MANUAL

Downloading a certificate using Internet Explorer

Version: 4.0 Date: 09.01.2018

103.10

KIBS AD Skopje

© 2017 KIBS AD Skopje, all rights reserved

http://www.kibstrust.mk



Table of Contents

1.	Prerequisites for downloading a certificate	2
2.	How to download the certificate?	6
3.	How to check whether the certificate is successfully installed?	11
4.	How to back up the certificate?	13

1. Prerequisites for downloading a certificate

Before you start the procedure for downloading a certificate, you need to check the security settings of your web browser. To be certain that no problems will arise while downloading the certificate, it is recommended to add the webpage https://e-shop.kibstrust.mk in the list of Trusted Sites and to enable execution of ActiveX controls in that zone.

To make the recommended settings, follow the next steps:

1. From the browser menu click on the **Tools** button and select **Internet Options** (Figure 1):



Figure 1

2. In the new window, select the **Security** tab. Click on **Trusted Sites** and then click on the **Sites** button (Figure 2):



Figure 2

3. In the Add this website to the zone text field enter https://e-shop.kibstrust.mk and click on the Add button (Figure 3). By doing this, this webpage will appear in the Websites list as shown on Figure 4. Click Close.

	×
You can add and remove websites from this zo this zone will use the zone's security settings.	ne. All websites in
Add this website to the zone: https://e-shop.kibstrust.mk	Add
Websites:	
	<u>R</u> emove
Require server verification (https:) for all sites in thi	s zone
	Close
Figure 3	
Trusted sites	×
You can add and remove websites from this zone this zone will use the zone's security settings.	ne. All websites in
You can add and remove websites from this zo this zone will use the zone's security settings. Add this website to the zone:	ne. All websites in
You can add and remove websites from this zo this zone will use the zone's security settings. Add this website to the zone:	ne. All websites in <u>A</u> dd
You can add and remove websites from this zo this zone will use the zone's security settings. Add this website to the zone:	ne. All websites in <u>A</u> dd
You can add and remove websites from this zo this zone will use the zone's security settings. Add this website to the zone:	ne. All websites in Add
You can add and remove websites from this zo this zone will use the zone's security settings. Add this website to the zone:	ne. All websites in Add <u>R</u> emove
You can add and remove websites from this zo this zone will use the zone's security settings. Add this website to the zone:	ne. All websites in Add Remove
You can add and remove websites from this zo this zone will use the zone's security settings. Add this website to the zone:	All websites in Add Remove

Figure 4

4. In the Security tab, choose Trusted Sites and click on the Custom Level... button (Figure 5):





5. In **Reset Custom Settings**, from the **Reset to**: list choose **Medium**, as shown on Figure 6. This enables execution of ActiveX controls on the websites you trust. Click **OK** two times.

Security Settings - Trusted Sites Zone 🛛 🗙 🗙
Settings
ActiveX controls and plug-ins ActiveX controls and plug-ins Allow ActiveX Filtering Disable Finable Allow previously unused ActiveX controls to run without prom Disable Finable Allow Scriptlets Disable Finable Fina
*Takes effect after you restart your computer
Reset custom settings <u>Reset to:</u> Medium (default) ~ Reset
OK Cancel
Figure 6

 In Internet Explorer 11, it is necessary to add the domain kibstrust.mk in the Compatibility View. To do that, from the browser menu select Tools->Compatibility View settings (Figure 7):

File	Edit	View	Favorites	Tools	Help	
				D	elete browsing history Private Browsing	Ctrl+Shift+Del Ctrl+Shift+P
				Ti A	urn on Tracking Protection ctiveX Filtering	
				R	x connection problems eopen last browsing session dd site to Apps	
				Vi Pr	iew downloads op-up Blocker	Ctrl+J >
				Si M	nartScreen Filter Ianage media licenses Ianage add-ons	>
				С	ompatibility View settings	
				Su	ubscribe to this feed	

Figure 7

In the new window check whether "kibstrust.mk" is entered in the Add this website field and then click Add (Figure 8):

Compatibility View Settings	:	×
Change Compatibility View	w Settings	
Add this website:		
kibstrust.mk	Add	1
Websites you've added to Compa	tibility View:	
	Remove	
Display intranet sites in Compa	atibility View	
Learn more by reading the Int	> ernet Explorer privacy statement	
	⊆lose	

Figure 8

To finish the procedure click Close (Figure 9):

Compatibility View Settings	×
Change Compatibility View Settings	
Add this website:	
1	<u>A</u> dd
Websites you've added to Compatibility View:	
kibstrust.mk	<u>R</u> emove
Display intranet sites in Compatibility View Use Microsoft compatibility lists Learn more by reading the <u>Internet Explorer privacy</u>	<u>statement</u>
	⊆lose



In order for the changes to take place, please close the web browser and then open it again. Now you are ready to download your certificate.

2. How to download the certificate?

From the certificates that KIBS CA offers, the certificates Verba Sign K1, Verba Sign Pro1 and Verba Seal S1 are generated on the disk of your PC.

To download one of the previous mentioned certificates, by using Internet Explorer, follow the next steps:

 Follow the link which is listed in the e-mail message that you received with a notification that your purchase order for a certificate is approved (<u>https://e-shop.kibstrust.mk/raweb/verbaen.aspx</u>). If you use Internet Explorer 11 continue with step 2, otherwise go to step 3.

On the web page (Figure 10) enter:

- Order: enter the number of the order which was sent in the same e-mail message
- E-mail: enter the e-mail address which was entered in the request for certificate form

Click Submit.

F KIB	STrust		
	DOWNI	OAD CERTIF	ICATE
	Verba Sign	K1	Pro1
	Insert information	tion for your cert	tificate order
Order number			
Email			
	1	SUBMIT	
	@ 2015 KIBS	AD Skooie All right	ts reserved

Figure 10

- 2. A new webpage will open to confirm the registration data (Figure 11). Check the data, enter an **Authentication phrase** and click **Submit**.
- 3. After clicking on **Submit**, a message will appear, as shown on Figure 12. Once again, check the e-mail address and click **OK** if everything is in order.

🗹 Syma	antec.	Enro	ollment		
Help with	this Page	ent Form			
Enter yo	ur Digital ID inf	ormation			
Fill in all re are viewat	quired fields. Fields le in the certificate's	marked with an a details.	asterisk (*) are	included with y	our Digital ID and
First Na Nickname	me: * (required) or middle initial allo	owed	First N	ame	-
Last Na (example	me: * (required)		Last N	ame	
Your E-	mail Address: *	(required) c.com)	name.	surname@dom	ain.
Compar (Example	y/Agency/Org: Symantec)	*	Compa	iny	
Dept/D (Example	iv/Proj: * Administration)		IT		
Rezervi	rano pole: *		Rezen	irano Pole	
Naracka	broj: (required)		99090	427	
Country (example	:* (required) US)		МК		
If a	Submit 5. Symantec Corporation.) above is correcting.	ct, Cancel	ב	∕ Symante
		Fig	ure 11		
ssage fro	m webpage				
? i	ionfirm your e- me.prezime@d	mail address: Iomain.mk	:		
lf c	your e-mail ac orrect it in the	dress is corre enrollment fo	ect, click OK. orm.	lf not, click	CANCEL and
lf D	the e-mail add igital ID.	dress is not co	orrect, you w	ill not be ab	le to use your
			-	OK	Cane



4. A windows appears, as shown on Figure 13, which asks for a confirmation that you allow the execution of the operation regarding the digital certificates. This window appears two times and both times you need to click **Yes**.





5. The certificate generation process start. Please wait while the process executes (Figure 14).

Please wait while the Digital ID is being issued ...



Figure 14

6. On the windows with messages on Figure 15 click Yes.



Figure 15

7. Congratulations, your certificate has been successfully generated and installed (Figure 16)!



Figure 16

3. How to check whether the certificate is successfully installed?

After receiving a message that your certificate is successfully installed, it is necessary to check whether it is added in the list of personal certificates in the web browser. To make this check, please follow the next steps:

1. From the browser menu click on the **Tools** button and select **Internet Options** (Figure 17):





2. In the new window select the **Content** tab. In the **Certificates** frame, click on the **Certificates** button (Figure 18):



Figure 18

3. If your certificate is successfully installed, it will be in the certificate list in the **Personal** tab (Figure 19):

	;						
tended p	urpose:	<all></all>					
Personal	Other Peop	ole In	ermediate Certification	Authorities	Trusted P	Root Cer	tificatior 4
ISSUEU	10	15	sueu by		expir	auo	Friendly N
Ime	10 Prezime1	о кі	bsTrust Qualified Certif	icate Services	26.1	1.2018	<none></none>
<							>
<	<u>E</u> xp	port	<u>R</u> emove			[Advanced
< Import Certificati	Exp	oort	Remove			[> <u>A</u> dvanced
Import Certificate	Exp e intended p chentication,	oort urpose Secure	<u>R</u> emove 5 Email, Smart Card Log	on			<u>A</u> dvanced



Click **View** and a new window will open which shows a detailed review of information regarding the certificate. In the **General** tab (Figure 20), the common information regarding the certificate are given:

Issued to: The name of the person to which the certificate is issued

Issued by: The name of the Certificate Authority (KibsTrust Qualified Certificate Services) **Valid from:** Issue date **to:** Expiration date

At the bottom there is information that you own the private key which corresponds to the certificate: **"You have a private key that corresponds to this certificate.** "

🐖 Certificate	×
General Details Certification Path	
Certificate Information	
This certificate is intended for the following purpose(s): • Proves your identity to a remote computer • Protects e-mail messages • 2.16.840.1.113733.1.7.23.2 • Smart Card Logon	-
* Refer to the certification authority's statement for details. Issued to: Ime10 Prezime10	-
Issued by: KibsTrust Qualified Certificate Services	
Valid from 26.11.2015 to 26.11.2018	
$\ref{eq: product}$ You have a private key that corresponds to this certificate.	
Issuer <u>S</u> tatemen	:
ОК	

Figure 20

The root certificates, with which your certificate is signed, are shown in the **Certification Path** tab (Figure 21). Check whether the three root certificates are shown: **VeriSign Class 2 Public Primary Certification Authority – G3, KibsTrust Certification Authority and KibsTrust Qualified Certificate Services**. In the bottom of the **Certification Path** tab is the information about the status of the certificate. If your certificate is OK, then this message will be shown: "This certificate is OK. "

<u>द्रा</u> Certi	ficate				×
General	Details	Certification Path			
Certif	ication <u>p</u> a VeriSign (KibsT	ath Class 2 Public Primary rust Certification Au ibsTrust Qualified Ce Time10 Prezime10	v Certification thority rtificate Serv	Authority - G3 ices	
Certific This ce	ate <u>s</u> tatu: rtificate i:	5: 5 OK.		⊻iew Certificate	K



4. How to back up the certificate?

Your certificate is installed on the disk of your PC and can be erased by a bug in operating system or hardware failure. To protect your certificate in these kind of situations, it is necessary to make a backup of the certificate i.e. export it in a .PFX file.

To make a backup of your certificate you need to follow these steps:

1. From the browser menu click on the **Tools** button and select **Internet Options** (Figure 22):



2. In the new window select the **Content** tab. In the **Certificates** frame, click on the **Certificates** button (Figure 23):

Internet Options		?	×
General Security Privacy Content Connections	s Programs	Adva	nced
CertificatesUse certificates for encrypted connection	ns and identif	ication	
Clear SSL state Certificates	Publish	ers	
AutoComplete			
AutoComplete stores previous entries on webpages and suggests matches for you.	Settin	gs	
Feeds and Web Slices			_
Feeds and Web Slices provide updated content from websites that can be read in Internet Explorer and other programs.	Settin	gs	
ОК	Cancel	Ap	ply

Figure 23

3. In the **Personal** tab, choose your certificate and click on the **Export** button (Figure 24):

Certificates			×
Intended purpose:	<all></all>		~
Personal Other Peop	le Intermediate Certification Authorities	Trusted Root Ce	rtification 💶 🕨
Issued To	Issued By	Expiratio	Eriendly Na
Ime10 Prezime10	KibsTrust Qualified Certificate Services	26.11.2018	<none></none>
<			>
Import	ort <u>R</u> emove		<u>A</u> dvanced
Certificate intended pu	urposes		
Client Authentication,	Secure Email, Smart Card Logon		
			View
			Close
			2036



4. By clicking the **Export** button, a wizard opens which will guide you through the procedure of exporting a certificate (Figure 25). To continue click **Next**:

🔶 🛯 🔗 Certificate Export Wizard	×
Welcome to the Certificate Export Wizard	
This wizard helps you copy certificates, certificate trust lists and certificate reve lists from a certificate store to your disk.	ocation
A certificate, which is issued by a certification authority, is a confirmation of yo and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.	ur identity
To continue, click Next.	
	Const
Next	Cancel

Figure 25

5. Choose the "Yes, export the private key" option (Figure 26). To continue click Next:

		×
←	🚰 Certificate Export Wizard	
	Export Private Key	
	You can choose to export the private key with the certificate.	
	Private keys are password protected. If you want to export the private key with the certificate, you must type a password on a later page.	
	Do you want to export the private key with the certificate?	
	○ <u><u>M</u>es, export the private key ○ No, do not export the private key </u>	
	<u>N</u> ext Canc	el

Figure 26

6. Choose a .PFX file format in which you the certificate will export and choose to export the root certificates (Figure 27). To continue click **Next**:



Figure 27

 Enter a password to protect the private key (Figure 28). You are the only one that knows the password, please remember it or keep it written down in a safe place! Click Next to continue:

			×
← <i> §</i> Cert	ificate Export Wizard		
Securi	ty		
To) maintain security, you must protect the private key I ing a password.	to a security principal or by	
	Group or user names (recommended)		-
		Add	
		Remove	
		Konovo	
J	Password:		
Ľ	••••••		
	<u>⊂</u> onfirm password:		
	••••••		
		Next Cancel	
		<u>in</u> ext Cancer	



8. Enter a file name and location to which you will export the certificate (Figure 29). Click **Next** to continue:

Fi	le to Export	
	Specify the name of the file you want to export	
	Eile name:	
	E:\ImePrezime.pf×	Browse

Figure 29

9. In the next window (Figure 30) you get a short preview of the settings you made. Click on the **Finish** button to finish the procedure of exporting a certificate:

← 🛛 🛃 Certificate Export Wizard	×
Completing the Certificate Export Wizard	
You have successfully completed the Certificate Export wizard.	
You have specified the following settings:	
File Name E:\ImePrezime.pfx	
Export Keys Yes	
Include all certificates in the certification path Yes	
File Format Personal Information I	Exchange (*.pfx]
<	>
	Einish Cancel



10. You will receive a message that you successfully exported your certificate (Figure 31):

Certificate Export Wizard	x k
The export was success	ful.
	ж



IMPORTANT: Store the .PFX file to which your certificate is exported and the password for it on a safe external media (external hard drive, USB flash, CD/DVD...)!

* * *