

MANUAL

Digital signing of pdf documents with Adobe Reader

Version: 4.0 Date: 29.01.2018 103.19

KIBS AD Skopje

© 2018 KIBS AD Skopje, all rights reserved

http://www.kibstrust.mk



Table of Contents

1. Pr	erequesties for signing a pdf document	2
1.1	Check the certificate	2
1.2	Setting up Adobe Reader	3
2. Di	gitally signing a pdf document	5

1. Prerequesties for signing a pdf document

This manual describes digitally signing pdf documents with the Adobe Reader application. This feature in Adobe Reader is available in version 11 or newer. Latest version of Adobe Reader can be downloaded from following location:

http://www.adobe.com/support/downloads/product.jsp?platform=windows&product=10

Before starting the procedure for signing a pdf document, it is necessary to make the following preparations:

Check the certificate 1.1

- If your certificate is on a PKI token (Verba Sign K2, Verba Sign Pro2 or Verba Seal S2), please insert the PKI token in your PC and check whether it is visible through the Internet Explorer web browser. In Internet Explorer, please click on Tools->Internet Options->Content->Certificates. In the Personal tab, your certificate should be listed (Figure 1). In case the certificate is not listed, please check whether you have the necessary drivers installed for your PKI token (Gemalto ID Prime or Gemalto Java), as stated in the corresponding manual How to start using a certificate issued on a Gemalto IDPrime PKI token with Internet Explorer or How to start using a certificate issued on a Gemalto Java PKI token.
- ✓ If your certificate is generated on a hard disk (Verba Sign K1, Verba Sign Pro1 or Verba Seal S1), please check whether it is located in the certificate store of the Internet Explorer web browser. In Internet Explorer, please click on Tools->Internet Options->Content->Certificates. In the Personal tab, your certificate should be listed (Error! Reference source not found.). In case your certificate is not listed, please import it in Internet Explorer, fowowing the FAQ "How to import a certificate in Internet Explorer from .pfx or .p12 backup file?"

			Internet Options ? ×
File Edit View Favorites	Tools Help Delete browsing history InPrivate Browsing	Ctrl+Shift+Del Ctrl+Shift+P	General Security Privac Content Connections Programs Advanced Certificates
	Turn on Tracking Protection		Certificates X
	ActiveX Filtering Fix connection problems Reopen last browsing session Add site to Apps		Interned purpose: <all></all>
	View downloads	Ctrl+J	Insection Prezime 10 KibsTrust Qualified Certificate Services 26.11.2018 <none></none>
	Pop-up Blocker SmartScreen Filter Manage media licenses Manage add-ons	>	
	Compatibility View settings		
	Subscribe to this feed Feed discovery	>	< >>
	Windows Update		Import Export Remove
	Performance dashboard F12 Developer Tools	Ctri+Shift+U	Certificate intended purposes
			Liept Authentication, Secure Email, Smart (Lard Logon
	OneNote Linked Notes Send to OneNote		
	OneNote Linked Notes Send to OneNote Report website problems		View Close

Figure 1

×

1.2 Setting up Adobe Reader

Adobe Reader has it own root certificate store (Trusted Certificates). This root certificate store differs from the one used by the Windows operating system. To avert the problems that might arise from the process of validating the signature with which a document has been signed, it is necessary to integrate these two stores, by following these steps:





2. From the right hand side select **Signatures**. In the **Verification** part, please click on **More**... (Error! Reference source not found.).

eterences		
Categories:	Digital Signatures	
Commenting Documents Full Screen General Page Display	Creation & Appearance • Control options for signature creation • Set the appearance of signatures within a document	More
3D & Multimedia Accessibility Adobe Online Services Email Accounts	Verification • Control how and when signatures are verified	More
Identity Internet JavaScript Language Measuring (2D)	Identities & Trusted Certificates • Create and manage identities for signing • Manage credentials used to trust documents	More
Measuring (2D) Measuring (3D) Measuring (Geo) Multimedia (legacy) Multimedia Trust (legacy) Reading	Document Timestamping • Configure timestamp server settings	More
Reviewing Search Security		
Signatures Spelling		
Tracker Trust Manager Units Undater		
		OK Cancel

Figure 3

3. In the new window, in the **Windows Integration** part, please enable the **Validating Signatures** option (Figure 4). To close the windows, please click on **OK** two times.

Verify signatures when the document is opened When document has valid but untrusted signatures, prompt to review and trust signers Verification Behavior When Verifying: Use the document-specified method; prompt if unavailable Use the gocument-specified method; if unavailable, use default method Always use the default method: Adobe Default Security Require certificate revocation checking to succeed whenever possible during signature verification Ignore document validation information Verification Time Verify Signatures Using: Time at which the signature was created Secure time (timestamp) embedded in the signature Qurrent time Use gapired timestamps Verification Information
 When document has valid but untrusted signatures, prompt to review and trust signers Verification Behavior When Verifying: Use the document-specified method; prompt if unavailable Use the gocument-specified method; if unavailable, use default method Always use the default method: Adobe Default Security Require certificate revocation checking to succeed whenever possible during signature verification Ignore document validation information Verification Time Verify Signatures Using: Time at which the signature was created Secure time (timestamp) embedded in the signature Qurrent time Use gapired timestamps Verification Information
Verification Behavior When Verifying:
Verification Behavior When Verifying: Use the document-specified method; prompt if unavailable Use the document-specified method; if unavailable, use default method Always use the default method: Adobe Default Security Require certificate revocation checking to succeed whenever possible during signature verification Ignore document validation information Verification Time Verify Signatures Using: Time at which the signature was created Secure time (timestamp) embedded in the signature Current time Use gxpired timestamps Verification Information
 Use the document-specified method; prompt if unavailable Use the document-specified method; if unavailable, use default method Always use the default method: Adobe Default Security Require certificate revocation checking to succeed whenever possible during signature verification Ignore document validation information Verification Time Verify Signatures Using: Time at which the signature was created Secure time (timestamp) embedded in the signature Current time Use gxpired timestamps Verification Information under the signature
Use the document-specified method; prompt if unavailable Use the document-specified method; if unavailable, use default method Always use the default method: Advays use the default method: Advacue certificate revocation checking to succeed whenever possible during signature verification Ignore document validation information Verification Time Verify Signatures Using: Image at which the signature was created Secure time (timestamp) embedded in the signature Qurrent time Use gapired timestamps Verification Information
Ose the good methody in dinavariable, use default method Always use the default method: Adobe Default Security * If Require certificate revocation checking to succeed whenever possible during signature verification Ignore document validation information Verification Time Verify Signatures Using: Ime at which the signature was created Secure time (timestamp) embedded in the signature Qurrent time Use gxpired timestamps Verification Information under suing signed PDF:
 Always use the default method: Adobe Default Security * Require certificate revocation checking to succeed whenever possible during signature verification Ignore document validation information Verification Time Verify Signatures Using: Time at which the signature was created Secure time (timestamp) embedded in the signature Current time Use gxpired timestamps Verification Information under the signature
Require certificate revocation checking to succeed whenever possible during signature verification Ignore document validation information Verification Time Verify Signatures Using: © Time at which the signature was created © Secure time (timestamp) embedded in the signature © Current time © Use gxpired timestamps Verification Information Verification Information
Ignore document validation information Verification Time Verify Signatures Using:
Verification Time Verify Signatures Using:
Verify Signatures Using:
Ime at which the signature was created Secure time (timestamp) embedded in the signature Current time Use gxpired timestamps Verification Information Automatically add verification information when raving signed PDF:
Secure time (timestamp) embedded in the signature Current time Use gxpired timestamps Verification Information Automatically add verification information when raving signed PDF:
Current time Use gxpired timestamps Verification Information Automatically add verification information when raving signed PDF:
Use gxpired timestamps Verification Information Automatically add verification information when raving signed PDF:
Verification Information
Verification Information Automatically add verification information when saving signed PDF:
Ask when verification information is too big Abusta
C Always
Windows Integration
Thus ALL foot certificates in the windows Certificate store for:
Validating Signatures
valuating Certified Bocuments
Selecting either of these options may result in arbitrary material being treated as trusted content. Take care before enabling these features.
Help OK Cancel

Figure 4

2. Digitally signing a pdf document

The procedure for signing a pdf document with Adobe Reader is consisted of the following steps:

 Through Adobe Reader, please open the pdf document, which needs to be digitally signed. From the menu on the right hand site, please select Fill&Sign->Work with Certificates->Sign with Certificate. (Figure 5)



Figure 5

2. A new window opens, as shown on Figure 6. Please select **Drag New Signature Rectangle...** and then in the document frame, please draw a rectangle where the signature should be visible (Figure 6).



Figure 6





3. After drawing the rectangle, a new window automatically appears, as shown Figure 8. In **Sign As**, please choose the certificate and in the middle, the visual appearance of the signature is shown. To sign the document, please click **Sign**.

Sign Document		×
Sign As: Ime14 Prezim	e14 (KibsTrust Qualified Certifica	ate Services) 👻 🕜
Certificate Issuer: Kibs Hu	ist Qualmed Certificate Services	<u>10</u> 10
	Appearance: Standard Text	t v
lme14 Prezime	Digitally signed by Ime14 Prezime DN: ou=Oddel14, o=Test Organizacija14, serialNumber=5529581, c=MK, email=ca-pomos@kibs.mk, sn=Prezime14, givenName=Ime1 cn=Ime14 Prezime14 Date: 2016.01.28 10:07:47 +01'00'	e14 (4,
Loc <u>k</u> Document After	Signing	•
 Click Review to see may affect signing 	e if document content J	Re <u>v</u> iew
	Sign	Cancel

Figure 8

4. Then, a window appears for saving the signed document. Please select the location and click **Save** (Figure 9).

Save As	H	×
🕞 🔾 🗢 💻 Desktop 🕨	🗸 🐓 🖉 Search Desktop	٩
Organize 🔻 New folder		= • 📀
 ▲ ★ Favorites ■ Desktop ③ Downloads ③ Recent Places ▲ ○ Libraries ▶ ○ Documents ▶ ○ Music ▶ ○ Pictures ▶ ♥ Videos 	 Name Libraries Advectu Agra Lib José Cos Computer Network Joga Balgimese Ruli Conjud? Virritusis Friene 75250 DryLingse Libraria 75250 DryLingse Libraria 75250 	
File <u>n</u> ame: Документ за потпис.pdf Save as type: Adobe PDF Files (*.pdf) Hide Folders	Save to Online Account 💌 Save	 ✓ ✓ Cancel



5. The next step for signing a document is inserting the PIN, if the certificate is on a token or inserting a password, if the certificate is on a disk (Figure 10).

Card	
\$	Please Enter your PIN Code
ОК	Cancel

Figure 10

6. After inserting the PIN or password, the document is digitally signed. On the document, the visual signature is shown, while in the upper part of the document there is a blue strip with a green sign (Figure 11), which confirms that the document is signed with a valid signature (Signed and all signatures are valid).



* * *