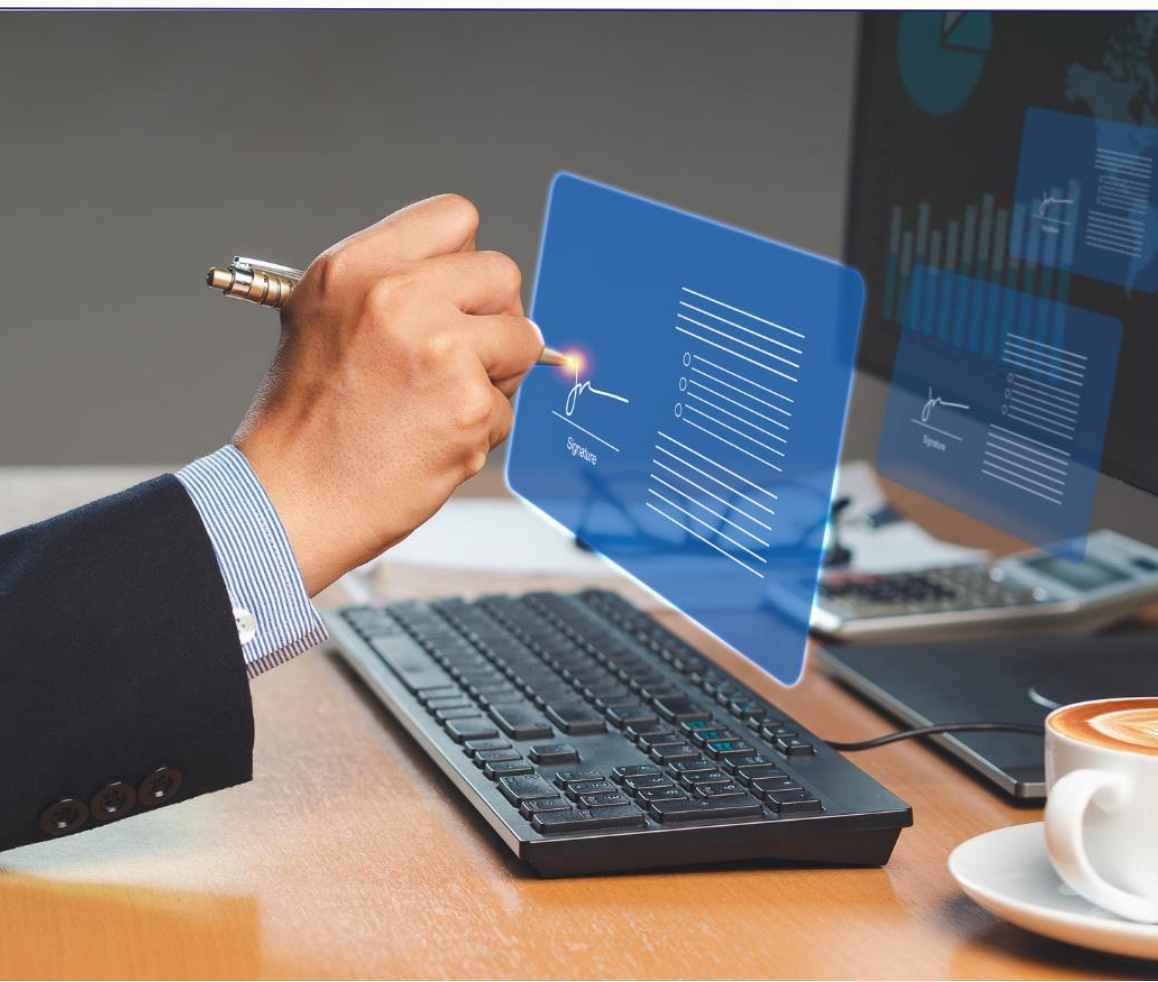# User
MANNUAL

DIGITAL SIGNING OF DOCUMENTS

PUBLIC PROCUREMENT BUREAU

DIGITAL SIGNING OF DOCUMENTS

This guide is intended for all economic operators participating in public procurement procedures as bidders, to familiarize themselves with the new method of signing documents within the bid.

With the latest upgrades to the e-GP system, the digital signing process will be automated and carried out directly within the system. When submitting a bid:
- Documents must be uploaded in **.PDF format**
- The **financial offer** must be completed directly in the "Submit Bid" module
- After finalizing the bid, the system will automatically apply the **digital signature** (manual signing via an external application will no longer be possible)

Note: There is no need for documents to be signed prior to uploading – the system will apply the digital signature automatically. Mandatory use starting from **April 1, 2025**.

Note: The digital signing tool has already been implemented in the e-GP system for some time, but starting from **April 1, 2025**, its use will become **mandatory** for signing bids.

Therefore, we recommend that you prepare in advance and submit your bids at least a few days before the start of the Public Opening, in order to avoid potential last-minute issues.

Step 1: Obtain a Digital Certificate

In the Republic of North Macedonia, there are two official and certified issuers of digital certificates:

- **KIBS** (https://www.kibstrust.com/)

- **Macedonian Telekom** (http://www.t-home.mk/mk/374/IKT_uslugi/Digitalni_sertifikati.html)

Their operations are regulated by the **Ministry of Digital Transformation**. Both certificate issuers provide different types of certificates for **natural persons** and **legal entities**.

For foreign economic operators, it is required to obtain a **Qualified Electronic Signature (QES)** that complies with the legal framework of the European Union, specifically Regulation (EU) No 910/2014 (eIDAS Regulation) on electronic identification and trust services for electronic transactions in the internal market.

The signing process is enabled only with qualified digital certificates issued on USB tokens or SMART cards by any Qualified Trust Service Provider (QTSP).

For more information on how to obtain a certificate, please contact the registered issuers directly.

Step 2: Install the Digital Certificate

Upon receiving the digital certificate, you will also receive instructions from the certificate issuer on how to install it on your computer or how to store and use it via another electronic medium (e.g., CD, token, smart card).

Note: To ensure the digital signature works correctly in the system, it must be properly installed on the user's computer. Please make sure to check the following:

1. **Check if the certificate contains the private key -** A digital signature consists of a certificate and a private key. The private key is required to sign documents. If the certificate is installed without the private key, signing will not be possible.

How to check:
* Open **Manage User Certificates (certmgr.msc)**
* Go to **Personal → Certificates**
* Locate your certificate and double-click to open it
* In the **General** tab, verify that it says: *"You have a private key that corresponds to this certificate."*

If this message is not present, the certificate does not contain a private key and cannot be used for digital signing. In that case, the certificate is not correctly installed (only the public part is installed).

2. **Check if the certificate is installed in the correct folder**
   The certificate must be installed in: **Personal (Certificates – Current User)**

If the certificate is installed in **Trusted Root Certification Authorities** or another folder, it cannot be used for digital signing. The **Trusted Root** folder is intended for trusted certificate authorities, not for personal signing certificates.

Step 3: Electronically Sign the Documents You Upload to the e-GP System

Currently, there are two methods for digital signing:

1. **Digital signing directly within the application**
2. **Digital signing via an external software application**

Note: Digital signing directly within the application is currently available only for economic operators in the bid submission module. Starting from **April 1, 2025**, this method of signing will become **mandatory**.

3.1 Digital Signing Directly Within the Application

Digital signing at the application level means that economic operators upload their documents in **.PDF format** into the appropriate fields within the **"Submit Bid"** module of the e-GP system. After uploading, with a single click on the **"Sign Documents"** button, the digital signature is applied to all documents at once.

Before starting the digital signing process, the following prerequisites must be fulfilled:

- **Download the PDF extension for digital signing**
- **Install the client application for signing**

Note: Depending on your company's IT policies, you may need to request permission to install these programs. This should be done in advance to avoid missing the deadline for submitting your bid.

3.1.1 Download the PDF Extension for Digital Signing

The PDF extension for digital signing is supported on the following operating systems: **Windows XP, 7, 8, 8.1, and 10.** Compatible web browsers include: **Google Chrome, Opera, Mozilla Firefox, and Microsoft Edge.**

To download the appropriate PDF extension, you must first log in as an economic operator and click the "**Sign PDF download**" button located in the upper right corner of the screen. After clicking the button, a new browser tab will open where you can install/add the extension.
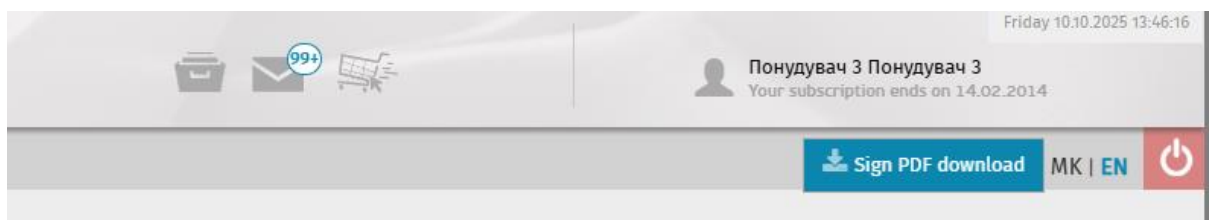

1 **Google Chrome**

After clicking the button, a new browser tab will open. Click on the **"Add to Chrome"** button, which will open a confirmation window. Then click **"Add extension"** to complete the installation process.
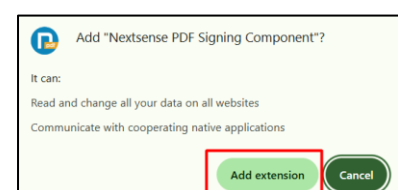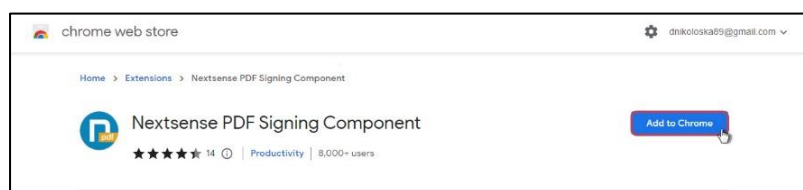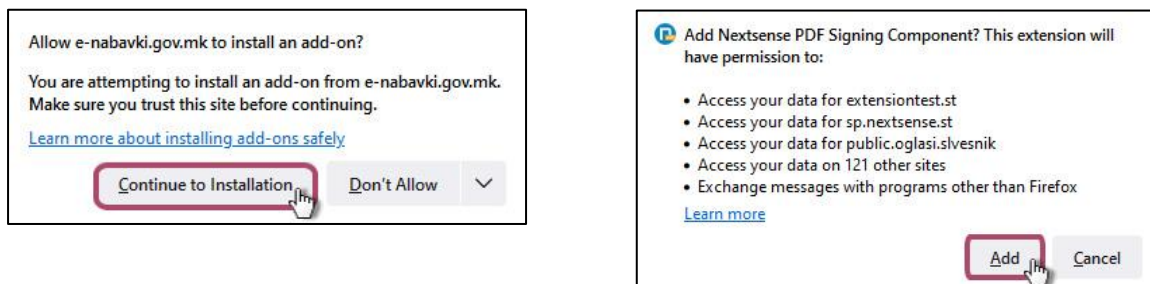
Note: If the **"Download the PDF Signing Extension"** button remains visible after installation, you may need to adjust the extension settings in Chrome. Go to the extension settings and select **"On all sites"** to enable proper functionality.
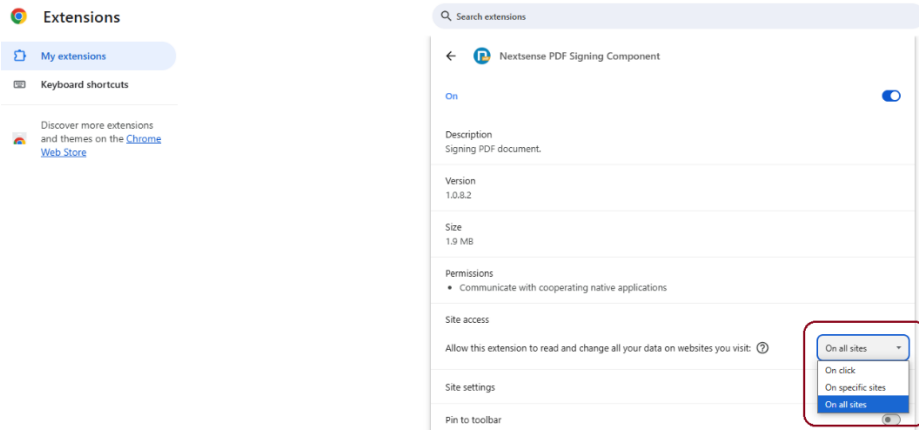

② **Mozilla Firefox**

If prompted, click **"Continue to Installation"**, then confirm by clicking **"Add"** in the pop-up window. This completes the extension installation process.

Note: If the **"Download the PDF Signing Extension"** button remains visible after installation, you may need to adjust the extension settings in **Mozilla Firefox**. Select **"Always Allow on e-nabavki.gov.mk"** to ensure proper functionality.
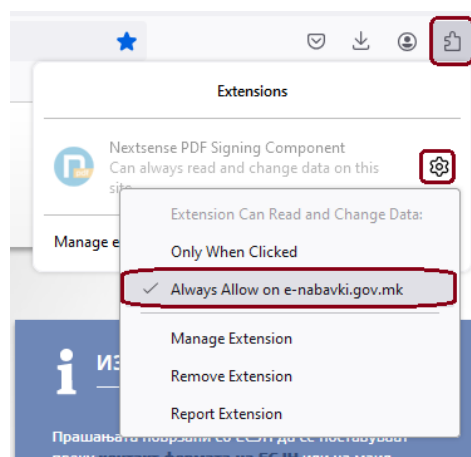
3 **Microsoft Edge**

Click on the **"Get"** button, which will open a confirmation window. Then click **"Add extension"** to complete the installation process.
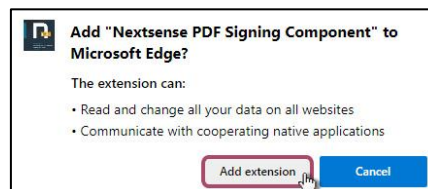
Note: If the **"Download the PDF Signing Extension"** button remains visible after installation, you may need to adjust the extension settings in **Edge**. Select **"This can read and change site data"** and choose either **"On e-nabavki.gov.mk"** or **"On all sites"**.
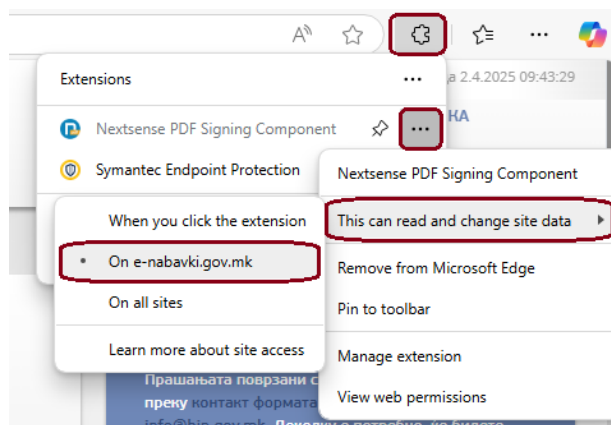

4 **Opera**

Click on the **"Add to Opera"** button to begin the extension installation. You will be automatically redirected to the page for downloading and installing the client signing application.
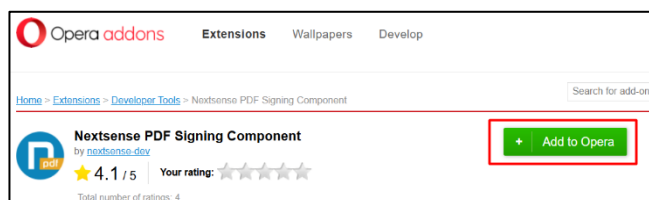
Note: If the **"Download the PDF Signing Extension"** button remains visible after installation, you may need to adjust the extension settings in **Opera**. Select **"Page access"** and choose either **"Always run on e-nabavki.gov.mk"** or **"Always run on all sites"**.
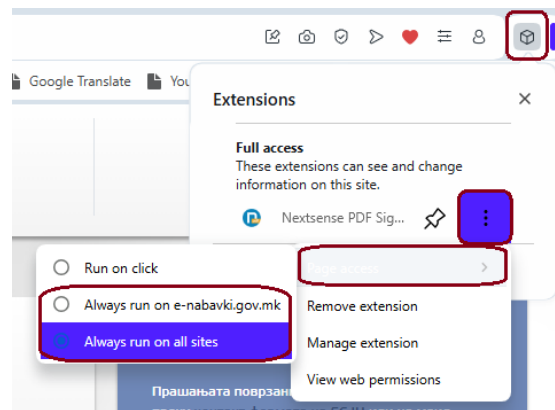
Note: It is recommended to always use the latest available version of your browser.

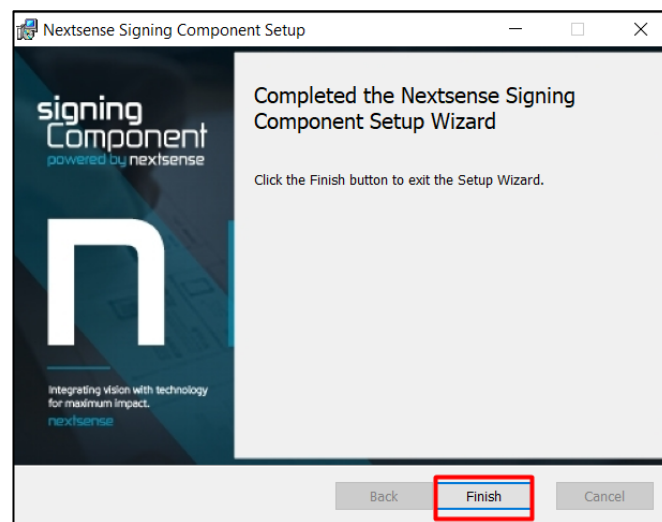## 3.1.2 Installation of the Client Signing Application

After successfully adding the extension, you will be redirected to the page for downloading the client signing application. Click on the **"Download"** button to download the installation file to your computer.
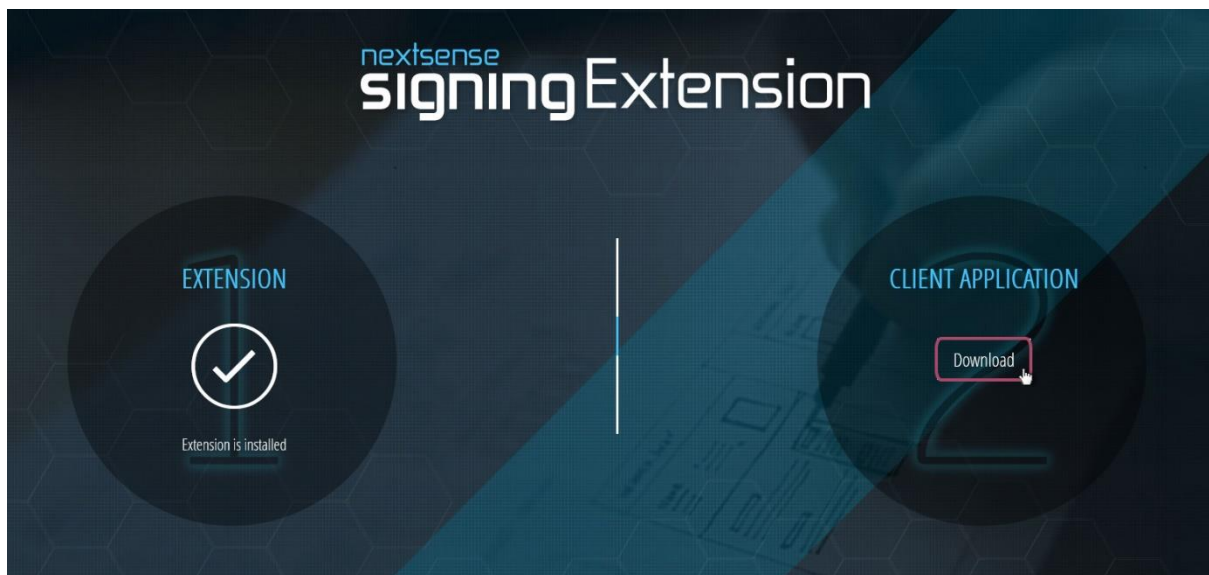
Once downloaded, start the **.msi** file by double-clicking it. A window will appear where you need to check the box **"I accept the terms in the License Agreement"**, after which the **"Install"** button will become available.
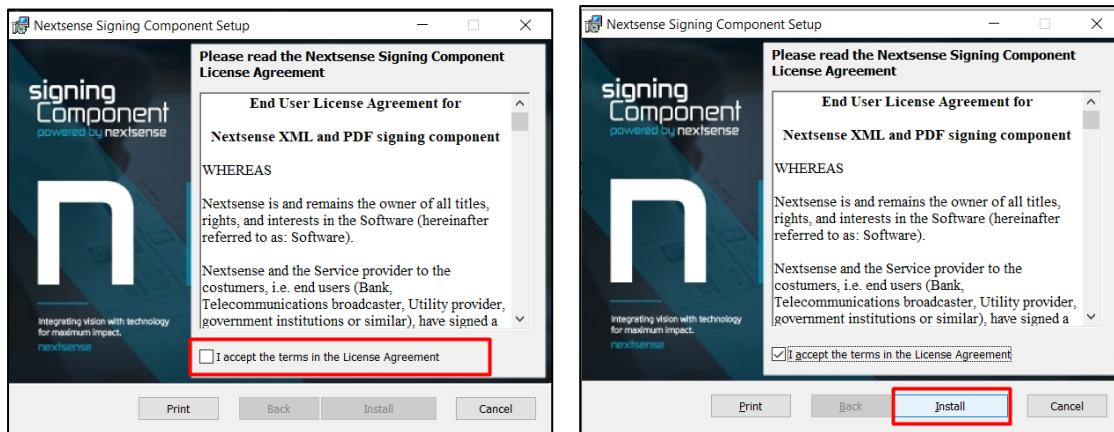
After successful installation, a new window will appear where you need to click the **"Finish"** button.

To verify that the extension and the client signing application have been successfully installed, follow these steps:

1. Completely close your browser (click the **X** in the top-right corner of the window)
2. Reopen your browser
3. In the URL field, enter the following address:

https://signingextension.nextsense.com/ExtensionVerify.html?typeExtension=pdf

If everything is correctly and successfully installed, the page should display messages as shown in the image below (installed extension (1) and installed client application (2)).

This confirms that your computer is ready to begin the document signing process.

3.1.3 Digital Signing of Bid Documents

Before you begin creating your bid and uploading the PDF documents for signing, you must ensure that your valid signing certificate is properly installed (under **User Certificates**), or, if your certificate is stored on a token, that the token is connected to your device.

When creating the bid, documents are uploaded using the **"Upload Document"** button. Once all bid documents are uploaded, those subject to signing will be digitally signed and marked accordingly.

After clicking the **"Sign Documents"** button, a window titled **"Choose certificate to sign files"** will appear. Click on the arrow to select the certificate you want to use for signing.

Choose certificate to sign files

Certificate name	Certificate issuer	Certificate thumbprint	Certificate valid to date	
Dragana Tasevska	CN=KIBSTrust Issuing Qsig CA G3, OID.2.5.4.97=NTRMK-5529581, OU=KIBSTrust Services, O=KIBS AD Skopje, C=MK	A9B6C5E9A0C9C15F2B82D8BA0CFD680BC6E61E7B	27.02.2026	→

First Previous 1 Next Last

↺ Cancel

After the documents are signed, an icon ✏ will appear next to each document indicating that it has been digitally signed directly within the e-GP application.

| CATEGORY	DOCUMENTS		
ABILITY OF THE ECONOMIC OPERATOR TO PERFORM BUSINESS ACTIVITY			
Document for registered activity	test.pdf		
OFFER DOCUMENTS			
Serious statement	Изјава за сериозност.pdf	✏	
Authorization for submit bid ⓘ	test.pdf	✏	
Technical offer	test.pdf	✏	
Offer form	Образец на понуда.pdf	✏	✖ DELETE FINANCIAL OFFER AND TEMPLATE
Financial offer	Финансиска понуда.pdf	✏	

✏ ➕ ⓘ

Note: Only certificates with a valid expiration date will appear in the list.

Note: For domestic economic operators, the certificate issuer must be validated (issued by **KIBS** or **Macedonian Telekom**), and the certificate must be a **professional certificate**. The **tax number** of the company registered in the e-GP system must match the tax number listed in the **Subject** field of the certificate. For **foreign economic operators**, there are **no additional checks** on the digital certificate regarding the issuer.

Note: If you are using a **token** for signing, that certificate can only be used on the device where the token is physically connected.

Note: Check the taskbar to see if a window appears that is blinking and needs to be clicked to enter the PIN. Entering the PIN may be required for each document individually if the certificate is on a token or if security settings were applied during the certificate installation.

Note: If documents need to be signed by **two or more authorized persons** (linked signatures), after the initial signing, an icon ✏ ➕ will appear that allows **re-signing** of all documents by the next signatory.

Note: Bill of quantities for works – In this field, upload the completed bill of quantities or description of technical items. This document must be digitally signed before being uploaded to the system.

3.1.4 Configuring the Digital Signature

If you want to visually configure your digital signature so that it appears on the document itself, you can do this through the **"Personal Data"** module available in the **"My Profile"** menu. In this section, you can define the following:

➢ **Digital Certificate** – Use the **"Select Digital Certificate"** button to upload the certificate you want to use for signing within your e-GP profile (from all certificates installed on your computer)

➢ **Template Document for Coordinate Setup** – Upload a document that will allow you to define the position of the digital signature

➢ **Signature Image** – Optionally, you can upload an image of your handwritten signature

➢ **"Set Coordinates"** – After uploading the template (used temporarily only for positioning the signature), use this option 📍 to automatically mark the coordinates of the signature„Постави координати".
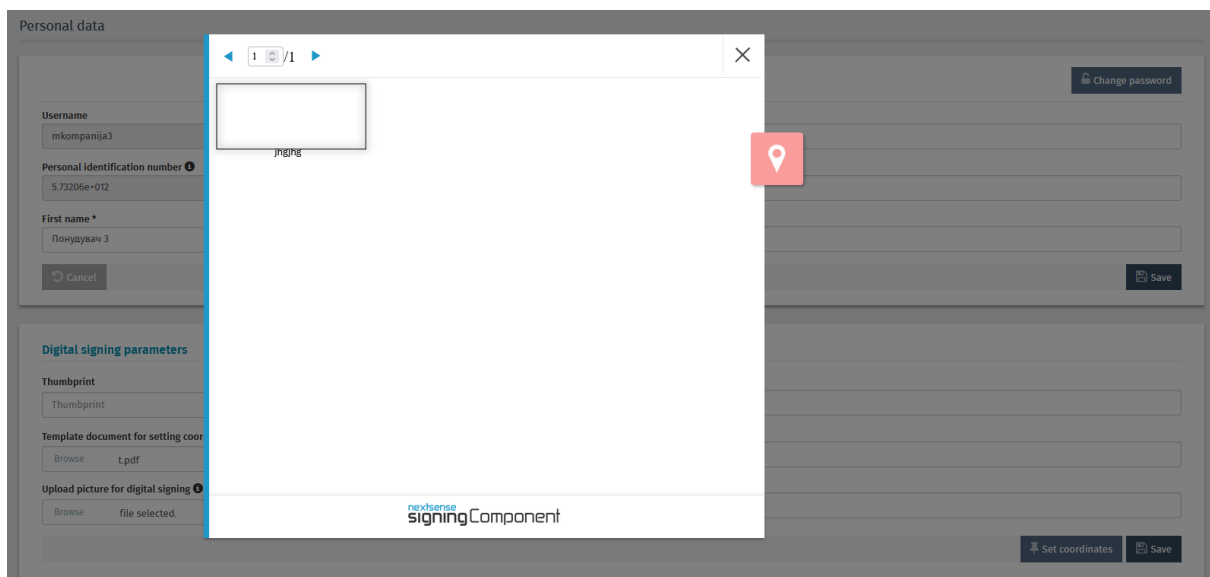
Once this option is selected, three fields will be populated with coordinate "values that can be modified:

● **Page location** where the signature should appear
● **Left coordinate**
● **Top coordinate**

After defining the parameters, click **"Save"** to store them. If needed, all parameters can be deleted by clicking the **"Delete Parameters"** button.

Note: Coordinates can be entered manually, or after selecting a template document, it is necessary to click the "Set Coordinates" button to configure them.

After setting the parameters for digital signing, when signing the documents from the offer template—by clicking the "Sign Offer" button—the selected documents are signed directly. Once the document is opened, the digital signature is visible on the document itself.

Note: Digital signing of documents is valid even without setting the digital signing parameters in the user's personal data. In both cases, the document is digitally signed (the Signature Panel ribbon is visible in the Adobe Acrobat Reader application for viewing PDF documents). By configuring the digital signature parameters, the digital signature on the document becomes additionally visible.
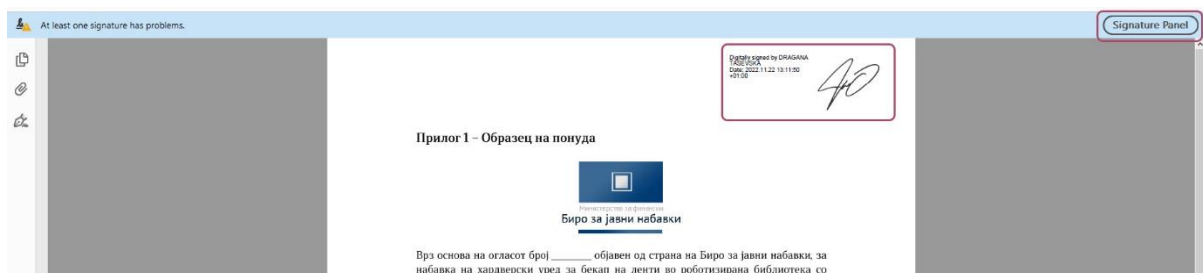
Note: If the message "At least one signature has problems" appears in the documents you signed, this does not mean the documents are invalidly signed. It simply means that the certificate needs to be added to the Trusted Certificates in Adobe. This can be done in a few steps:

1. **Right-click** on the signature in Adobe and click the link **"Validate Signature"**
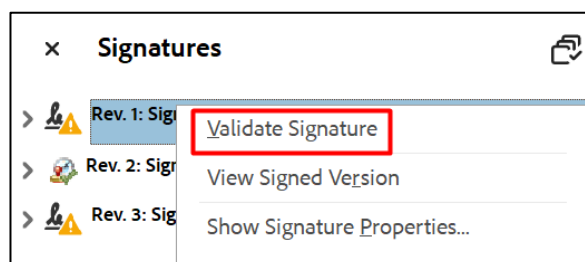
2. A window will appear – **Signature Validation Status**, where you need to click the **"Signature Properties"** button

3. Then, a window will open – **Signature Properties**, where you need to click the **"Show Signer's Certificate…"** button
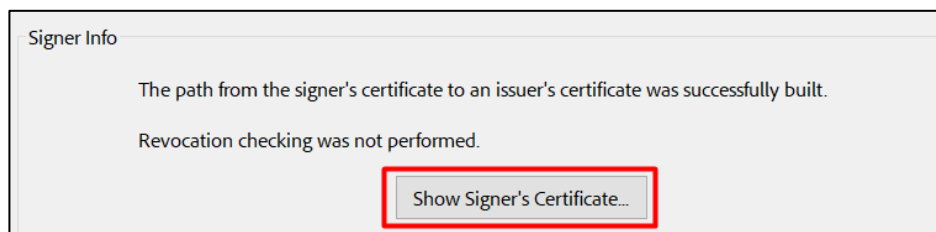
4. In the window – **Certificate Viewer**, click the **"Trust"** tab, then click the **"Add to Trusted Certificates…"** button
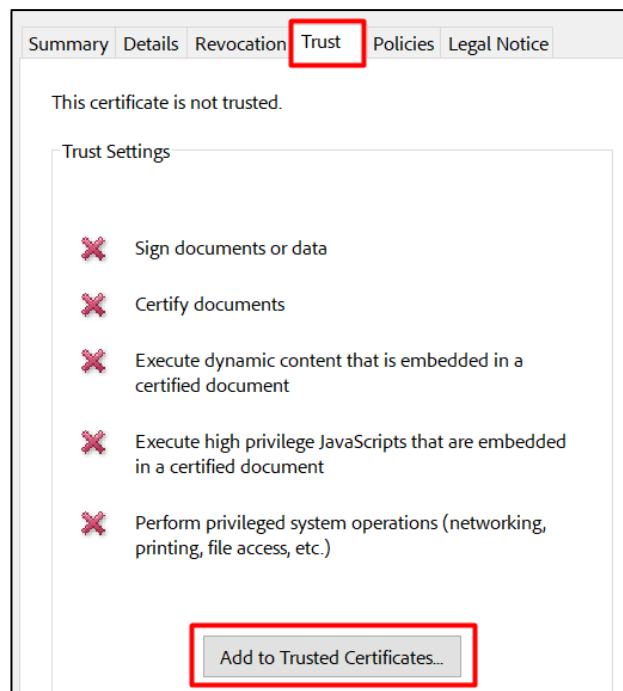
5. the **Acrobat Security** window, click the **"OK"** button

Acrobat Security ✕

⚠ If you change the trust settings, you will need to revalidate any signatures to see the change.

Trusting certificates directly from a document is usually unwise. Are you sure you want to do this?

[OK] [Cancel]

6. Check all the marked checkboxes shown in the image below, then click the **"OK"** button

Trust

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.
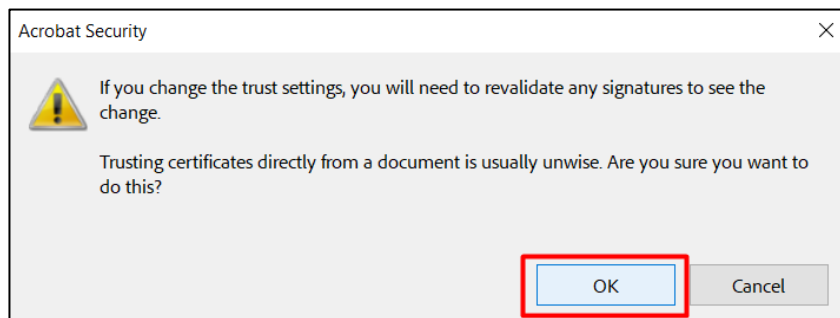
☑ Use this certificate as a trusted root

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.)

[Help] [OK] [Cancel]

7. Once you are returned to the previous window, click the **"OK"** button again

After closing and reopening the document in Adobe Acrobat Reader, the icon changes from yellow to green
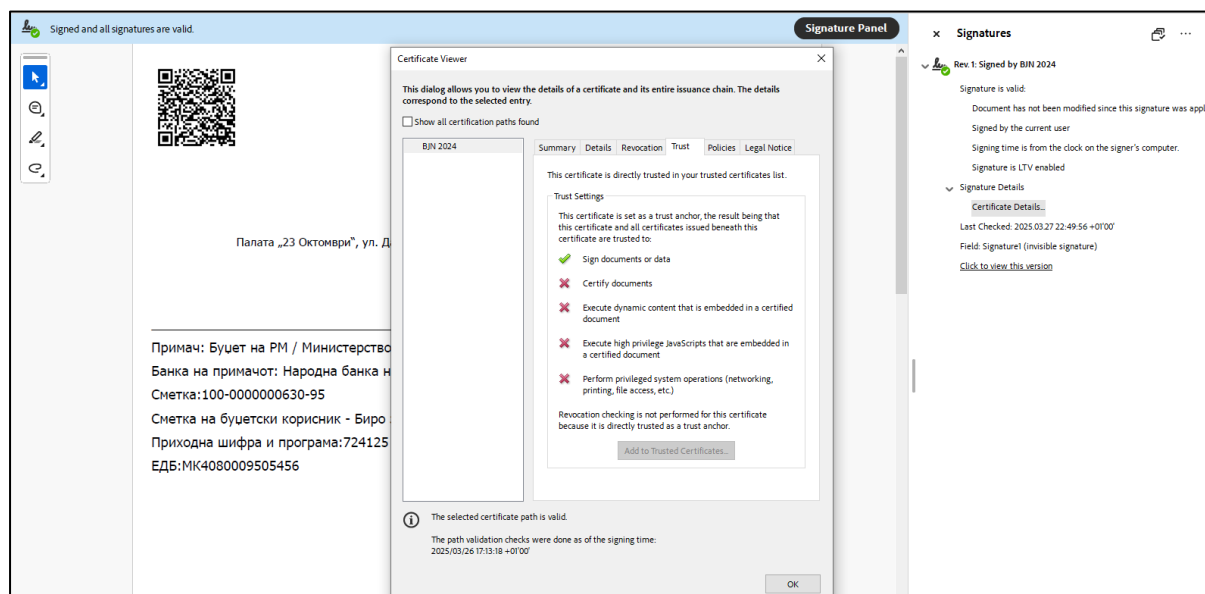
NOTE: For all questions and issues related to digital signing and the signing tool, please report them via the following email address – potpisesjn@bjn.gov.mk

3.2 Digital Signing via Application

Digital signing via an application is used by contracting authorities when it is necessary to upload a digitally signed document.

On the other hand, economic operators digitally sign the documents of their bids at the application level (explained in more detail in Chapter 3.1). However, signing via an application is used in all other cases where it is necessary to submit a digitally signed document through the e-Procurement System (for example, when a document needs to be signed as a response to a question during evaluation or a request to participate, submission of documents to prove eligibility in a simplified open procedure, submission of comments for technical dialogue, bid for a mini-tender, submission of an e-Complaint, and other cases).

3.2.1 Digital Signing via Application

The method of electronically signing documents varies depending on the application being used.

Below is an explanation of the procedure for electronically signing documents using the most commonly used applications.

Note 1: A user signing a document on their computer may have multiple digital signatures installed, issued by a bank, another institution such as the Official Gazette, or a domain certificate within their own institution or company. Care must be taken when signing to ensure that the document is signed with the correct digital certificate. Authorized issuers of digital certificates in North Macedonia are KIBS and Makedonski Telekom. If a certificate is issued by a foreign provider, the issuer must be authorized (registered) in its country of origin as an official digital certificate provider. The Public Procurement Commission reserves the right to request additional proof of the certificate's validity and the issuer's credibility. Any bids signed with an invalid certificate are considered unacceptable.

Attention must also be paid in cases where multiple users' digital signatures (i.e., different names) are installed on the same computer.

Note 2: A document created in any application can be signed with multiple digital certificates. However, please note that if any changes are made to the document between the time one digital certificate is applied and the time another certificate is applied, the previously applied certificate(s) will be invalidated.

Note 3: If you are using a newer version of the MS Office suite (2007 or 2010), the document you want to sign electronically—even if saved in a format compatible with MS Office 97-2003—may not display the attached digital signature to users of MS Office 2003 or earlier versions (or other software suites such as OpenOffice). However, if a document is signed using the Microsoft Office 2003 suite, the digital signature remains visible when the document is opened in Microsoft Office 2007/2010.

Microsoft Office 2007

If you are using Microsoft Office 2007, the signing procedure is carried out as follows:

Note 1: The procedure for applying a digital certificate to any MS Office 2007 document (Word, Excel, PowerPoint) is identical.

Open the document you want to sign electronically. Click the **Office Button** located in the upper left corner of the screen, then select **Prepare** and choose **Add a Digital Signature**.
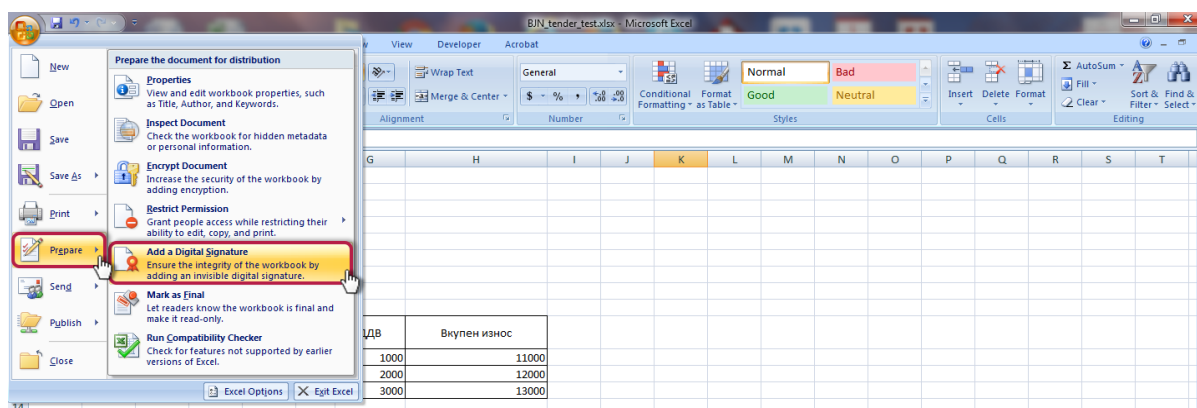

A blank field will appear on the screen, where you can enter the purpose of signing the document (for example, "Signing a bid"), and then be sure to click the **Sign** button.
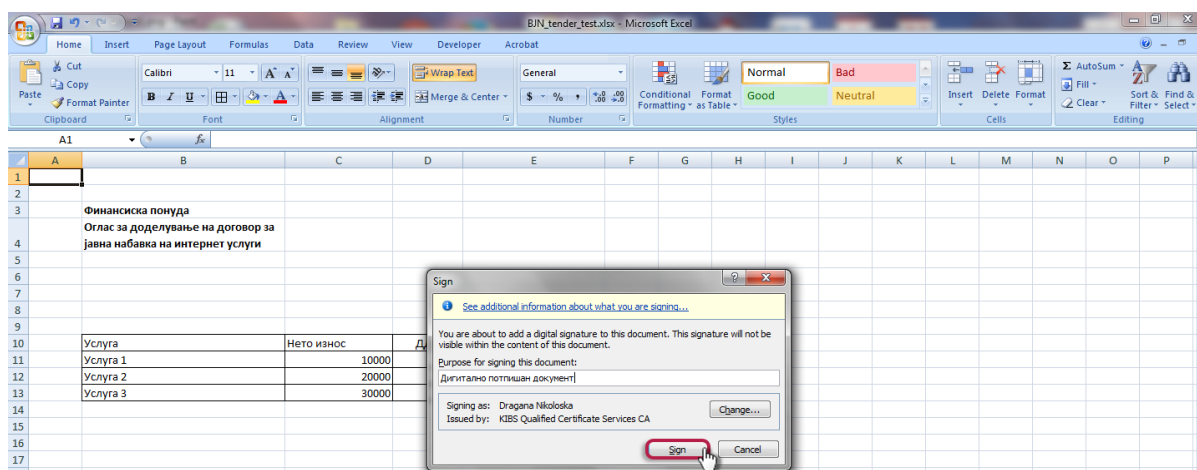
After clicking the **Sign** button, a screen will appear with a blank field where you enter the password for your digital certificate and click **OK**. During the installation of the digital signature (certificate), there is an option to require a password each time you sign. If this option was not selected, no password will be requested when signing the document.
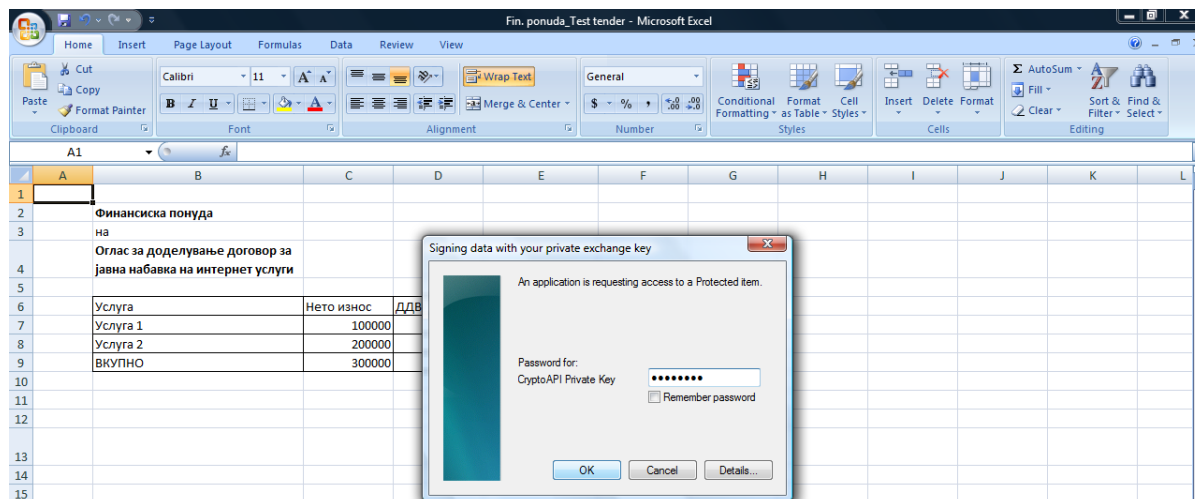
After clicking **OK**, a red icon (ribbon) will appear at the bottom of the document (in the Task Bar), indicating that your document has been successfully signed and is ready to be uploaded to the e-Procurement System (ePPS).
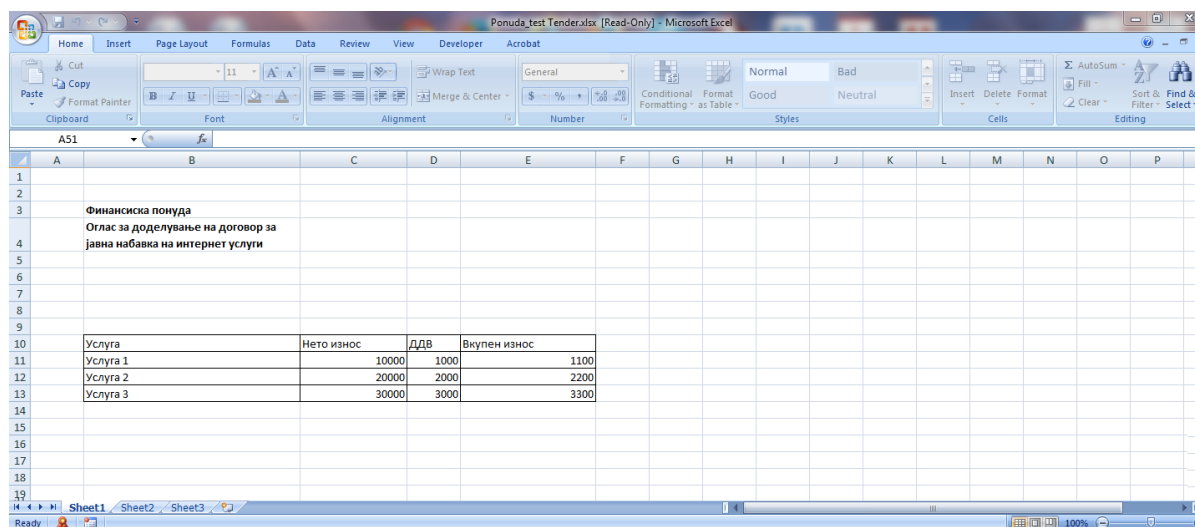

The recipient of the electronically signed document can click on the red icon (ribbon) on the right side of the document to open a screen displaying the details of the digital certificate (when it was issued, by which issuer, and its validity period), as well as the details of the signer, i.e., the holder of the digital certificate.
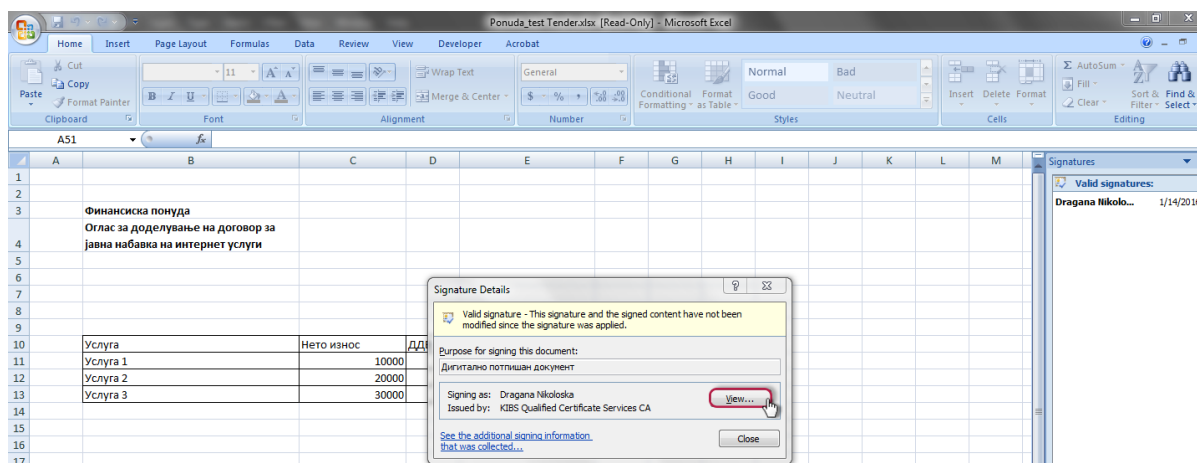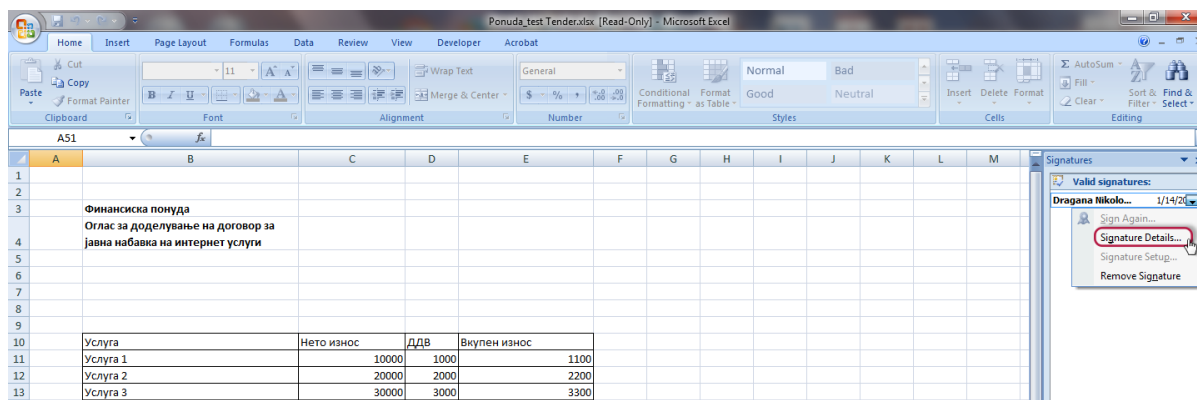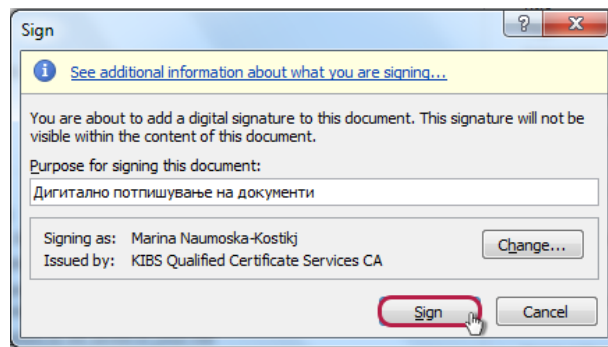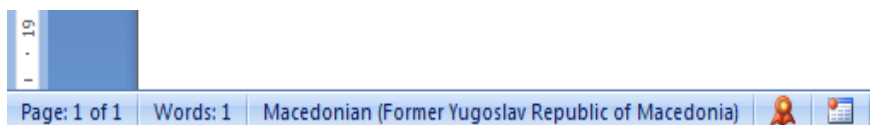
Microsoft Office 2010

Before signing a document, it must be saved under a specific name, and the digital certificate/signature must be installed on the computer. The signing procedure is as follows: **File → Info → Protect Document → Add a Digital Signature**.
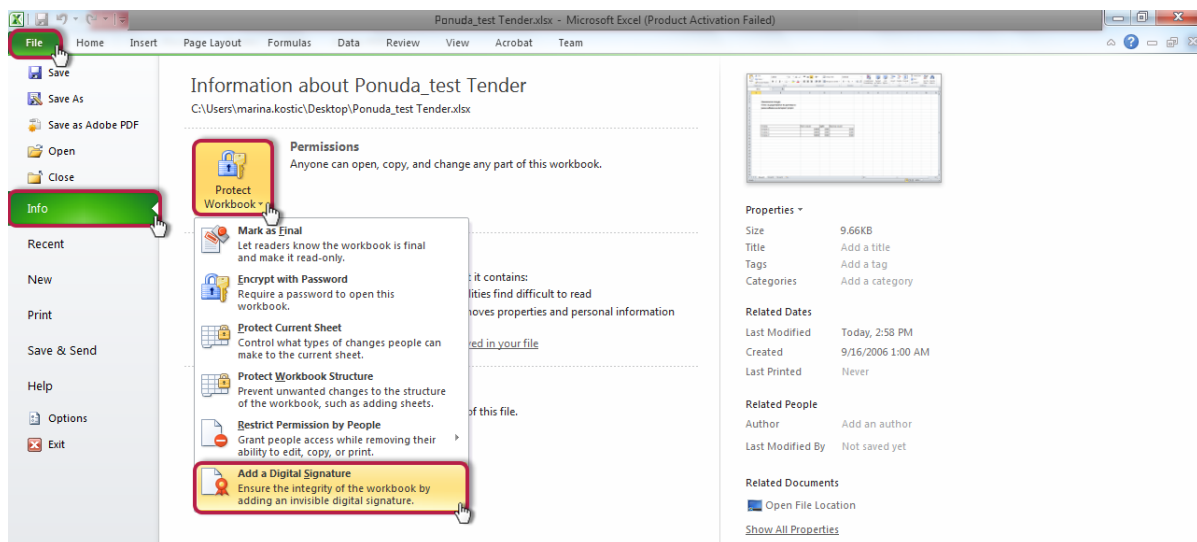
Select the digital certificate (issued by KIBS or Makedonski Telekom) and click the **Sign** button.

A red ribbon will appear at the bottom of the document indicating that it contains digital signatures. To view the details of the signer, click on the red ribbon, and the details will appear in the upper right corner (**Signatures → Signature Details**).

A document that has been digitally signed using the Microsoft Office 2007 suite will have its digital signature visible even when opened in Microsoft Office 2010.

Microsoft Office 2016

Before signing: the document must be saved under a specific name, and the digital certificate must be installed on the computer.
The signing procedure is as follows:
1. File → Info → Protect Document → Add a Digital Signature
2. Select the certificate (KIBS or Makedonski Telekom) and click **Sign**
3. A red ribbon will appear at the bottom of the document, indicating that it contains digital signatures

To view signature details: click the ribbon → **Signatures → Signature Details**
A document digitally signed in Word 2016 is visible and verifiable in all newer versions of Word.

Microsoft Office 2019

Before signing: the document must be saved under a specific name, and the digital certificate must be installed on the computer.
The signing procedure is as follows:
1. File → Info → Protect Document → Add a Digital Signature
2. Select the certificate (KIBS or Makedonski Telekom) and click **Sign**
3. A red ribbon will appear at the bottom of the document, indicating a digital signature

To view signature details: click the ribbon → **Signatures → Signature Details**
Documents signed in Word 2019 are visible and verifiable in Word 2016, 2021, and Microsoft 365.

Word 2021 и Microsoft 365 (останати понови верзии)

Before signing: the document must be saved under a specific name, and the digital certificate must be installed on the computer.

Procedure:
1. File → Info → Protect Document → Add a Digital Signature
2. Select the certificate (KIBS, Makedonski Telekom) and click **Sign**
3. The red ribbon at the bottom will display a message indicating the digital signature

**Signature details:** click the ribbon → **Signatures → Signature Details**

Documents digitally signed in these versions are verifiable and compatible with all previous versions from 2010 onwards.

OPEN OFFICE

If you are using **OpenOffice**, the signing procedure is carried out as follows:

Note: The procedure for applying a digital certificate to any OpenOffice document (Writer, Calc, Impress) is the same.
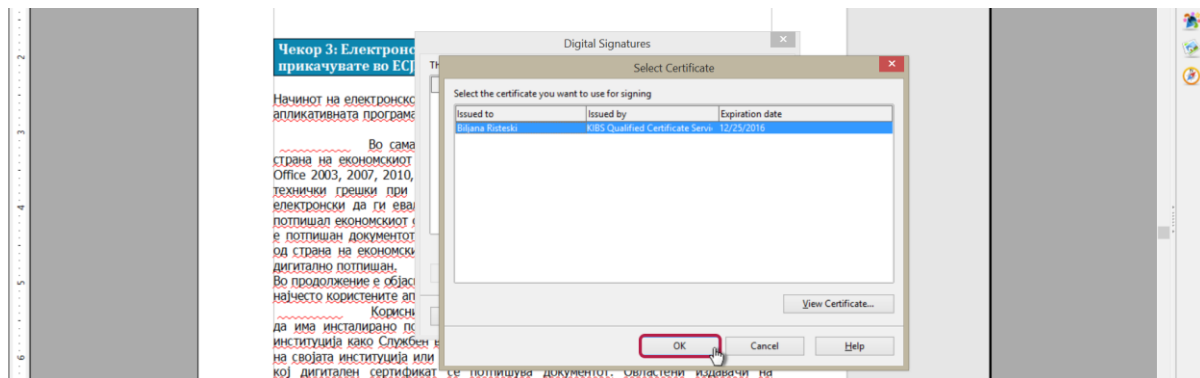
Open the document you want to sign electronically. Click the **File** button in the upper left corner of the screen, then select **Digital Signatures**.
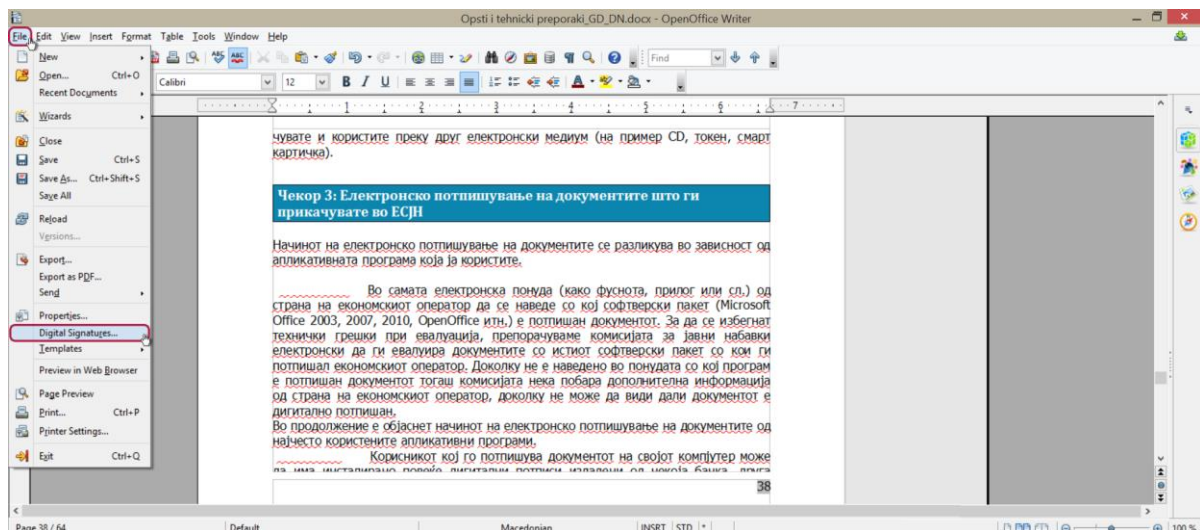

Click the **Sign Document** button to select the certificate you want to use for signing.
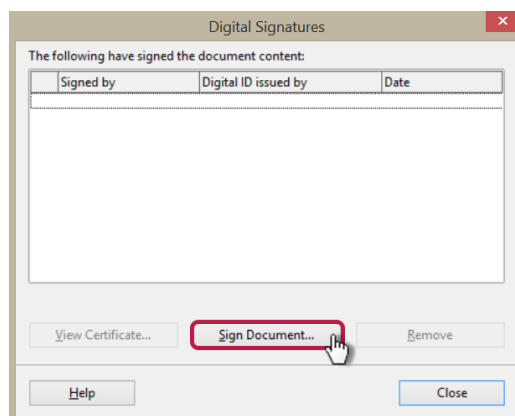
Select the digital certificate you want to use for signing and click **OK**.

After clicking **OK**, a screen will appear with a blank field where you enter the password for your digital certificate (if you chose during installation to require a password for each signing) and click **OK**. Click **OK** again to complete the signing process. After this, a red icon (ribbon) will appear at the bottom of the document (in the Task Bar), indicating that your document has been successfully signed and is ready to be uploaded to the e-Procurement System (ePPS).
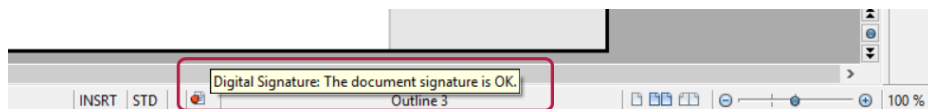

The recipient of the electronically signed document can click on the red icon on the right side of the document to open a screen showing the details of the digital certificate (when it was issued, by which issuer, and its validity period), as well as the details of the signer, i.e., the holder of the digital certificate.

Начин на потпишување ПДФ документи

To convert documents to PDF format, you need to install **PDF Creator** (an open-source application) on your computer, which you can download from the internet or directly from the following link: http://www.pdfforge.org/download.

If you are using **MS Office 2007**, you also have the option to save the document (Word or Excel) directly as a PDF by clicking **Save As**, then selecting **PDF or XPS** (see screenshot).
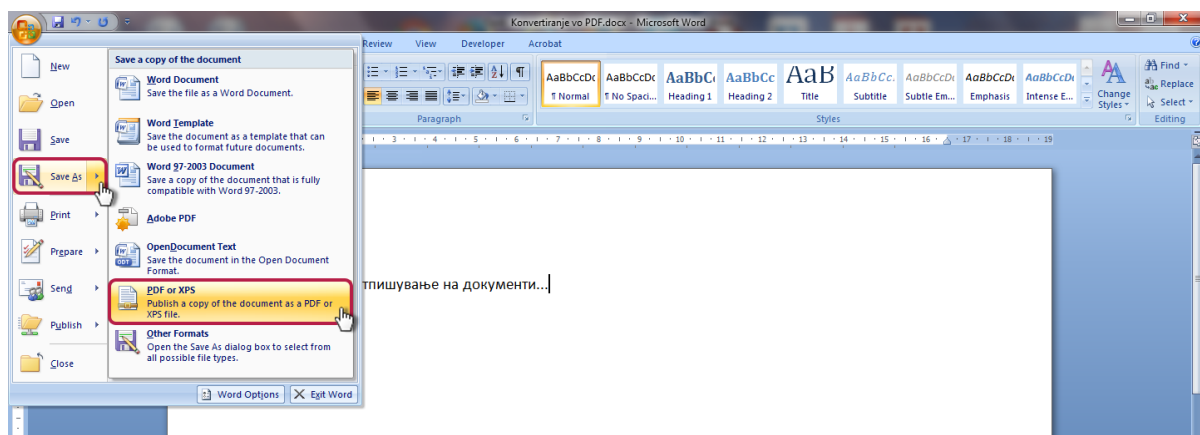
After performing this action, your application will automatically convert the original document into PDF format, which will be ready for digital signing.

Signing documents in **.pdf** format can be done using several applications. Here, we provide an explanation of signing using the **jSignPdf** program (free – open source) and **Adobe Acrobat Pro**.

Jsignpdf

To digitally sign PDF documents, you can use the **jSignPdf** software, which can be downloaded for free from the following link: http://jsignpdf.sourceforge.net/

Complete documentation for installation and instructions on how to sign using this software can be downloaded from: http://jsignpdf.sourceforge.net/uploads/JSignPdf.pdf

You must first have the digital certificate installed on your computer. Then, open the **jSignPdf** program and select the **Advanced view** button to display additional options. In the **Load keys** field, select the digital certificate installed on your computer. If you have multiple digital signatures installed (issued by a bank, another institution such as the Official Gazette, or a domain certificate within your organization or company), you must select in the **Key alias** field the digital certificate issued by an authorized certificate provider (KIBS or Makedonski Telekom).
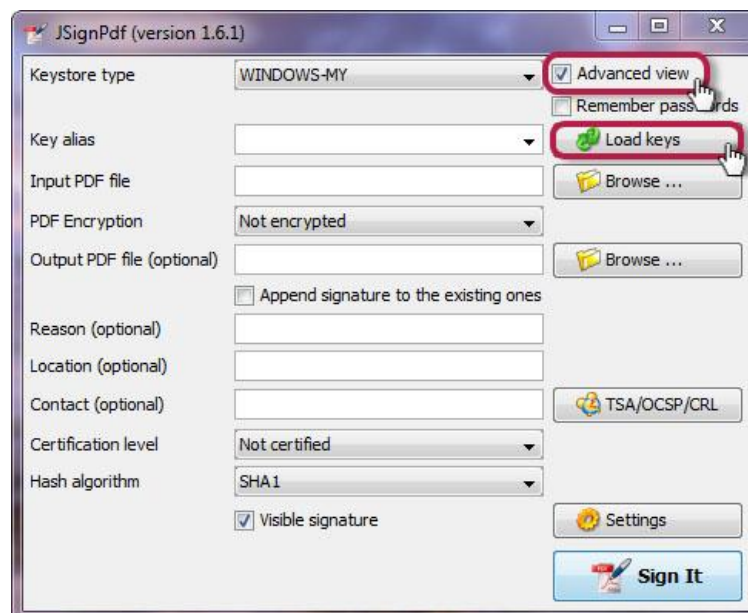
In the **Input PDF File** field, click the **Browse** button and select the PDF document you previously saved. Finally, click the **Sign It** button, then **OK**. The signed document will be saved in the same location as the original document, with the addition of **_signed** in the file name._
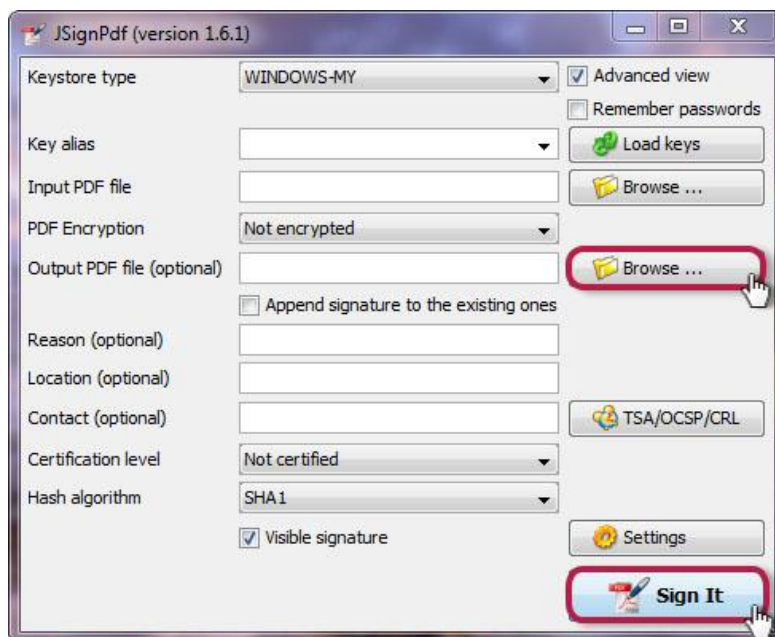
Below is a preview of a document signed in **.pdf** format.
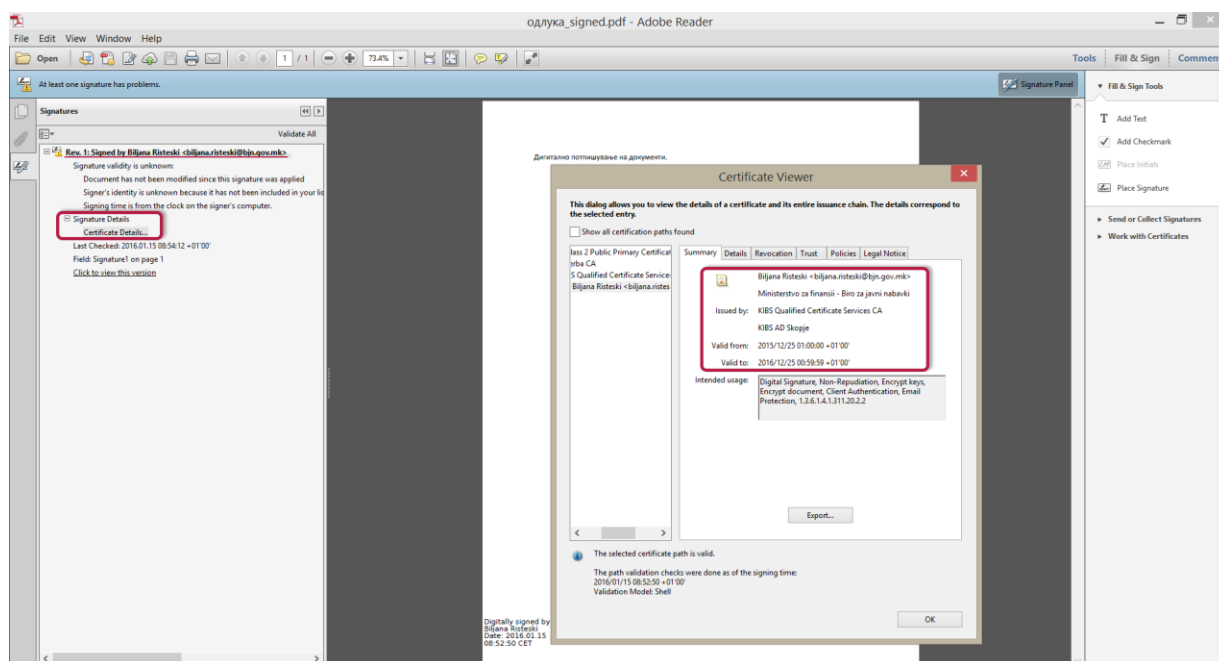
Adobe Reader

Adobe Reader is a free application for viewing and managing PDF documents. In addition to allowing you to read PDFs, Adobe Reader also supports signing documents with a digital certificate, which is a secure and officially recognized method of electronic signing.

You can download Adobe Reader from the following link: https://get.adobe.com/reader/

Before you start digitally signing documents, you must have the digital certificate installed on your computer. Then, open the document you want to sign using Adobe Reader. In the **All Tools** tab, click **View more** to display all options, and then click **Use a certificate**.

Next, click the **Digitally sign** button. Adobe Reader will prompt you to draw a field in the document where your signature will appear. Click **OK**.
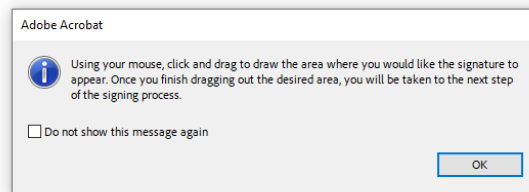

Click and drag with the mouse to define the signature field. After creating the field, a window will open where you can select your digital certificate. Make sure the correct certificate is selected and click **Continue**.
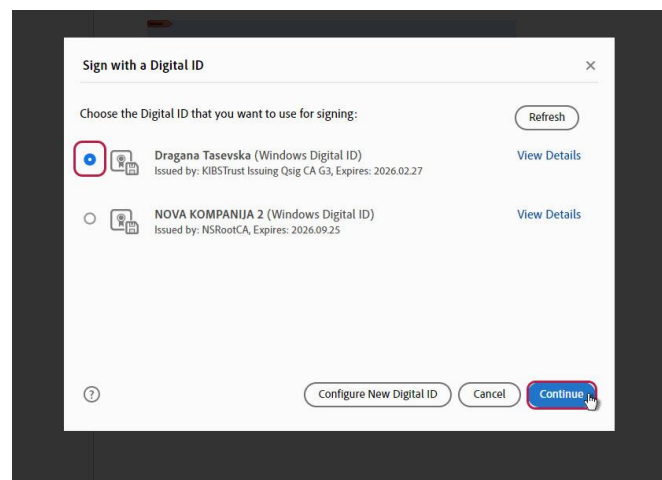
In the new window, your digital signature will be displayed, and then click the **Sign** button
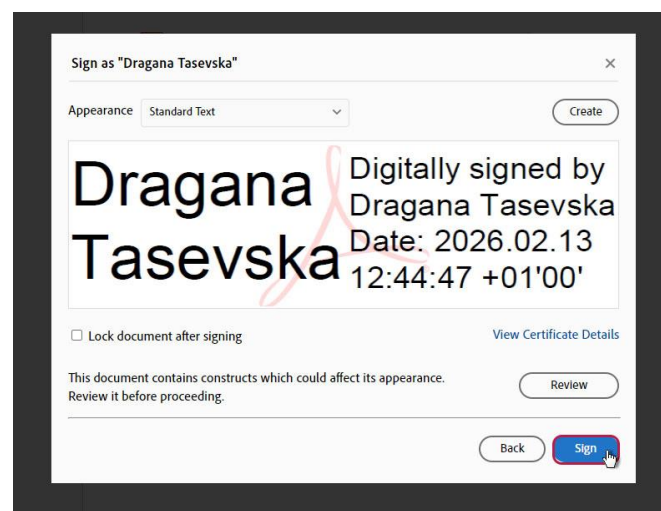
The application will prompt you to save a new version of the document with the signature. The document is now digitally signed and secured. The signature can be verified by any user with a PDF reader that supports digital certificates.
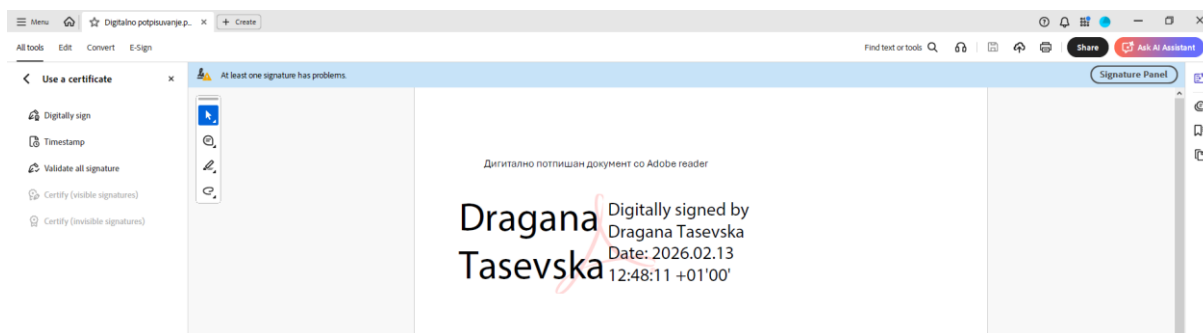
Adobe Acrobat Pro

Adobe Acrobat is a suite of computer programs developed by Adobe Systems, designed for creating, viewing, and managing Adobe Portable Document (PDF) files. The **Adobe Acrobat Pro** program can be used for digitally signing PDF documents, as well as for reviewing and verifying the validity of digital certificates.

You can download Adobe Acrobat Pro from the following link: https://helpx.adobe.com/acrobat/kb/acrobat-downloads.html

Before you start digitally signing documents, you must have the digital certificate installed on your computer. Then, open the document you want to sign using Adobe Acrobat Pro. In the **Fill & Sign → Fill & Sign Tools** tab, click the **Place Signature** button.
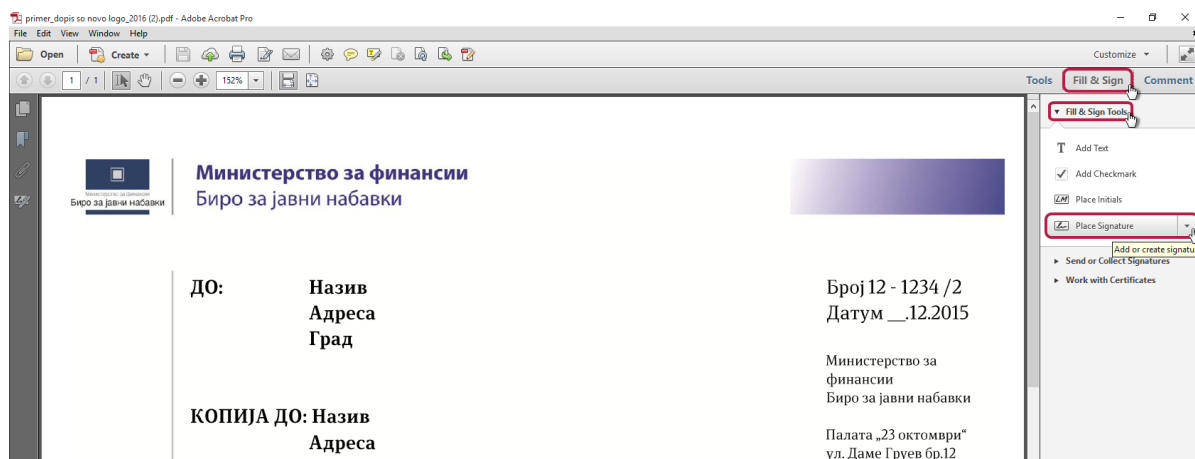

Next, click the **Drag New Signature Rectangle** button and mark the area in the document where you want the digital certificate to be applied.
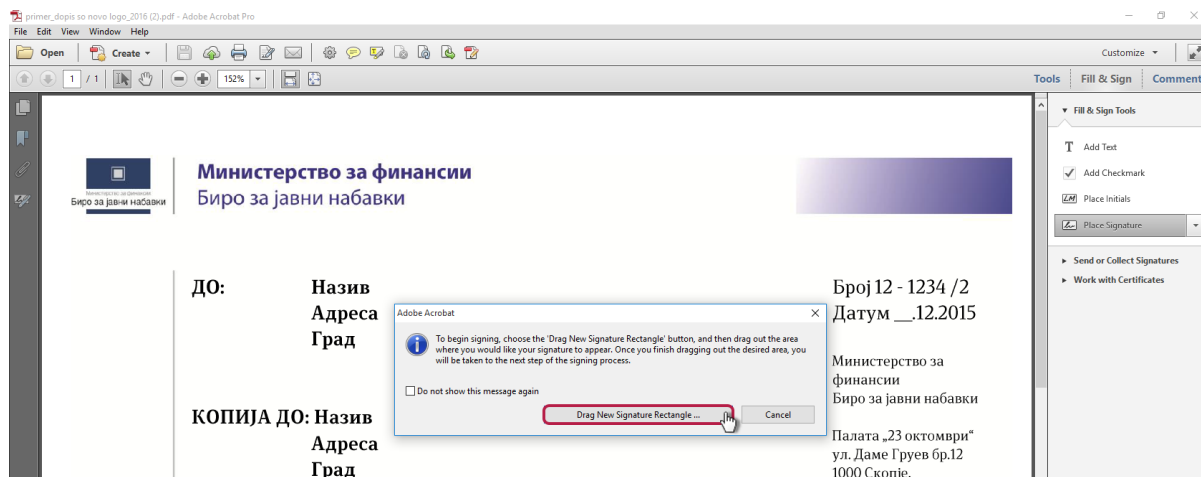
In the window that opens, in the **Sign As** field, select the certificate you want to use for signing if multiple digital certificates are installed on your computer, and then click the **Sign** button.
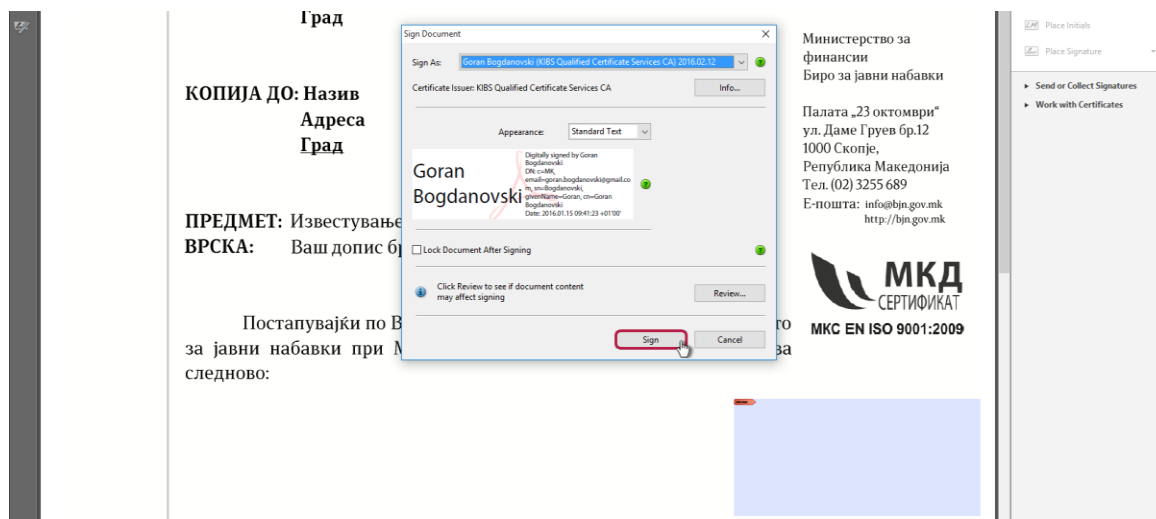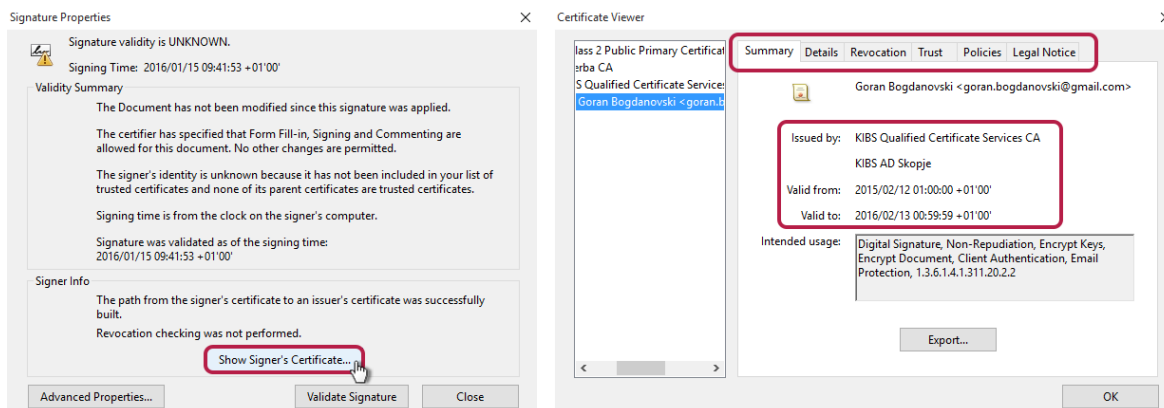

The following image shows a digitally signed PDF document using Adobe Acrobat Pro.
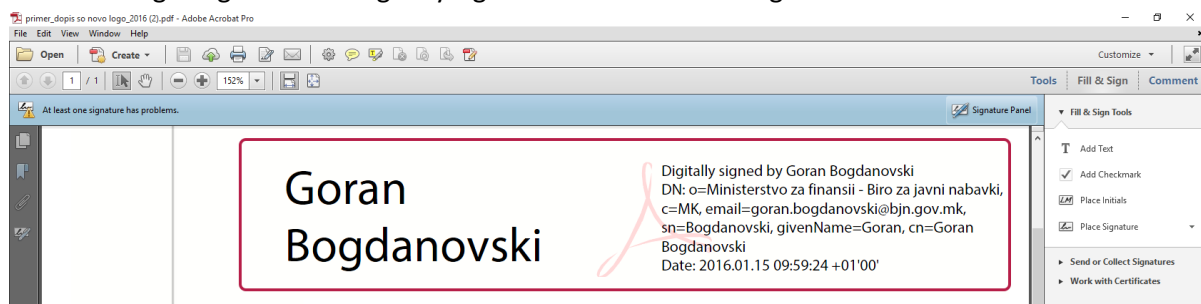
Note: If the root certificates of the digital signature issuer are not installed on the computer, a message may appear in the upper right corner of the document stating "At least one signature has a problem." However, this does not mean that the certificate is invalid.

To verify the validity of the digital signature, click the Signature Panel button, and in the Signature Properties window, click Show Signer's Certificate to view the details of the certificate holder and issuer.

What to do if an "Invalid signature" appears?

If the root certificates of the digital signature issuer are not installed on the computer, a message may appear in the upper right corner of the document stating **"Invalid signatures."** However, this does not mean that the certificate is invalid. To evaluate the certificate, click the **View** button.
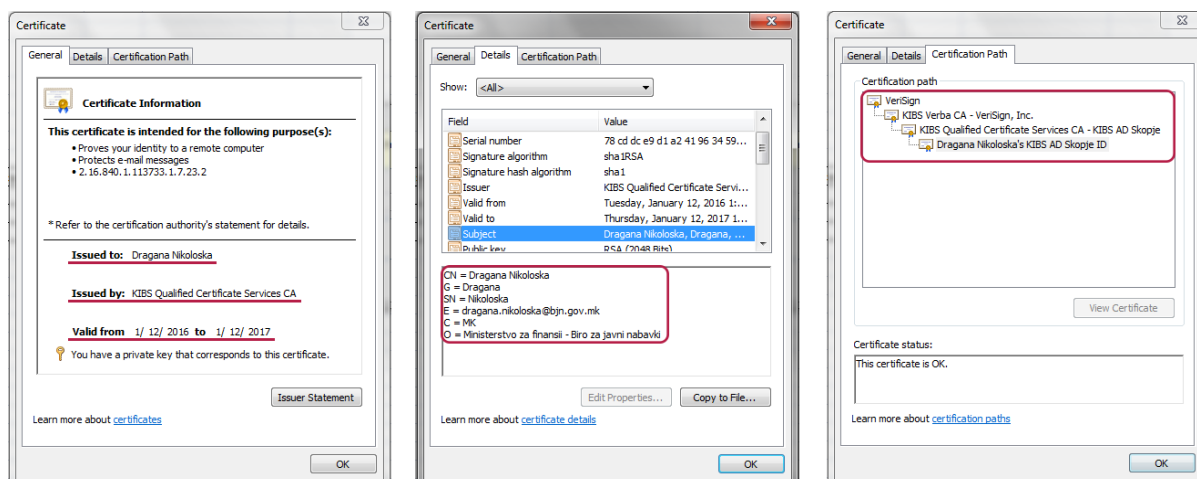
When checking the certificate, you should pay attention to the following:

- In the **General** tab, you can see to whom the certificate is issued, the issuer (whether it is issued by a registered digital certificate provider), and whether it is valid.

- In the **Details** tab, you can see the certificate's serial number, the issuer, validity, and in the **Subject** section you can check the details of the person to whom the certificate is issued and whether it is issued to a legal entity or an individual.

- In the **Certification Path** tab, you can see the path of the specific certificate up to its issuers.

The validity of the certificate can also be checked using the applications provided by digital certificate issuers in North Macedonia. Below are screenshots from the KIBS and Telekom applications.