

Manual pentru Instalarea Certificatului Digital Calificat DigiSign

Versiunea 2.1

În vederea folosirii corespunzătoare a certificatului digital calificat emis de DigiSign, vă rugăm să urmați instrucțiunile din acest manual.

Nerespectarea acestor specificații sau utilizarea altor opțiuni din aplicație decât cele indicate în manual pot duce la întarzierea folosirii cu succes a certificatului digital sau la pierderea acestuia.

În continuare, vă este prezentat un exemplu de instalare a certificatului pe sistemul de operare Windows 7. Imaginile pot fi diferite în cazul altor versiuni de Windows, însă pașii sunt aceiași.

Atenție: În cazul în care ați <u>reînnoit</u> certificatul digital, iar aplicațiile sunt deja instalate pe calculator, vă rugăm <u>să reinstalați doar lanțul de incredere</u> de la punctul **2. a)** (pag. 2).

1. Asigurați-vă că sistemul dumneavoastră de operare este actualizat la zi și că nu aveți vreun program de tip antivirus/firewall ce ar putea bloca instalarea corespunzătoare a driver-ului dispozitivului USB Aladdin eToken PRO.

Folosiți funcția **Windows Update** sau urmați procedurile de pe site-ul Microsoft în vederea instalării ultimelor update-uri aferente sistemului dumneavoastra de operare și a browser-ului Internet Explorer.

Asigurați-vă că:

- aveți drept de administrator pe sistemul pe care doriți să instalați certificatul digital
- ceasul, data și fusul orar de pe calculator sunt corect setate
- dispozitivul e-token NU este conectat în extensia USB a calculatorului pe durata procesului de instalare al aplicațiilor!



2. Instalarea aplicațiilor necesare utilizării dispozitivului e-Token și a certificatului digital calificat.

Pentru a putea folosi dispozitivul securizat Aladdin e-Token pe care se află certificatul digital calificat (utilizat pentru crearea semnăturii electronice extinse), trebuie să instalați **lanțul de încredere DigiSign**, precum și **driverul DigiSign e-Token PKI Client 8 al dispozitivului dvs Aladdin PRO.**

a) Instalarea lanțului de încredere DigiSign

- > Accesați <u>http://www.digisign.ro/uploads/cert.zip</u> și salvați lanțul de încredere în calculatorul dvs.
- Deschideți arhiva *cert.zip* pe care ați descărcat-o și dezarhivați-o (click-dreapta -> *Extract Here* sau dublu-click -> *Extract To*). În acest moment, ați extras executabilul *cert.exe*.
- Dacă folosiți sistemul de operare <u>Windows 7</u> sau <u>Windows 8</u>, instalați lanțul de încredere prin click-dreapta pe executabilul cert.exe și Run as Administrator. Dacă folosiți sistemul de operare <u>Windows XP</u>, instalați lanțul de încredere prin dublu-click pe executabil.





> Vi se va deschide utilitarul de importare a certificatelor DigiSign. Apăsați butonul Install.



IMPORTANT: Asigurați-vă că lanțul de încredere a fost instalat cu success!

Într-o fereastră asemănătoare cu cea prezentată în imaginea de mai jos, va fi afișat mesajul "CertMgr Succeeded" atunci când lanțul de incredere a fost instalat cu succes.



Dacă primiți mesajul **CertMgr Failed**, va trebui să dați *click-dreapta* pe fișierul *cert.exe* și să selectați opțiunea *"Run as Administrator"* (!).



În continuare, apăsați butonul <u>Next</u>, iar în următoarea fereastră, lăsați câmpul •Automatically... bifat și alegeți butonul <u>Next</u>.

Certificate Import Wizard	X	Certificate Import Wizard
	Welcome to the Certificate Import Wizard	Certificate Store Certificate stores are system areas where certificates are kept.
	This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store. A certificate, which is issued by a certification authority, is	Windows can automatically select a certificate store, or you can specify a location for the certificate. @ Automatically select the certificate store based on the type of certificate
	 a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept. 	Place all certificates in the following store Certificate store: Prowse Prowse
	To continue, click Next.	
		Learn more about certificate stores
	< Back Next > Cancel	< Back Next > Cancel

> Importarea certificatului a fost făcută cu success, apăsați butonul <u>Finish</u>, iar apoi <u>OK</u>.

Completing th Wizard The certificate will be in	e Certificate Import
Certificate Store Selec Content File Name	cted Automatically determined by t PKCS #7 Certificates DigiSign-1.p7b
•	···· →
< Ba	ck Finish Cancel







b) Instalarea driver-ului DigiSign e-Token PKI Client 8

Compatibilitate: Windows XP, Windows Vista, Windows 7, Windows 8, Windows Server 2003, Windows Server 2008, Windows Server 2012.

Vă rugăm să alegeți driverul în funcție de versiunea sistemului de operare folosit:

- ✓ 32 biti : <u>http://www.digisign.ro/uploads/DigiSign_eToken_PKI_Client_x32.msi</u>
- ✓ 64 biti : <u>http://www.digisign.ro/uploads/DigiSign_eToken_PKI_Client_x64.msi</u>

IMPORTANT: Înainte de a instala driver-ul, asigurați-vă că dispozitivul e-Token NU este conectat în portul USB al calculatorului dvs.

Selectați fișierul descărcat; în cazul în care folosiți sistemul de operare <u>Windows 7</u> sau <u>Windows</u> <u>B</u>, prin *click-dreapta* apăsați butonul **Run as administrator**, iar în cazul în care folosiți <u>Windows</u> <u>XP</u>, apăsați *dublu-click*. Apăsați butonul <u>Run</u>.





 Str. Virgil Madgearu nr. 2-6, București, Sector 1, 014135, Tel: 031 620 12 84, Fax: 031 620 12 91, office@digisign.ro

 www.digisign.ro

 SEMNATURA ELECTRONICA | CERTIFICATE DE SERVER | MARCARE TEMPORALA



În fereastra deschisă, apăsați butonul <u>Next</u> pentru a începe procesul instalării, selectați limba dorită și <u>Next</u>.

送 SafeNet	Authentication Client 8.2_01 Setup 🛛 – 🗖 💌	SafeNet Auth	entication Client 8.2_01 Setup 🛛 – 🗖 💌
SafeNet Authentication	Welcome to the SafeNet Authentication Client 8.2_01 Installation Wizard	Interface Language Select the interface language.	SafeNet
Client	The Setup wizard will install SafeNet Authentication Client 8.2_01 on your computer.	Calabelia Catalia A dia dia	
3 · · ·	It is strongly recommended that you close all Windows programs before running the Setup wizard.	English	ation client 6.2_01 interface language.
0 4 5 6 9 6	Click Next to continue.		
	GafeNet		
	Next > Cancel		< Back Next > Cancel

Bifați câmpul •I accept the license agreement, apăsați butonul <u>Next</u>, iar în următoarea fereastră lăsați bifat tipul *Standard* și continuați alegând buntonul <u>Next</u>.

🖞 SafeNet Authentication Client 8.2_01 Setup 🗧 🗆 🔀	🛃 SafeNet Authentication Client 8.2_01 Setup 😑 🗵 🗙
License Agreement Please read the following license agreement carefully.	Installation Type Select the installation type.
SAFENET SOFTWARE LICENSE TERMS ^ SafeNet Authentication Client ^ Legal notice:	Standard Standard installation Includes new implementation and user interface for all eT oken and iKey tokens. BSec-compatible Legacy BSec-compatible installation Includes new implementation and user interface for all eT oken and iKey tokens.
CONTROLS AND ALTERS YOUR USE OR DISTRIBUTION OF THE SAFENET SOFTWARE, THE TERMS AND CONDITIONS OF THE APPLICABLE LICENSE AGREEMENTS BELOW APPLY TO YOU. Please read the agreement	<pre>c Back Next > Cancel</pre>

Virginitation Virginitation Registered Partner Virginitation Virginitation Virginitation Str. Virginitation Virginitation Vir	RIA 1 620 12 91, office@digisign.ro WER MARCARE TEMPORALA Instalarea driver-ului.
BafeNet Authentication Client 8.2_01 Setup -	😼 SafeNet Authentication Client 8.2_01 Setup 😑 🖂 🗙
Destination Folder Select a folder in which the application will be installed. Setup will install the files for SafeNet Authentication Client 8.2_01 in the following folder. To install in a different folder, click Browse, and select another folder. Destination Folder C:\Program Files\SafeNet\Authentication\	SafeNet Authentication Client Click Finish to exit Setup.
	(SafeNet
< Back Next > Cancel	Finish

3. Verificarea instalării corespunzătoare a aplicațiilor

a) Verificarea instalării corespunzătoare a lanțului de încredere DigiSign

Alegeți **una** dintre variantele de mai jos pentru a verifica instalarea cu succes a lanțului de încredere DigiSign. Dacă observați că certificatele de mai jos **nu se regăsesc** în aplicațiile de pe calculatorul utilizat, va trebui să repetați procesul de instalare al lanțului de încredere prezentat la punctul 2. a) (pag.2) al acestui document.



Str. Virgil Madgearu nr. 2-6, București, Sector 1, 014135, Tel: 031 620 12 84, Fax: 031 620 12 91, office@digisign.ro
www.digisign.ro
SEMNATURA ELECTRONICA | CERTIFICATE DE SERVER | MARCARE TEMPORALA

1. Folosind browserul Internet Explorer

S

А

• Deschideți browserul Internet Explorer. Din meniul Tools selectați \rightarrow Internet Options \rightarrow Content \rightarrow Certificates \rightarrow Intermediate Certification Authorities

În lista respectivă ar trebui să apară certificatul: *DigiSign Qualified Public CA* și *DigiSign Qualified Root CA v2* dacă instalarea lanțului de încredere a fost facută corespunzător.

• Deschideti browserul Internet Explorer. Din meniul Tools selectati \rightarrow Internet Options \rightarrow Content \rightarrow Certificates \rightarrow Trusted Root Certification Authorities

In lista respectiva ar trebui sa apara certificatul: *DigiSign Qualified Root CA v2* dacă instalarea lanțului de încredere a fost facută corespunzător.

2. Folosind utilitarul Certificate Manager

Din meniul **Start** al **Windows**-ului alegeți opțiunea <u>**Run.**</u> Tastați *certmgr.msc* și apăsați butonul **OK**.

• Selectați Certificates–Current User \rightarrow Trusted Root Certification Authorities \rightarrow Certificates. În lista din dreapta ar trebui să apară un certificat DigiSign: *DigiSign Qualified Root CA v2* dacă instalarea lanțului de încredere a fost facută corespunzător.

• Certificates–Current User \rightarrow Intermediate Certification Authorities \rightarrow Certificates. În lista din dreapta ar trebui să apară un certificat DigiSign: *DigiSign Qualified Public CA* și *DigiSign Qualified Root CA* v2 dacă instalarea lanțului de încredere a fost facută corespunzător.

🕨 🧼 🖄 📰 🖌 🛍 🗶 🖻			
Certificates - Current User Personal Certificates Cert	Issued To AddTrust External CA Root America Online Root Certificati Baltimore CyberTrust Root Class 3 Public Primary Certificat Copyright (c) 1997 Microsoft Ca DigiCert Assured ID Root CA DigiCert High Assurance EV Ro	Issued By AddTrust External CA Root America Online Root Certification Baltimore CyberTrust Root Class 3 Public Primary Certificatio Copyright (c) 1997 Microsoft Corp. DigiCert Assured ID Root CA DigiCert High Assurance EV Root	Expiration Di 5/30/2020 11/19/2037 5/13/2025 8/2/2028 1/8/2004 12/31/1999 11/10/2031 11/10/2031
Crimit of the people Client Authentication Issuers Other People Certificate Enrollment Requee Smart Card Trusted Roots	DigiSign Qualified Root CA v2 DT Soft Ltd Furthrust.net Secure Server Certifi Equifax Secure Certificate Auth GeoTrust Global CA GlobalSign Root CA Go Daddy Class 2 Certification GET CyberTrust Global Root	DigiSign Qualified Root CA v2 VeriSign Class 3 Code Signing 200 Entrust.net Secure Server Certifica Equifax Secure Certificate Authority GeoTrust Global CA GlobalSign Root CA Go Daddy Class 2 Certification Au GTE CyberTrust Global Root	12/9/2031 11/4/2012 5/25/2019 8/22/2018 5/21/2022 1/28/2028 6/29/2034 8/14/2018

Þ 🔿 🚾 🔏 🖬 🗙 🖻			
Certificates - Current User Personal Trusted Root Certification Author Enterprise Trust Intermediate Certification Author Certificates Revocation List Certificates Active Directory User Object Trusted Publishers Untrusted Certificates Third-Party Root Certification A Trusted People Client Authentication Issuers Other People Certificate Farollment Requests	Issued To COMODO High-Assurance Sec DigiCert High Assurance CA-3 DigiSign DEMO CA DigiSign Qualified Public CA DigiSign Qualified Root CA v2 Go Daddy Secure Certification GiGCTI Certification Authority GiGCTI Class 1 Extended Certifica GiGCTI Root Certification Author Microsoft Internet Authority Microsoft Secure Server Authori Microsoft Windows Hardware RapidSIC CA	Issued By AddTrust External CA Root DigiCert High Assurance EV Root DigiSign Qualified Root CA v2 DigiSign Qualified Root CA v2 DigiSign Qualified Root CA v2 Go Daddy Class 2 Certification Au IGCTI Root Certification Authority IGCTI Certification Authority IGCTI Certification Authority GTE CyberTrust Global Root Microsoft Internet Authority Microsoft Root Authority	Expiration D. 4 5/30/2020 4/3/2022 3/5/2015 12/9/2021 12/9/2031 11/16/2026 9/15/2017 9/2/2016 9/5/2031 4/14/2018 5/20/2014 12/31/2002
Smart Card Trusted Roots	Root Agency Symantec Class 2 Employee Em	Root Agency VeriSign Class 2 Public Primary Ce	1/1/2040 2/24/2016
	Thawte SGC CA - G2	VeriSign Class 3 Public Primary Ce	7/29/2020



- b) Verificarea instalării corespunzătoare a driver-ului DigiSign e-Token PKI Client 8.1
- ✓ Din meniul Start, alegeți All Programs → SafeNet → SafeNet Authentication Client → SafeNet Authentication Tools.



✓ Dacă utilitarul a fost instalat cu succes, vi se va afișa fereastra din imaginea următoare:

SafeNet Authentication Client Tools				-		X
		0	S	1	?	
	/	Rename	Token			
	****	Change Toker Unlock 1	n Password Token			
	\otimes	Delete Toker View Token Ir	n Content			
	Dis.	connect SafeNe	et eToken Virtu	Jal		
				www.sa	fenet-inc	.com

În acest moment, lanțul de încredere DigiSign și driverul sunt corect instalate !



4. Folosirea utilitarului DigiSign e-Token PKI Client 8.1

- > Introduceți dispozitivul e-Token în extensia USB a calculatorului.
- > Din meniul Start, alegeți All Programs \rightarrow SafeNet \rightarrow SafeNet Authentication Client \rightarrow SafeNet Authentication Tools.
- > Pe ecran se va afișa **Panoul de comandă** al utilitarului Aladdin e-Token:

SafeNet Authentication Client Tools		• • • • • • • • • • • • • • • • • • •	
CONFIRMARE	Rename Token **** Change Token Password Unlock Token O Delete Token Content		Functie optionala de redenumirea a dispozitivului eToken Functie recomandata pentru schimbarea
	View Token Information Disconnect SafeNet eToken Virtual	nc.com	parolei dispozitivului dvs e-Token



a) Rename e-Token (funcția de redenumire a dispozitivului e-Token)

Această funcție este opțională și permite utilizatorului să schimbe numele dispozitivului (pentru personalizare). Numele inițial al dispozitivului dvs este *eToken*.

ne Token

În fereastra care se va deschide, introduceți parola dispozitivului dvs și apăsați OK.

Token Logon	
Enter the Token Password.	
Token Name:	eToken
Token Password:	Aici introduceți parola dispozitivului dvs
	Current Language: EN
	OK Cancel

> În câmpul New token name, introduceți denumirea personalizată dorită și apăsați OK.

	SIGN
New token name:	Aici introduceti numele dorit
	Current Language: EN
Use this name to identify your	r token.



b) Change Password (funcția de schimbare a parolei dispozitivului e-Token)

Această funcție este recomandată și permite utilizatorului să schimbe parola dispozitivului.

Dacă optați pentru schimbarea parolei inițiale, vă rugăm să luați în considerație faptul că driver-ul nu păstrează un istoric al parolelor. Prin urmare, odată schimbată parola inițială, noua parolă devine responsabilitatea dvs.

IMPORTANT (!):

• În cazul în care parola este introdusă greșit de mai mult de 15 ori consecutiv, dispozitivul se va bloca. <u>NU EXISTĂ</u> posibilitatea de deblocare a acestuia.

- > Apăsați butonul **** Change Token Password
- În fereastra deschisă, scrieți parola actuală în primul câmp, iar în următoarele doua câmpuri scrieți parola nouă și apăsați butonul OK.

Change Password: eToken		
	SIGN	
Current Token Password:	Aici introduceți parola actuală	
New Token Password:	Aici introduceți noua parolă	
Confirm Password:	Rescrieți noua parolă	
The new Password must com	ply with the quality settings defined on the	token.
A secure Password has at lea numerals, and special charact	st 8 characters, and contains upper-case l ers (such as !, \$, #, %).	etters, lower-case letters,
Current Language: EN		
Enter a Password.		
		OK Cancel

În acest moment, parola a fost schimbată cu succes, iar driverul este configurat corect; nu mai sunt necesare alte operații în aplicație și certificatul poate fi utilizat.



Str. Virgil Madgearu nr. 2-6, București, Sector 1, 014135, Tel: 031 620 12 84, Fax: 031 620 12 91, office@diglsgn.ro www.digisign.ro SEMNATURA ELECTRONICA | CERTIFICATE DE SERVER | MARCARE TEMPORALA

Activarea/dezactivarea modulului e-Token în browser-ul Mozilla Firefox

Activarea modulului e-Token în browser-ul Mozilla Firefox este **strict opțională** și recomandată doar în cazul în care doriți să vă logați pe anumite portale cu acest browser sau să completați formularul de reînnoire online a certificatului digital calificat care poate fi accesat la adresa <u>portal.digisign.ro</u>.

- 1. Activarea modulului e-Token
 - > Deschideți browser-ul Mozilla Firefox, accesați:

 $\textit{Options} \rightarrow \textit{Advanced} \rightarrow \textit{Encryption} \rightarrow \textit{Security Devices}$

- > În noua fereastră deschisă, apăsați butonul Load, selectați din calculatorul dvs prin butonul Browse fișierul eTPKCS11.dll (gasit în directorul Windows → system32).
- > Apăsați butonul OK, iar modulul eToken se va activa în browser.

Options						X
	-		00		O	{Ô};
General Tabs	Content	Applications	Privacy	Security	Sync	Advanced
General Network U	odate Encry	/ption				
Protocols						
Vse SSL <u>3</u> .0		✓ Use TLS <u>1</u> .0				
Certificates						
When a server rec	juests my pe	rsonal certificat	e:			
Select one au	tomatically	Ask me ev	ery t <u>i</u> me			
View Certificates	Revoca	tion Lists	alidation	Security	Devices	
			014			
			UK	Cance		Неір

IGISIGN

IMPORTANT:

Dacă aveți introdus în calculator dispozitivul dvs e-Token și deschideți browser-ul Mozilla Firefox, iar acesta vă afișează o fereastră de tipul celei de mai jos, va trebui să introduceți parola dispozitivului dvs eToken.







- 2. Dezactivarea modulului e-Token
 - > Deconectați dispozitivul dvs e-token din calculator
 - > Deschideți browser-ul Mozilla Firefox, accesați meniul:

Options \rightarrow *Advanced* \rightarrow *Encryption* \rightarrow *Security Devices*

- În noua fereastră deschisă, selectați câmpul: · numele dispozitivul dvs e-Token Sau
 · "New PKCS#11 Module"
- > Apăsați butonul **Unload** și apăsați butonul OK.

Security Modules and Devices	Details	Value	Log I <u>n</u>
ANSS Internal PKCS #11 Module Generic Crypto Services	Module Path	New PKCS#11 Module C:\Windows\System3	Log <u>O</u> ut
Software Security Device			Change Password
ANew PKCS#11 Module			
eToken			Load
Rainbow Tec Confirm	-	×	Unload
Unnamed Sic Unnamed Sic Unnamed Sic Unnamed Sic	u sure you want to del	ete this security module? ancel	Enable <u>FI</u> PS
Unnamed Slot			
Builtin Roots Module			
Builtin Object Token			

În acest moment, modulul e-Token din browser-ul Mozilla Firefox este dezactivat.



S.C. DigiSign S.A. eliberează certificate digitale calificate conform Legii 455/2001(Legea semnaturii electronice). Aceste certificate calificate pot fi utilizate în mai multe sisteme (de exemplu: **ANAF, CNVM, ONRC, CSSPP, AEGRM, CSA-CEDAM, SEAP**), unde S.C.DigiSign S.A. nu este operator și nu are posibilitatea de a vă acorda consultanță/sprijin pentru utilizarea facilităților acestor sisteme care aparțin unor instituții ale statului. Pentru a beneficia de accesul în aceste sisteme, precum și modalitatea de utilizare a certificatului digital calificat obținut în cadrul acestora, vă rugăm să contactați administratorii respectivelor sisteme.

Link-uri utile:

- > Instalare și configurare Semnătură Electronică pentru Microsoft Office 2007
- > Instalare și configurare Semnătură Electronică pentru Microsoft Outlook 2007
- > Instalare și configurare Semnătură Electronică pentru Mozzila Thunderbird 3.0.1
- Instalare și configurare Semnătură Electronică pentru Outlook Express 6
- > <u>Instrucțiuni completare fișier de confirmare</u>
- Instrucțiuni depunere declarații on-line ANAF
- Download Adobe Acrobat Reader 8.2

Tutoriale video:

- Înstalarea certificatului digital tutorial video
- Înregistrarea certificatului digital la ANAF tutorial video