BANCO DE ESPAÑA
Eurosistema

INFORMATION TECHNOLOGY COMMITTEE

ESCB-PKI PROJECT

ADMIN GUIDE:

SMARTCARD MANAGEMENT BROWSER CONFIGURATION

VERSION 1.1

ECB-RESTRICTED
06-Feb-2024

TABLE OF CONTENTS

Project name:	ESCB-PKI
Author:	ESCB-PKI team
File name:	Smartcard management browser configuration
Version:	1.1
Date of issue:	06.02.2024
Status:	First version
Approved by:	
Distribution:	

RELEASE NOTES

In order to follow the current status of this document, the following matrix is provided. The numbers mentioned in the column "Release number" refer to the current version of the document.

Release number	Status	Date of issue	Revisions
1.0	Final	11.11.2021	Initial version.
1.1	Final	06.02.2024	Updated http links to ESCB-PKI website to https

1. INTRODUCTION

ESCB-PKI advanced certificates are stored into a secure signature creation device, such as a smartcard or token device.

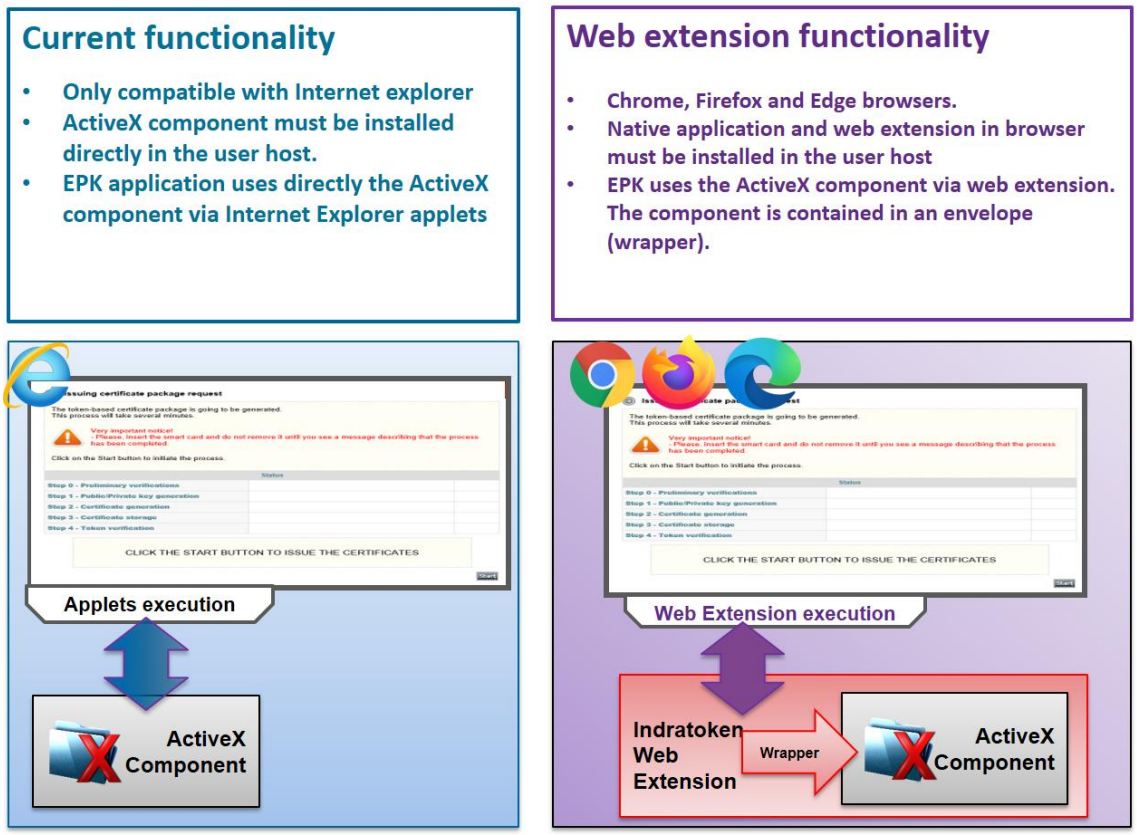
For the ESCB-PKI to be able to install certificates into your device, you need to install the software below, available at https://pki.escb.eu/epkweb/en/support.html:

- ESCB-PKI Smartcard drivers
- Native application required to manage certificates in a smart card, which enables your Microsoft Windows
- One of the following web extensions of your choice, according to your browser preferences:
    - Mozilla Firefox ESCB-PKI Certificate Enrollment extension.
    - Chrome and Edge ESCB-PKI Certificate Enrollment extension.

This document will explain to System Administrators how to deploy the aforementioned software in an organisation.

2. SOLUTION DESIGN

The aim of the new solution is to replace the current ActiveX component and the limitation usage of being compatible only with Internet Explorer browser.



The Wrapper in the picture below represents the native application, which communicates with the web extensions installed in the selected browser.

3. NATIVE APPLICATION INSTALL

The native application is available to download at:

https://pki.escb.eu/epkweb/files/EPKuserCertEnrollment-setup-win.exe

To deploy the native application in other computers, it would be necessary to run the installation program in silent mode. The proper way to do it is by just executing it with the following parameters:

- **/S**: program installation in silent mode. This method will install the native application for both Chrome and Firefox browsers.

- **/D=<install_path>**: it indicates the desired install path. By default, without defining this parameter, the native application will be installed in C:\Program Files (x86).

4. WEB EXTENSION INSTALL

Web extensions are addons or extensions to browsers. As such, the installation process is mostly dependant on the browser where it will be installed and therefore the install instructions may differ.

The following browsers have been thoroughly tested and are therefore recommended:

- Internet Explorer 11
- Google Chrome 94
- Mozilla Firefox 92
- Microsoft Edge 95

Higher versions should also work properly, but as newer versions are updated more and more often, it may happen some adjustment is required to maintain compatibility. In case your preferred browser is one of the above and does not work properly, do not hesitate reporting an incident to the ESCB-PKI service. If this happens, while the incident is solved, it is recommended using a different browser.

Below is described the procedure to install the web extension for any of the aforementioned browsers:

INTERNET EXPLORER 11

No web extension is needed for this browser. It is enough if you have installed the Native application as it is described in the previous chapter. The previous ActiveX component is included in the native application, so older configuration than this one will still work properly.

GOOGLE CHROME

Web extensions may be distributed to Google Chrome without the user intervention. There are different options to get this goal, but all of them involve making use of the Google Chrome extensionsettings registry key, located at **{USER_SID}\Software\Policies\Google\Chrome\ExtensionSettings**.

For more information about extension settings parameters: https://cloud.google.com/docs/chrome-enterprise/policies/?policy=ExtensionSettings.

In case your computer is managed by your organisation, it is possible to deploy the extensionsettings configuration via Group Policy Object (GPO).

Some configuration examples would be the following, where pnaapcaggocnllecimkopedaacemikbb is the ESCB-PKI Google Chrome extension identifier:

- Installation allowed for all users included in the GPO (but no silent installation):

```
{
  "pnaapcaggocnllecimkopedaacemikbb": {
    "installation_mode": "allowed"
  }
}
```

- Silent installation for all users included in the GPO:

```
{
  "pnaapcaggocnllecimkopedaacemikbb": {
    "update_url": "https://clients2.google.com/service/update2/crx",
    "installation_mode": "force_installed"
```

```
    }
}
```

MICROSOFT EDGE

In case your computer is managed by your organisation, as the Microsoft Edge version includes the chromium engine, the same procedure as in the previous chapter must be followed as described in the distributed installation in Google Chrome browser via GPO.