

User Manual

How to start using a certificate issued on a Gemalto IDPrime PKI token?

Version: 4.2 Date: 02.02.2022 103.18

KIBS AD Skopje ©2022 KIBS AD Skopje, all rights reserved <u>http://www.kibstrust.com/</u>

Table of Contents

1.	Purpo	ose of use1
2.	How	to install the middleware software used for the Gemalto IDPrime PKI token?1
	2.1	Intro 1
	2.2	Installation of middleware software on Windows operating system
3.	Check	the content of the Gemalto IDPrime PKI token6
4.	Chan	ge of user PIN6
5.	Toker	n information7
6. Ex	How t plorer	to check if the certificate from my Gemalto IDPrime PKI token is shown in Internet ?
	6.1	How to check if the certificate is shown in Internet Explorer
	6.2	Installation of root certificates in Internet Explorer 11
7.	Does	my certificate from the Gemalto IDPrime PKI token is shown in Google Chrome?11
	7.1	Check if the certificate is shown in Google Chrome
8.	How 1 12	to check if the certificate from my Gemalto IDPrime PKI token is shown in Mozilla Firefox?
	8.1	Adding a Gemalto IDPrime PKI token as a security device
	8.2 Fire	How to check if the certificate from the Gemalto IDPrime PKI token is shown in Mozilla fox?
	8.3	How to install root certificates in Mozilla Firefox?16

1. Purpose of use

This user manual is strictly intended for the users of Qualified certificates for qualified electronic signature: **Verba Sign PKI token and Verba Sign Pro PKI token.**

Those users who have obtained Gemalto IDPrime PKI token, with a generated pair of keys and a certificate, in a Local Registration Authority (LRA) of Certificate Authority KIBS (CA KIBS), and need to access the certificate trough Microsoft Internet Explorer, Google Chrome or Mozilla Firefox.

Definitions:

QSCD = Qualified Signature Creation Device

Gemalto IDPrime PKI token can refer to:

- Gemalto IDPrime MD 840 token (QSCD)
- Gemalto IDPrime MD 940 token (QSCD)
- Gemalto IDPrime .NET token (non QSCD, used in legacy certificates profiles)

The same software is used for all types of tokens.

The certificate is installed on Gemalto IDPrime PKI token, in the presence of the user, using a software for secure certificate management. This software guarantees that the private key is solely stored on the Gemalto IDPrime PKI token, which is delivered to the user.

NOTICE: The Gemalto Classic Client software is not applicable for Gemalto IDPrime token!

2. How to install the middleware software used for the Gemalto IDPrime PKI token?

2.1 Intro

In most of the cases, without additional middleware software installation, only with plugging the Gemalto IDPrime PKI token in your computer with Windows operating system, Plug&Play installation is initialized, and the certificate is loaded in your Internet Explorer web browser.

However, for better support for most recent versions of Windows 11 and Windows 10, our recommendation is to install the special package **SafeNet Authentication client (SAC Client)** from the following links:

For x86-based PC, for 32-bit operating system: <u>https://www.kibstrust.com/Storage/Support/Software/KIBSTrust-SAC-x32-10.8-R6.msi</u> For x64-based PC, for 64-bit operating system: <u>https://www.kibstrust.com/Storage/Support/Software/KIBSTrust-SAC-x64-10.8-R6.msi</u>

Notes:

This software package replaces the need for separate installation of minidriver and PKCS#11 library. <u>For Legacy</u>, those packages are still available on our web site <u>https://www.kibstrust.com/en-GB/Home/Support/</u>:

1. You can download the older version of minidiver from the section "Software & Drivers", part "Minidrivers for Gemalto ID Prime (.NET & MD) PKI tokens" 2. You can download the older version of PKCS#11 library, from the section "Software & Drivers", part "PKCS#11 Library for Gemalto ID Prime (.NET & MD) PKI tokens"

IMPORTANT: Before installation of SAC Client, you need to uninstall minidriver and PKCS#11 library!

To make a right choice of the middleware packet (32 or 64-bits), check the type of your computer's operating system by following the next procedure:

Click Start->Programs->Accessories->System Tools->System Information.

In the part: **OS name** is the information about the operating system version.

In the part: System Type, there is one of the following information:

- x86-based PC, for a 32-bit operating system
- x64-based PC, for a 64-bit operating system

Note: If you are our customer, you can obtain middleware software for Gemalto IDPrime PKI tokens for MAC and Linux Operation systems, after request via e-mail message to helpdesk@kibstrust.com.

2.2 Installation of middleware software on Windows operating system

Supported Windows operation systems for **SafeNet Authentication client** version 10.8 R6 are:

- Windows 11 (64-bit), Windows 10 (32-bit, 64-bit), Windows 8.1 (32-bit, 64-bit), Windows 8 (32-bit, 64-bit);
- Windows Server 2019 (64 bit), Windows Server 2016 (64 bit), Windows Server 2012 and 2012 R2 (64-bit), Windows Server 2008 R2 SP1 (32-bit, 64-bit), Windows Server 2008 SP2 (32-bit, 64-bit)

The installation process is very simple, following the screens and predefined values. The installation starts with double click of proper installation file (<u>32-bit</u> or <u>64-bit</u>), and proceeds by clicking the **Next** button (Figure 1).



Figure 1

On next window, leave the predefined interface language – English, do not select "Use the existing configuration settings" and then click **Next** (Figure 2):

🛃 SafeNet Authentication Client 10.8 R6 Setup 🛛 👋			
Interface Language Select the interface language.		THALES	
Select the SafeNet Authentication (English Setup has detected existing conf	Client 10.8 R6 interface	language:	
InstallShield	< <u>B</u> ack	Next > Cancel	

Figure 2

On the next window, select "I accept the terms in the license agreement", and then click **Next** (Figure 3):

餶 SafeNet Authentication Client 10.8 R6 Setup	×			
License Agreement Please read the following license agreement carefully. THALE	5			
THALES SOFTWARE LICENSE TERMS SafeNet Authentication Client	^			
Legal notice:				
Thales software is not sold; rather, copies of Thales software are licensed all the way through the distribution channel to the end user. UNLESS YOU HAVE ANOTHER AGREEMENT DIRECTLY WITH THALES THAT CONTROLS AND ALTERS YOUR USE OR DISTRIBUTION OF THE THALES SOFTWARE. THE TERMS				
● I <u>a</u> ccept the license agreement ○ I <u>d</u> o not accept the license agreement				
InstallShield				
< <u>B</u> ack <u>N</u> ext > Cancel				

Figure 3

Leave the predefined installation path and choose **Next** (Figure 4):

🖟 SafeNet	SafeNet Authentication Client 10.8 R6 Setup X					
Destinatio	on Folder					
Click N	leve to install to this folder, or click Change to THALES					
GICKIN						
Install to	o a different folder.					
	Install SafeNet Authentication Client 10.8 R6 to:					
	C:\Program Files\SafeNet\Authentication\					
InstallShield -						
	< Back Next > Cancel					

Figure 4

On next window (Figure 5), click Install:

😹 SafeNet Authentication Client 10.8 R6 Setup	×
The wizard is ready to begin installation.	THALES
Click Install to begin the installation.	
If you want to review or change any of your installa Click Cancel to exit the wizard.	tion settings, click Back.
InstallShield	
< <u>B</u> ack	€Install Cancel

Figure 5

103.18 How to start using a certificate issued on a Gemalto IDPrime PKI token? v.4.2

	🛃 SafeNet	Authentication Client 10.8 R6	Setup	_	
	Installing :	SafeNet Authentication Client	: 10.8 R6	тна	LES
	The pro	ogram teatures you selecte	ed are being installe	ed.	
	Please wait while the InstallShield Wizard ins Authentication Client 10.8 R6. This may take			nstalls SafeNet e several minu	tes.
		Status:			
		Starting services			
	InstallShield -				
			< <u>B</u> ack	<u>N</u> ext >	Cancel
Wait for installation process (

Figure 6):

🛃 SafeNet Authentication Client 10.8 R6 Setup — 🗆 🗙					
Installing S The pro	Installing SafeNet Authentication Client 10.8 R6 The program features you selected are being installed.				
17	Please wait while the Ins Authentication Client 10.	tallShield Wizard in 8 R6. This may take	stalls SafeN several mi	let nutes.	
	Status: Starting services				
InstallShield –					
		< <u>B</u> ack	Next >	Cano	el

Figure 6

When the installation is finished, chose **Finish** (Figure 7):



Figure 7

If you get the message like in Figure 8, restart the computer!

👘 Instal	记 Installer Information			
	You must restart your system for the to SafeNet Authentication Client 11 restart now or No if you plan to rest	e configuration changes made).7 to take effect. Click Yes to art manually later.		
	<u>Y</u> es	No		



IMPORTANT: The procedure of installing the middleware software described in part 2.2 should be repeated on each PC on which you intend to use the Gemalto IDPrime PKI token.

3. Check the content of the Gemalto IDPrime PKI token

After the installation of middleware software SAC, you will notice 💭 icon in the right down corner of

your screen. When you plug in your PKI token, the icon gets fulfilled red color: 🧟 . When you right click on the icon, you can see the following information about Your PKI token, like in Figure 9:

Tools
About
Change Token PIN
Certificate Information
Exit

Figure 9

If You choose "Certificate Information", You should get the Figure 10.

Under "User" type, the user certificate is shown.

Under "CA" type, the intermediate certificates are shown.

You can open certificates by double click and check their characteristics.

🤶 Token	S Token Certificate Information: Lile Gagovska X				
U	KIBS Trust	SafeNe	TH et Authentica	ALES ation Client	
Type Type CA CA CA	Issued To Lile Gagovska Baltimore CyberTrust Root KIBSTrust Issuing CA for e-Signatures	Status Valid Valid Valid	Serial Number 25597FE4CDC 020000B9 0F5F12D3FC3	Container name p11#5ff477db6	
۲.				>	
Log Or	Log On Close				

Figure 10

4. Change of user PIN

You can change Your current PIN with right click on the icon ^{See}, where you can choose "Change Token PIN" and you can set new PIN, by entering current PIN, see Figure 11:

Change PIN: Lile Gagovska	×
	THALES SafeNet Authentication Client
Current Token PIN:	
New Token PIN:	
Confirm PIN:	
The new password must comply with	the quality settings defined on the token.
A secure password has at least 8 ch numerals, and special characters (su	aracters, and contains upper-case letters, lower-case letters, ich as !, \$, #, %).
Current Language: EN	
Enter your current password.	
	OK Cancel

Figure 11

You can reach the same "Change Token PIN" menu (Figure 11) trough right click on icon sthere the choose Tools, and (Figure 12**Error! Reference source not found.**) choose "Change Token PIN".

SafeNet Authentication Client Tools		- D X THALES SafeNet Authentication Client () 20 1 ? 🚖
Lile Gagovska SCMP	1	Rename Token
	****	Change Token PIN
	6	Unlock Token
	\otimes	Delete Token Content
	Q	View Token Info
		thalesgroup.com

Figure 12

5. Token information

With right click on icon \Re we choose "Tools"(Figure 11**Error! Reference source not found.**) then "View Token Info" and you will get your PKI token information, as shown on Figure 13.

🕵 Token Information: Lile Gagovs	ika	×
	st SafeNet Authentication Clier	5 nt
Token name	Lile Gagovska SCMP	^
Token category	Hardware	
Reader name	Generic EMV Smartcard Reader 0	
Serial number (PKCS#11)	0B41E1DA3DC5E199	
Free space (minimum estimated)	66108	
Card ID (GUID)	0x3DC0017936442A773DC0017936442A77	
Product name	IDPrime 940	
Card type	IDPrime	
Applet Version	IDPrime Java Applet 4.4.2.A	
Mask version	G286	
Token PIN	Present	
Token PIN retries remaining	5	
Maximum Token PIN retries	5	
Token PIN expiration	No expiration	
Administrator PIN	Present	
Administrator PIN retries remaining	5	
Maximum administrator PIN retries	5	
FIPS	N/A	
Common Criteria (CC)	CC EAL5+ / PP QSCD	
Token unlock objects	Administrator	¥
	Сору ОК	

Figure 13

6. How to check if the certificate from my Gemalto IDPrime PKI token is shown in Internet Explorer?

6.1 How to check if the certificate is shown in Internet Explorer

You need to insert the Gemalto IDPrime PKI token in the PC, which has the SAC middleware software installed, according to part 2.2 of this user manual.

Open the web browser Internet Explorer and from the menu, choose **Tools** ->**Internet Options** (Figure 14)





In the new window, choose the **Content** tab and click on **Certificates** (Figure 15).



Figure 15

Your certificate should be in **Personal** tab (Figure 16).

nueu p	urpose:	<ai< th=""><th>></th><th></th><th></th><th></th><th></th></ai<>	>				
ersonal	Other Peo	ple	Intermedia	ate Certification Authorities	Trusted Roo	t Certification	•
Issued	То			Issued By		Expiratio	^
ime Ime	PKIToken Pr	rezime	PKIToken	KIBSTrust Issuing CA for	e-Signatures	05.9.2021	
							~
<						>	~
<						>	~
<	<u>E</u> x	port.		Remove	_	> <u>A</u> dvan	v
< (mport		port.	. ses	<u>R</u> emove	_	> <u>A</u> dvan	v
< (mport ertificati	Ex	port.	 ses	<u>R</u> emove	_	> <u>A</u> dvan	v
< (mport ertificati	<u>Ex</u> e intended p thentication,	port. ourpo , Secu	ses ure Email	<u>R</u> emove		<u>A</u> dvan	×

Figure 16

When double-click on the certificate you should get a preview like on Figure 17, which shows information regarding the certificate.

🛒 Certificate	×
General Details Certification Path	
Certificate Information	
This certificate is intended for the following purpose(s): • Proves your identity to a remote computer • 0.4.0.194112.1.2 • 0.4.0.2042.1.2	
* Refer to the certification authority's statement for details. Issued to: ImePKIToken PrezimePKIToken	
Issued by: KIBSTrust Issuing CA for e-Signatures	
Valid from 04.9.2020 to 05.9.2021 P You have a private key that corresponds to this certificate.	
Issuer <u>S</u> tatement]
OK	

Figure 17

After that, check the **Certification Path**. There are two possible previews:

1. If the preview is like on Figure 18 all the settings for the certificate are OK and it is ready for use.

103.18 How to start using a certificate issued on a Gemalto IDPrime PKI token? v.4.2

🐖 Certificate	×
General Details Certification Path	
Certification path	s KIBS AD Skopje ID
	View Certificate
Certificate status:	
This certificate is OK.	
	ОК

Figure 18

2. If the preview is like on Figure 19 (only the name and surname are shown) or only one root certificates is shown, **you must continue with part 6.2.**

Certificate	×
General Details Certification Path	
Certification gath	
Certificate status: This certificate is OK.	View Certificate
	ОК

Figure 19

6.2 Installation of root certificates in Internet Explorer

If some of KIBSTrust root certificates is missing in the certificate chain, you can download them from section **Root certificates** from <u>https://www.kibstrust.com/en-GB/Home/Support/ and</u> please install them:

<u>KIBSTrust Root CA G2</u> (install in Trusted Root Certficate Authorities) <u>KIBSTrust Issuing Qsig CA G2</u> (install in Intermediate Certificate Authorities)

After importing the two root certificates, make sure you get a preview as in one of the pictures in Figure 18!

The installation is described in one of the FAQ on the following link: <u>https://www.kibstrust.com/en-GB/Home/Support</u> "How to install root certificates in Internet Explorer".

7. Does my certificate from the Gemalto IDPrime PKI token is shown in Google Chrome?

7.1 Check if the certificate is shown in Google Chrome

Gemalto IDPrime PKI should be inserted in the computer where the middleware software is installed, according 2.2 from this manual.

Open Google Chrome, then Settings, Privacy and Security, Security, Manage Certificates. Open User Certificate store, as is open in Internet Explorer.

8. How to check if the certificate from my Gemalto IDPrime PKI token is shown in Mozilla Firefox?

8.1 Adding a Gemalto IDPrime PKI token as a security device

To access the certificate issued on Gemalto IDPrime PKI token, in Mozilla Firefox, beside the installation of middleware software, you need to add proper security device.

From the browser menu click on the right upper button and select **Options** (Error! Reference source not found.Figure 20):



Figure 20

In the new tab select the **Privacy & Security** option from the menu on the left side, go down and click on the **Security Devices** button (Figure 21)



Figure 21

In the next window click Load (Figure 22)

	Devi	ce Manager	
Convity Madulas and Davisos	Dataile	Mahan	
Security Modules and Devices	Details	value	Log I <u>n</u>
VNSS Internal PKCS #11 Module Generic Crypto Services			Log <u>O</u> ut
Software Security Device			Change Password
Builtin Roots Module			Load
			Unload
			Enable EIPS
			ОК



In the new window, in the field **Module Name** enter "Gemalto IDPrime" and click **Browse** (Figure 23) in order to find the required file.



Figure 23

- C:\Program Files (x86)\Gemalto\IDGo 800 PKCS#11 (for 64-bit OS), or
- C:\Program Files\Gemalto\IDGo 800 PKCS#11 (for 64-bit OS).

Select the file **IDPrimePKCS11.dll** for 32-bit version of Mozilla Firefox (or IDPrimePKCS1164.dll for 64-bit version) and click **Open** (Figure 24) and then click **OK** (Figure 25).

🥑 Choose a PKCS#11 devic	e to load			>
← → 🗸 🛧 📙 C:\P	rogram Files (x86)\Gemalto\IDGo 800 PKCS#11	~ Ū	Search IDGo 800 PKCS#11	م
Organize 🔻 New fold	er			
🔮 Documents 🔦	Name	Date modified	Туре	Size
🕂 Downloads	IDPrimePKCS11.dll	12.12.2013 10:50	Application extens	1.98
♪ Music E Pictures	lDPrimePKCS1164.dll	12.12.2013 10:50	Application extens	2.50
📳 Videos 🏪 Local Disk (C:)				
🕳 New Volume (E:) 🗸	<			
File r	ame: IDPrimePKCS11.dll	~	All Files (*.*)	~
			Open C	ancel
	Figure 24			
	Load PKCS#11 Device	—	×	
	Enter the information for the module	you want to add.		
	Module Name: Gemalto IDPrime			
	Module <u>filename</u> : C:\Program Files	(x86)\ <u>B</u> rowse		
	ок	Cancel		



Your PKI token Gemalto IDPrime is now shown in the list on the left side of the window (Figure 26)

		C 4, Search	н		•	*	0
	Device	a Manager					
Security Modules and Devices	Details	Value			Log	a la	
×NSS Internal PRCS #11 Module					Log	Qut	
Generic Crypto Services				0	inne i		ed.
Software Security Device							
ime prezime					To.	ad	
Builtin Roots Module					<u>U</u> ni	oad	
Builtin Object Token					Enable	e <u>E</u> IPS	

Figure 26

Click **OK** two times to close the window.

8.2 How to check if the certificate from the Gemalto IDPrime PKI token is shown in Mozilla Firefox?

The Gemalto IDPrime PKI token should be inserted in the PC. Open the web browser Mozilla Firefox, click on the right upper button, and select **Options**, select the **Privacy & Security** option from the menu on the left side, then click on the button **View Certificates** (Figure 27).



Figure 27

In the next window (Figure 28) a password is required, **DO NOT ENTER ANYNOTHING**, just click OK or Cancel:



Figure 28

Your personal certificate is located in Your Certificates (Figure 29)

103.18 How to start using a certificate issued on a Gemalto IDPrime PKI token? v.4.2

		Cer	tificate M	anager			
Your Certifica	ites Peo	ple	Servers	Authori	ties		
/ou have certific	ates from the	ese orga	nizations	that identify	you		
Certificate Nar	me Se	curity De	evice	Serial Num	ber	Expires On	C‡
~ KIBS AD Skop	oje						
Ime Prezime	e Ime	Prezime		00:A2:0F:F0:	1F:FF:D N	londay, Dece	em
<u>⊻</u> iew	<u>B</u> ackup	Bac <u>k</u> u	ıp All	I <u>m</u> port	<u>D</u> elete	_	Or

Figure 29

8.3 How to install root certificates in Mozilla Firefox?

Save locally root certificate's files from:

KIBSTrust Root CA G2

KIBSTrust Issuing Qsig CA G2,

Than you can go to Options, Privacy & Security, View Certificates, Authorities chose Import and browse to local path where you have saved the certificates and import them one by one.

The installation of root certificates more detailed is described in one of the FAQ on the following link <u>https://www.kibstrust.com/en-GB/Home/Support</u> "How to install root certificates in Mozilla Firefox?"
