, different entities will be considered and users must have different certificates to access.

2.2 Client end technology requirements

The user equipment that accesses the DCP application must meet several requirements:

- Compatible browser.
- Trust in the PKIBDE certification hierarchy.
- Installation of the electronic signature component
- Trust in the Web application URL

Each one of the previous requirements is detailed below.

2.2.1 Compatible browser

Access to the DCP application must be through one of the browsers indicated below:

- Internet Explorer 9 (or later).
- Mozilla Firefox 52 (or later).
- Google Chrome 55 (or later).

2.2.2 Trust in the PKIBDE certification hierarchy

PKIBDE hierarchy must have been installed on the user's device. The steps to be followed for the installation are detailed in the document [BDE-Installation manual of certification hierarchy of PKIBDE-V01.](#)

2.2.3 Installation of the electronic signature component

Requesting or renewing a certificate through this application requires electronically signing the request with the same certificate used to access. In order to sign, the electronic signature component of the BdE is used.

If the browser used to access is Internet Explorer, the electronic signature component is an ActiveX; if the browser used to access is Google Chrome or Mozilla Firefox, it will be a browser

extension. Please follow the relevant steps regarding the browser to be used to access the application.

2.2.3.1 Installation in Internet Explorer

There are two different alternatives if the used browser is Internet Explorer:

- The ActiveX component is automatically installed when the request signature webpage is first accessed. This automatic installation only works if the signature webpage is accessed from a computer on which administrative privileges are available.
- It is also possible to download the ActiveX component installation program from the webpage <http://pki.bde.es/pkibde/es/menu/solicitudes/> (link "Electronic signature component installer for Internet Explorer"), for which administration privileges will be required.

Follow the instructions detailed in 2.2.4 *Trusted URL settings for different browsers* in order to set the required options to allow downloading and running ActiveX add-ons in the browser.

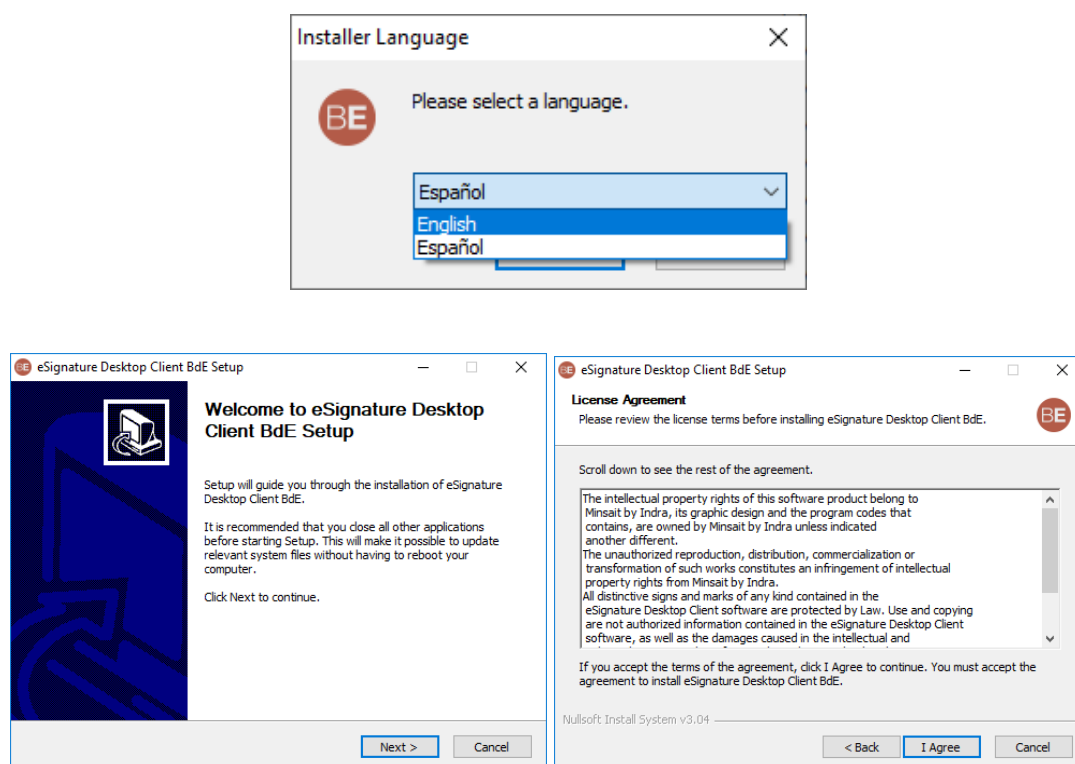
2.2.3.2 Installation in Google Chrome and/or Mozilla Firefox

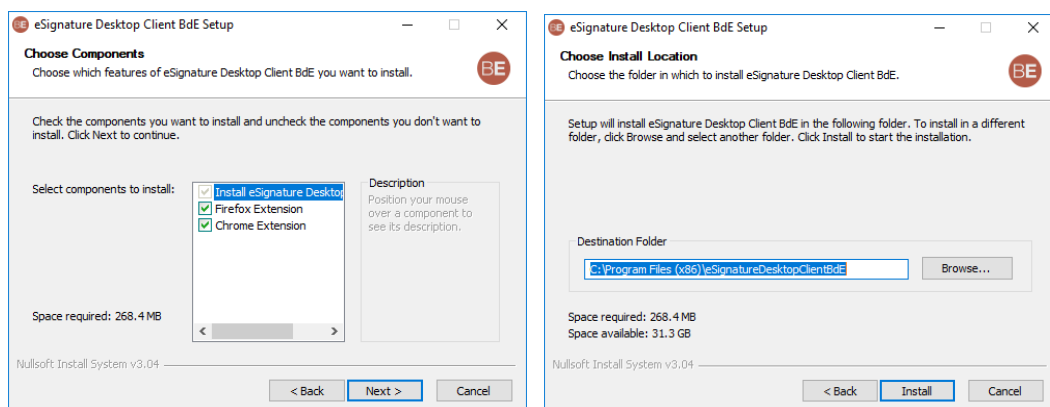
In the case that Mozilla Firefox or Google Chrome browsers are used, it will be necessary to install eSignature Desktop Client beforehand, that you can find in the following link:

<https://pki.bde.es/dcp/eSignatureDesktopClientBdE-setup-win.exe>

The application is installed on the user's computer, for this it is essential that the user has write permissions on the route where to install it.

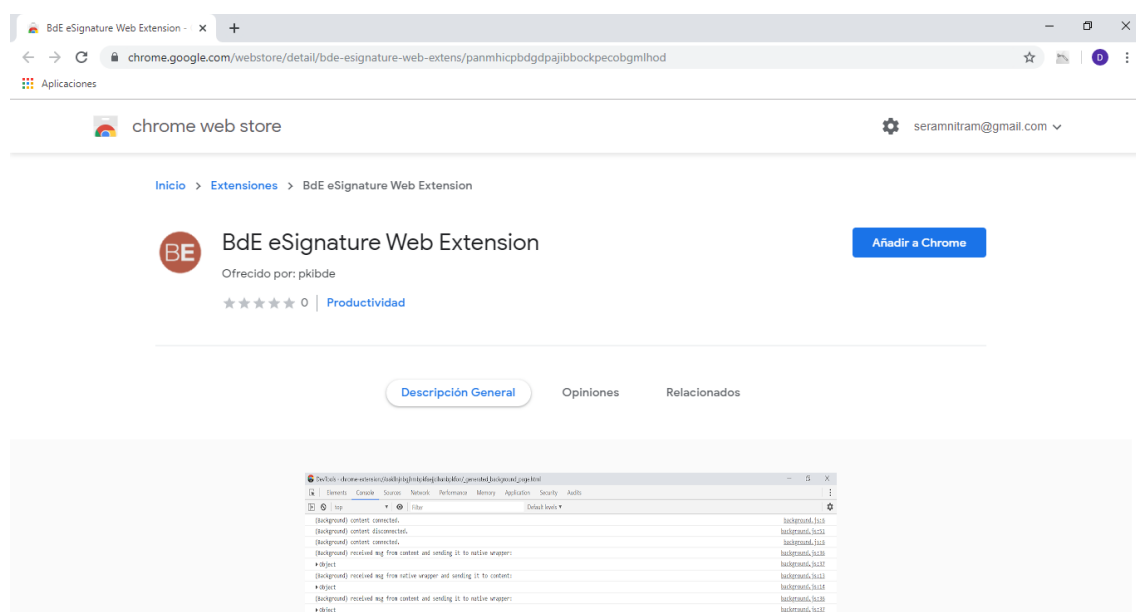
Once downloaded to the computer, run the installer and follow the instructions:





The extension allows, as shown on the screen, to choose for which browsers the user wants to enable it, as well as to choose the language.

When the extension is installed, the selected browsers (Firefox, Chrome or both) will open, if both are installed on the computer.



After adding it to the browser, the component is installed.

2.2.4 Trusted URL settings for different browsers

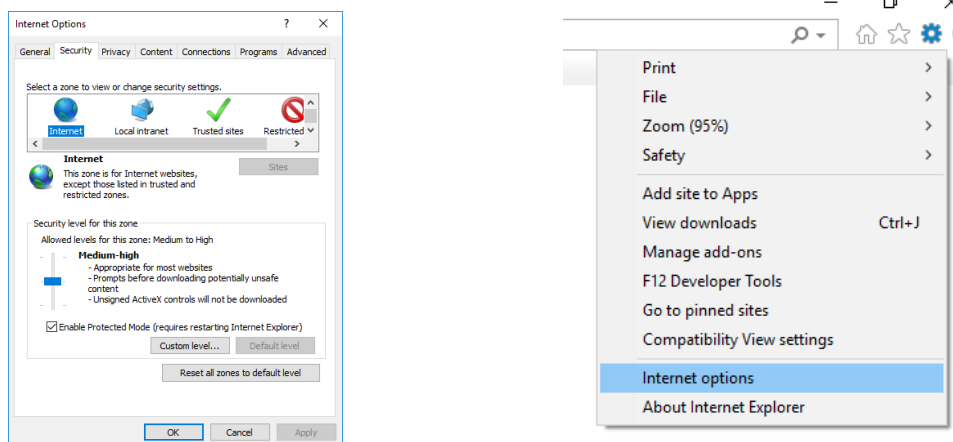
The user must include the following addresses in the list of Trusted Sites of the browser:

- <https://app.bde.es>
- <https://aps.bde.es>

The way to include a trusted URL, thus allowing components to be installed from that place, is different depending on the browser used:

Internet Explorer

The “Internet Options” option can be accessed from the tools menu. In the pop-up window, access the security tab and click on “Trusted Sites”:



Click on the “Sites” button and add the desired address in the pop-up window.

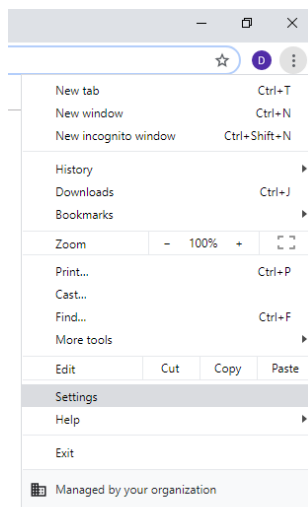
Additionally, it must be verified that the “Trusted Sites” zone allows the download and execution of ActiveX components. To do this, in the "Trusted Sites" area of the Security tab, press the "Custom level ..." button, access the "ActiveX Controls and Add-ons" section and confirm that the following options are set:

- Binary and Script Behaviours: enabled
- Download signed ActiveX controls: enabled
- Run ActiveX controls and plug-ins: enabled
- Script ActiveX Controls marked safe for scripting: enabled
- Initialize and script ActiveX controls not marked as safe: enabled
- Only allow approved domains to use ActiveX without prompt: disabled
- Allow previously unused ActiveX controls to run without prompt: enabled

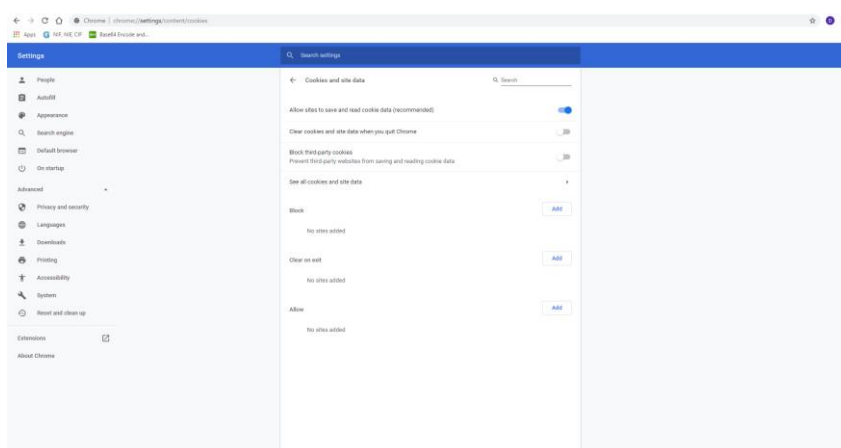
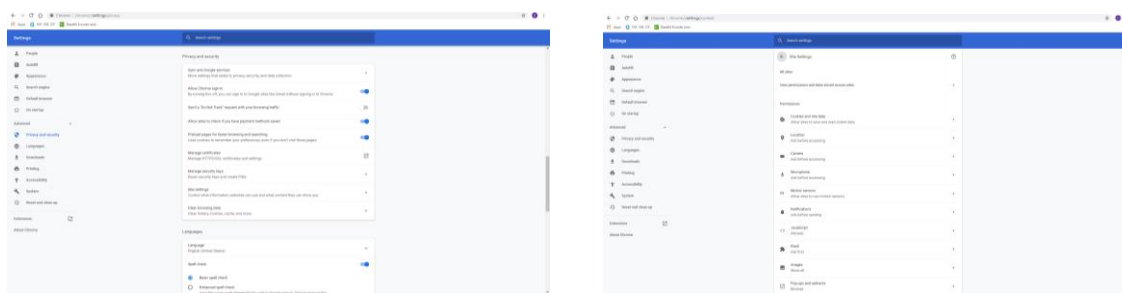
Press *Accept* and *Accept* again. Restart your browser for the new configuration to be applied.

Google Chrome

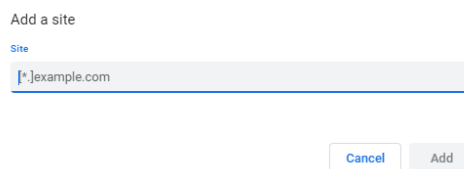
Access the Settings option in the tools menu:



In the pop-up window, access “Advanced Settings”, “Privacy and Security”, “Website Settings”, “Cookies and Site Data”.

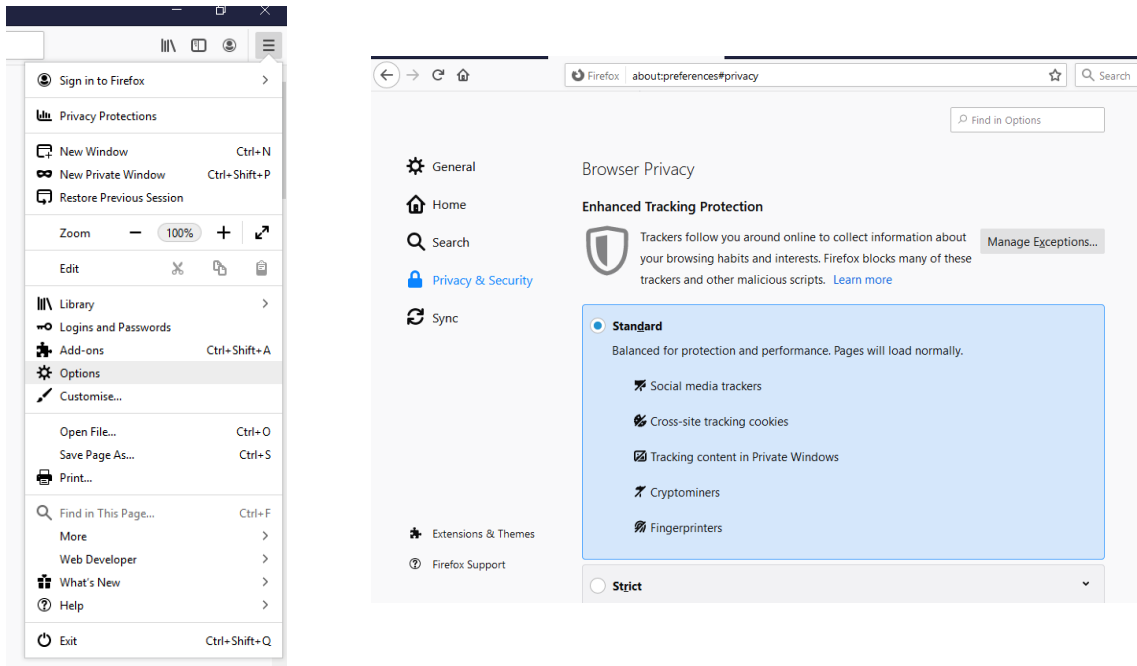


By clicking on the Add button, a website can be added:

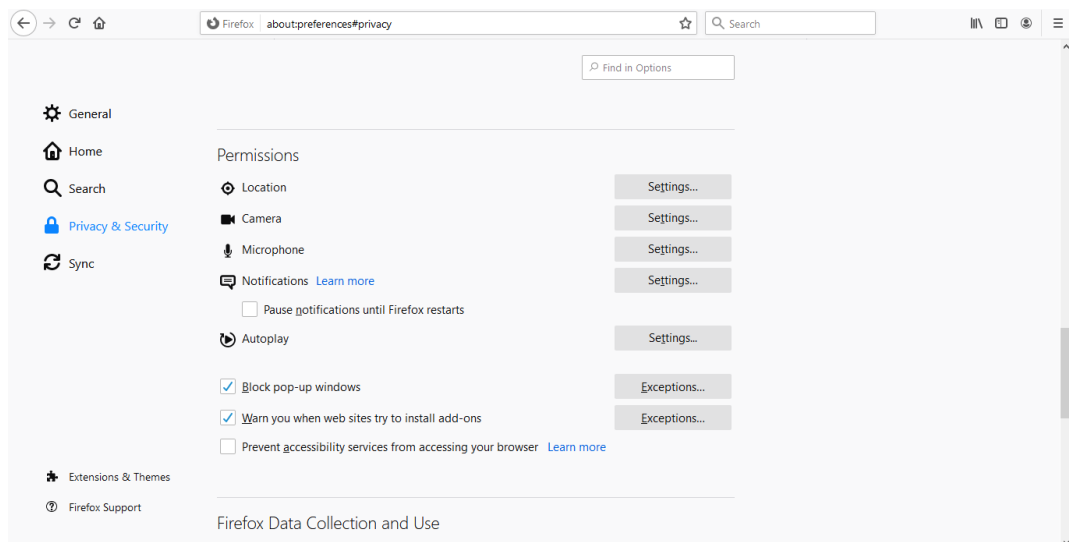


Mozilla Firefox:

Also access the Options, Security & Privacy menu:



Move the scroll bar until reaching “Permissions”:



By clicking on the “Exceptions...” buttons, a specific website can be chosen to allow components to be installed and open pop-up windows:

Allowed Web Sites - Pop-ups X

You can specify which web sites are allowed to open popup windows. Type the exact address of the site you want to allow and then click Allow.

Address of web site

Allow

Web Site	Status
https://apps.indraweb.net	Allow
https://employee.indraweb.net	Allow

Remove Web Site Remove All Web Sites

Cancel Save Changes

Allowed Web Sites - Add-ons Installation X

You can specify which web sites are allowed to install add-ons. Type the exact address of the site you want to allow and then click Allow.

Address of web site

Allow

Web Site	Status
https://fpm.firefox.com	Allow
https://addons.mozilla.org	Allow
https://private-network.firefox.com	Allow

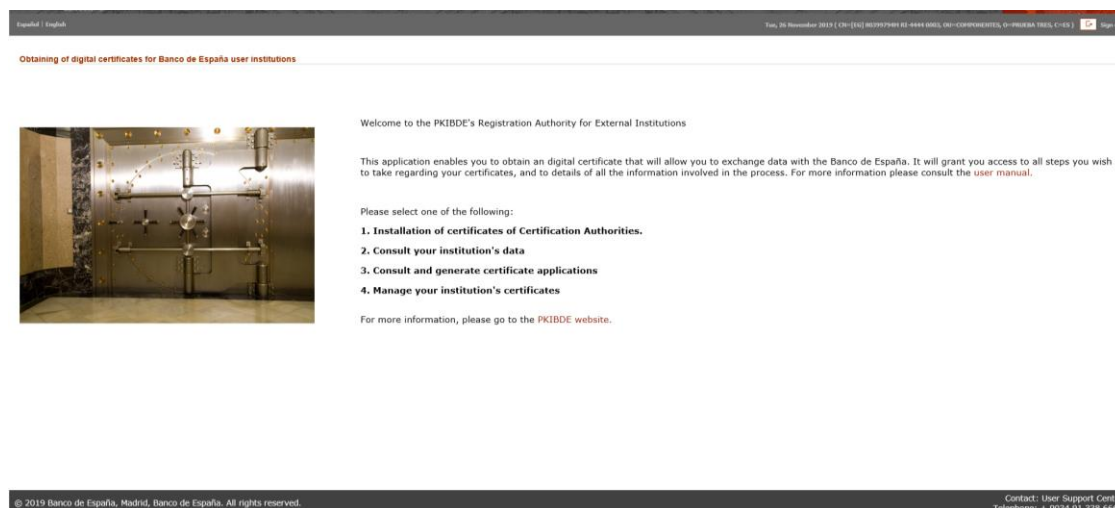
Remove Web Site Remove All Web Sites

Cancel Save Changes

3 Description of the application

3.1 Home page

Successful authentication in the application will show the home page, similar to the one that can be seen below:



Note that the contents of the Subject field of the certificate with which the user has accessed are shown in the upper right section of the page. If a generic external entity component certificate issued by PKIBDE was used, the NIF or BIC is included in that field, as can be seen, marked with a circle in red, in the previous image.

The home page shows several available options, which are detailed below:

3.2 Installation of certificates from Certification Authorities

Link to the page: https://pki.bde.es/pkibde/es/menu/certificados_pki, where certificates from Certification Authorities can be downloaded. They are needed so the user's browser will recognise certificates issued by the BdE.

3.3 Consult your institution's data

Applicant Institution's detail

Institution detail	Applications	Certificates
Institution's data		
Corporate name	PRUEBA TRES	
NIF(tax ID number)/BIC	80399794H	
Maximum number of certificates	20	
Institution code	--	

[Back](#)

By selecting this option, the data of the entity are displayed:

Note that two other tabs are available (Applications and Certificates). They provide quick access to the management of certificate requests and certificates issued respectively.

3.4 Consult and generate certificate applications

By virtue of this option, the history of requests made by the entity is displayed, indicating its use, the state thereof and date of request.

Applications

Institution detail Applications Certificates

Certificate usage	State	Application date
Inspection-secure mail	USER PENDING	04/11/2019 12:50:59
Inspection-secure mail	FINISHED	04/11/2019 09:23:51
Sepblac	USER PENDING	17/10/2019 09:14:14
Inspection-secure mail	FINISHED	15/10/2019 14:50:08

New Back

By default, applications are sorted by request date, and this order can be changed by clicking on the column heading "Application date".

Similarly, they can be sorted alphabetically by state, by clicking on the column heading.

The possible states of any request are:

- **APPROVAL PENDING:** the entity must wait for the application to be approved by the BdE.
- **DOWNLOAD PENDING:** the application has been approved and the entity can download the certificate. Note that the download operation can be done only once.
- **FINISHED:** The certificate has already been downloaded. Please note that it is not possible to repeat the download once the request is in this state.
- **CANCELLED:** The request has been cancelled and no operation on it can be performed.
- **EXPIRED:** Once a request has been created, 30 days are available to complete the process, after the last change in the status of the request. If this deadline is exceeded, the request will be considered EXPIRED and no operation can be performed on it.

By clicking on the "Certificate usage" field of each record, the details of the application can be accessed, with its different options detailed in section [3.4.1 Details of the request](#).

The lower button "New" is linked to the record of new certificate requests, which is detailed in section [3.4.2 Record of a certificate request](#).

3.4.1 Details of the certificate request

In the list of applications, by clicking on each one of them, every detail is presented with different information and options according to the status thereof.

3.4.1.1 Approval pending and finished


Applicant Institution's detail

Application's data	
NIF(tax ID number)/BIC	80399794H
Corporate name	PRUEBA TRES
Application detail	
Use for which the certificate is requested	Inspection-secure mail
Email	
Certificate manager's details	
Name (certificate manager)	GONZALEZ , FERNANDO
Position	REPRESENTANTE
Tel.	91827384748
Type of ID document	Spanish tax ID/foreigner ID card
ID card/Passport number	960233098
Email (certificate manager)	qdanmmx@correo.interno
Application's data	
State	FINISHED
Creation date	15/10/2019 14:50:08

[Applications list](#)

3.4.1.2 Download pending

Applicant Institution's detail

 **The application for certificate will expires 16/11/2019**

Application's data	
NIF(tax ID number)/BIC	80399794H
Corporate name	PRUEBA TRES
Application detail	
Use for which the certificate is requested	Segplac
Email	
Certificate manager's details	
Name (certificate manager)	FUENTES , PABLO
Position	DIRECTOR
Tel.	9111131233
Type of ID document	Spanish tax ID/foreigner ID card
ID card/Passport number	452081908
Email (certificate manager)	qdanmmx@correo.interno
Application's data	
State	DOWNLOAD PENDING
Creation date	17/10/2019 09:14:14

[Applications list](#)[Process application](#)

In this case, the "Process application" button is displayed, which allows the download of the certificate as described in section [3.4.3 Certificate download](#).

3.4.2 Record of a certificate request

By clicking on the "New" button from the webpage of the list of applications, the following record form is accessed:

Registration of application for certificate

Applicant Institution's details

NIF(tax ID number)/BIC 80399794H
Corporate name PRUEBA TRES

Application details

* Use for which the certificate is requested -Select an option--
Email (recommended if to be used for electronic signature)

Certificate manager's details

* First name (certificate manager)
* First surname (certificate manager)
Second surname (certificate manager)
* Position
* Tel.
* Type of ID document * Spanish tax ID/foreigner ID card * Passport
* ID Card/Passport number
* Email (certificate manager)

(*) Obligatory field

Cancel Visualize information to sign Continue

Here are some instructions to help users complete this form appropriately.

The section **Applicant Institution's details**:

- If your institution has a tax identification number (NIF, as it is known in Spain), entering the NIF corresponding to the user's institution is recommended. Otherwise, the Business Identifier Code (known as BIC, SWIFT-BIC, SWIFT ID or SWIFT code) for the institution may also be used. In this last case, use the eight-character BIC (the eleven-character BIC is not necessary).
- Enter the user's Corporate Name without using any commas (",").

The section **Application details**:

- The Bank of Spain department with which the user maintains relations will have indicated the use for which the certificate is being requested that must be selected.

If the Sepblac option is selected, please remember that the certificate controller details must coincide with those declared by the institution on form F22 (if any data has changed, it must be communicated to Sepblac before completing the form as, otherwise, the request would be rejected).

- The email address requested in this section will be included on the certificate generated so please remember that if the reason this certificate is being requested is the exchange of information by email with the Bank of Spain (signed or encrypted information or both), this will be the only valid email address for the exchange of such information.

The section **Certificate manager's details**:

- Enter the personal details for the person who will be considered the certificate controller. Preferably, if possible, use the NIF as the identity document type.
- The email address in this section will be the email address where all notifications concerning the expiry, renewal, cancellation and other events in the certificate request lifetime as well as the certificate itself will be sent.

All fields are mandatory except the Email field under the Application details section.

Before registering the request, the data included in the different fields will be checked to see if they are correct.

Only alphanumeric characters can be entered in the text fields and all unnecessary blank spaces will be deleted. To this end, the set of acceptable characters is limited to the following:

- Alphanumeric (A-Z, a-z, 0-9), including (ñÑ).
- Hyphens (-).
- Apostrophes (').

The “Visualize information to sign” displays the request data and allows the user to download the XML file of the certificate request. In this regard, the user can view the data to be signed before doing so:

* Email (certificate manager) (*) Obligatory field

Cancel Visualize information to sign Continue

© 2019 Banco de España, Madrid, Banco de España. All rights reserved. Contact: User Support Center Telephone: + 0034 91 338 6666

80399794M.xml 80399794M.p12 Mostrar todo X

The XML will have the following format:

```
80399794M: Bloc de notas
Archivo Edición Formato Ver Ayuda
<?xml version="1.0" encoding="UTF-8"?><FORMULARIO>
  <INFORMACION_ENTIDAD>
    <NOMBRE>PRUEBA TRES</NOMBRE>
    <CIF>80399794M</CIF>
    <CODIGO_BE>
    </CODIGO_BE>
  </INFORMACION_ENTIDAD>
  <INFORMACION_SOLICITANTE>
    <NOMBRE>JUAN</NOMBRE>
    <PRIMER_APELLIDO>PEREZ</PRIMER_APELLIDO>
    <SEGUNDO_APELLIDO>
    </SEGUNDO_APELLIDO>
    <E_MAIL>juan@juan.com</E_MAIL>
    <CARGO>GERENTE</CARGO>
    <TIPODOCID>NIF_NIE</TIPODOCID>
    <DOCID>71234566R</DOCID>
  </INFORMACION_SOLICITANTE>
  <INFORMACION_ADICIONAL>
    <NUMERO_PETICION>
    <EMAIL_CERTIFICADO>
    </EMAIL_CERTIFICADO>
  </INFORMACION_ADICIONAL>
  <LOCALIZACION_FECHA>
    <LOCALIZATION>
    </LOCALIZATION>
    <FECHA>
      <DIA>5</DIA>
      <MES>11</MES>
      <ANYO>2019</ANYO>
    </FECHA>
    </LOCALIZACION_FECHA>
  <ACEPTACION_CONDICIONES>
</FORMULARIO>
```

Once the required fields have been filled, press the “Continue” button to continue the process. The following page will be displayed:

Confirmation of registration and signing of application.

Applicant Institution's detail	
NIF(tax ID number)/BIC	80399794M
Corporate name	PRUEBA TRES

Application details	
Use for which the certificate is requested	Inspection-secure mail
Email	

Certificate manager's details	
First name (certificate manager)	PEREZ , JUAN
Position	GERENTE
Tel.	911111111
Type of ID document	Spanish tax ID/foreigner ID card
ID Card/Passport number	71234566R
Email (certificate manager)	juan@juan.com

The “Back” button returns to the previous page, allowing the user to modify the values of the fields. If everything is correct, press “Sign” so that the application is registered. This process may take a few seconds:

Confirmation of registration and signing of application.

The certificate application has been successfully registered.
 Press "Start download" to continue the process.

Applicant Institution's detail	
NIF(tax ID number)/BIC	80399794M
Corporate name	PRUEBA TRES

Application details	
Use for which the certificate is requested	Inspection-secure mail
Email	

Certificate manager's details	
First name (certificate manager)	PEREZ , JUAN
Position	GERENTE
Tel.	911111111
Type of ID document	Spanish tax ID/foreigner ID card
ID Card/Passport number	71234566R
Email (certificate manager)	juan@juan.com

If, despite having correctly installed the signature component and configured the browser options according to the instructions in section 2.2.3 of this manual, you could not complete the signature, it is possible that some security software installed on your computer (typically a local antivirus or firewall) is preventing it. Please verify this circumstance and, if necessary, **temporarily** disable this software in order to perform the desired operation and then enable it again.

The request has been left in the “DOWNLOAD PENDING” state and can be processed by pressing the “Start download” button, which starts the generation of the certificate and its possible download, as described in the following section.

3.4.3 Downloading a certificate

By pressing the “Start download” button, the following screen is accessed:

Download the certificate

IMPORTANT: Save the certificate PIN in a safe place.

- Your PIN must be a combination of upper and lower case letters, numbers and special characters(these are : @ % + / ' ! # \$ ^ ? . () { } [] ~ ` - _)
- It must have between 15 and 25 characters

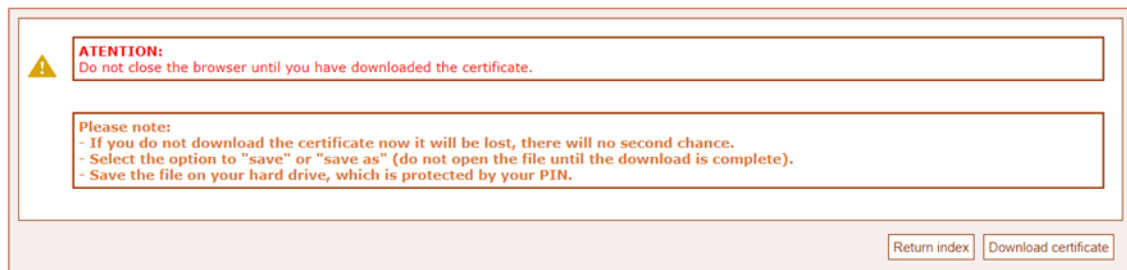
Set the certificate PIN:

* Certificate PIN

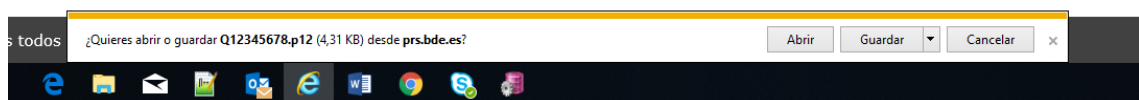
* Certificate PIN confirmation

(*) Obligatory field

Enter your PIN and **make sure you don't lose it** as this is the password protecting the file with the certificate once downloaded. The Bank of Spain does not save this PIN meaning the user will be the only person who knows it.



Then, click on the button "Download certificate" to get the file with the certificate ready for installation. The browser will display several options just as shown in the screenshot below:



It is **VERY IMPORTANT to select the option Save** as this is the only way the certificate will be available and can be installed on future devices requiring it. This will be **the only opportunity** to download the certificate.

Once the user has arrived at the webpage informing that the certificate was correctly issued, the request will move to FINISHED status. This means the process will **NOT** be repeated.

3.5 Manage your institution's certificate

This option displays the entity's certificates, indicating its serial number, status, date of issue, and expiration date.

Certificate list

Institution detail Applications Certificates			
Serial number	State	Date of issue	Expiration date
39551365a2b62abc5dc13d32b3438e11	ACTIVE	05/11/2019 10:12:22	05/11/2023 10:12:22
382ca56f5afffa315dbff51389741d2f	ACTIVE	04/11/2019 10:52:23	04/11/2023 10:52:23
4938f8f4d069e0015db29289171a9bad	ACTIVE	25/10/2019 08:12:29	25/10/2023 08:12:29

Back

The certificates are sorted by Date of Issue, in descending order (from most recent to oldest). The order placement can be reversed, as in the list of requests, by clicking on the column header. Similarly, the list can be sorted by expiration date or alphabetically by state.

The possible states of any certificate are:

- **ACTIVE:** The certificate is in force.
- **REVOKED:** The certificate has been invalidated and it is no longer possible to use it.
- **RENEWED:** The certificate has been renewed. It remains in force, and remains valid until its expiration date, but a new certificate has been generated in order to replace this one.
- **EXPIRED:** The expiration date of the certificate has been exceeded, so it is no longer possible to use it.

By clicking on the “Serial number” field of each record, the user can access the certificate detail, with its different options detailed in the following section.

3.5.1 Details of the certificate

Through the “Serial number” in the list of certificates, the data of the certificate consulted can be accessed:

Detail of the certificate

Certificate information	
Certificate CN	CN=[80] 80399794H RI-C365A 0004
Type	ENTIDAD EXTERNA PKCS12 (Nivel de confianza 3)
Valid from	05/11/2019 10:12:22
Valid to	05/11/2023 10:12:22
State	ACTIVE
Serial number	39551365a2b62abc5dc13d32b3438e11
Certificate type	Certificate for external institution of BDE

Applicant institution's details	
NIF(tax ID number)/BIC	80399794H
Corporate name	PRUEBA TRES
Email	
Use for which the certificate is requested	Inspection-secure mail
Name (certificate manager)	PEREZ , JUAN
Type of ID document	Spanish tax ID/foreigner ID card
ID card/Passport number	960233098
Tel.	543223344
Email (certificate manager)	Juan@juan.com

[Certificate list](#) [Renew Certificate](#) [Revoke Certificate](#) [Show certificate](#)


From this webpage, the user can “Show certificate”, an option that allows the download of the certificate already issued.


For certificates in RENEWED or ACTIVE status, the option to revoke or renew it is offered, which are explained in the following sections, [3.5.2 Revoke a certificate](#) and [3.5.3 Renewing a certificate](#).

3.5.2 Revoking a certificate

From the view of a certificate in RENEWED or ACTIVE status, by pressing “Revoke Certificate”, this screen can be accessed:

Revoke certificate

 **IMPORTANT:** This is an irreversible process. Be sure before continuing.

Data of the requesting entity	
NIF(tax ID number)/BIC	80399794M
Corporate name	PRUEBA TRES
Detail of the certificate	
Serial Number	39551365a2b62abc5dc13d32b3438e11
Date of issue	05/11/2019 10:12:22
Expiration date	05/11/2023 10:12:22
State	ACTIVE
Data of the revocation	
* Revocation Reason 	<div><input checked="" type="radio"/> UNSPECIFIED <input type="radio"/> AFFILIATION CHANGED <input type="radio"/> KEY COMPROMISE <input type="radio"/> CESSATION OF OPERATION <input type="radio"/> PRIVILEGE WITHDRAWN</div>

(*) Obligatory field

Cancel Accept

Where the certificate data is displayed, together with the warning of the **irreversibility of this action**.

The user can select one of the following causes of revocation:

- **AFFILIATION CHANGED:** Any information in the certificate has been changed, but there is no reason to believe that the private key is compromised.
- **KEY COMPROMISE:** The private key has been compromised.
- **CESSATION OF OPERATION:** The certificate is no longer necessary for the purpose for which it was issued and there is no suspicion that the private key is compromised.
- **PRIVILEGE WITHDRAWN:** Some privilege included in the certificate has been withdrawn.

If none of the reasons fit the reason for rejection, **UNSPECIFIED** will be selected.

Once the reason is selected, after pressing “Accept”, the certificate is thus revoked.

3.5.3 Renewing a certificate

A certificate in RENEWED or ACTIVE status can be renewed if it is within the renewal period; which is 30 days from the expiration date. The user will receive by email the notice stating that the certificate is about to expire. From that moment, the certificate can be renewed.

To do so, in the details of the certificate, by pressing “Renew Certificate”, the user can access a form with the same characteristics as those of the request record [3.4.2 Record of certificate request](#), except that the “Use for which the certificate is requested” field is not editable:

Request for the certificate renewal

Applicant institution's detail	
* NIF(tax ID number)/BIC	80399794H
* Corporate name	PRUEBA TRES
Application details.	
* Use for which the certificate is requested	Inspection-secure mail
Email	
Certificate manager's details	
* First name (certificate manager)	JUAN
* First surname (certificate manager)	PEREZ
* Second surname (certificate manager)	
* Charge (certificate manager)	GERENTE
* Tel.	611223344
* Type of ID document	<input checked="" type="radio"/> Spanish tax ID/foreigner ID card <input type="radio"/> Passport
* ID card/Passport number	96023309B
* Email (certificate manager)	juan@juan.com

(*) obligatory field

Clicking on “Sign” generates a new request. Once processed, as shown in section [Downloading a certificate 3.4.3](#), a new certificate is obtained with the same characteristics as the original, but with its issuance date equal to that of the day on which the renewal is carried out and a new extended expiration date.

The certificate is RENEWED.

4 Error and warning messages

The error or warning messages that may appear while using this application are explained below.

4.1 System Error

If there were some type of isolated technical problem, the following message would be shown:



Please try again after a few minutes. If the problem persists, call the phone number shown.

4.2 Application under maintenance

Access may be temporarily unavailable due to application maintenance tasks. The following screen will appear in such circumstance:



Please try again after a few minutes.

4.3 Messages on home page


If you try to access the application with an invalid certificate, a message will be displayed indicating the authentication error:

 The digital certificate that you have used to identify yourself is not allowed to access this application. Please, use an external component certificate of PKIXDIE or legal entity recognized by the Banco de España.

4.4 Messages while downloading the certificate

If the certificate PIN entered or confirmed upon downloading a certificate is not in the appropriate format or they do not coincide, an error message will be displayed at the top of the screen:

Download the certificate

 **IMPORTANT:** Save the certificate PIN in a safe place.

- Your PIN must be a combination of upper and lower case letters, numbers and special characters(these are : @ % + / ' ! # \$ ^ ? . () { } [] ~ ' - _)
- It must have between 15 and 25 characters

Set the certificate PIN:

* Certificate PIN

* Certificate PIN confirmation


(*) Obligatory field

Cancel Accept

4.5 Messages in the record of a request

Either by pressing the “Continue” or “Visualize information to sign”, the fields are validated. In the event of missing a mandatory field or if any other one had an erroneous format, descriptive error messages would be displayed:

Registration of application for certificate

 Use of certificate requested
First name of certificate manager required.
First surname of certificate manager required
Position of certificate manager required
Tel. required
Managers ID document required
Email of certificate manager required

Applicant Institution's details

NIF(tax ID number)/BIC
Corporate name

Application details

* Use for which the certificate is requested
Email (recommended if to be used for electronic signature)

Certificate manager's details

* First name (certificate manager)
* First surname (certificate manager)
Second surname (certificate manager)
* Position
* Tel.
* Type of ID document ☒ Spanish tax ID/foreigner ID card ☐ Passport
* ID Card/Passport number
* Email (certificate manager)

(*) Obligatory field

Cancel Visualize information to sign Continue

There are a maximum number of certificates per user entity. If this value has been reached and an attempt is made to request a new certificate, an information message will be displayed by the application indicating that is not possible to request more certificates.



4.6 Messages during the signing of the request

In the case of operating with Chrome or Firefox browsers, if the signature was not installed correctly as indicated in [item 3.1.1](#), the application will show the following error when signing a request:



It is possible that the signature component was installed correctly, but it was not added to the browser and the connection between them is not possible. In that case, the following error will be displayed:



If the certificate to be used to sign is not valid, the following message will be displayed after pressing the signature button:



4.7 Messages in the renewal of a certificate

When the user presses the renewal button of a certificate, if it is not in the renewal period, the following message will display:



Allowing to return to the list of certificates by pressing the button.