

I.CA SecureStore User guide

Version 7.1.2 and higher

První certifikační autorita, a.s.

Version 7.18, 18.7.2024

Contents

1.	Introduction	3
2.	Card access data	3
	2.1 Card initialization	3
3.	Main screen	4
	3.1 Switching between application language	4
	3.2 Version of the I.CA SecureStore	4
	3.3 Settings	5
	3.4 Diagnostic Tools	9
	3.5 Selecting smart card reader	. 10
	3.6 Toolbar	. 10
	3.7 Changing PIN	. 11
4.	Display key pair information	. 12
	4.1 Deleting a public key	. 13
	4.2 Removing the container	. 14
	4.3 Deleting a container using the key removal wizard	. 15
5.	Certificates	. 17
	5.1 Displaying the certificate	. 17
	5.2 Working with a personal certificate	. 17
	5.3. Using CA Root Certificate	. 19
	5.4. Registering Personal Certificate in Windows	. 20
6.	Personal Repository	. 21
7.	Application control	. 23
	7.1 Toolbar for card information	. 23
	7.2 Toolbar for Personal certificates folder	. 24
	7.2.1 Create certificate request	. 25
	7.2.2. Importing a personal certificate	. 31
	7.2.3 Importing a key pair from a backup (PKCS#8) and importing keys (PKCS#12)	. 32
	7.2.4 Set the certificate as the default for logging into Windows	. 32
8.	Definitions	. 33



1. Introduction

This User guide applies to the application I.CA SecureStore, Version 7.1.2 and higher. The specified versions have the same function and identical user interface.

2. Card access data

STARCOS 3.0

Smart card access is PIN-protected as is with payment cards, for example. PIN is a number of 4–8 digits. PIN will be automatically disabled if a wrong PIN is entered three times in a row. The user needs PUK to have his PIN re-enabled. PUK is a number of 4–8 digits. Entering a wrong PUK 5 times in a row will disable the PUK and thus also the smart card.

STARCOS 3.5

Smart card access is PIN-protected as is with payment cards, for example. PIN is a number of 6–8 digits. PIN will be automatically disabled if a wrong PIN is entered three times in a row. PUK is a number of 6–8 digits. Entering a wrong PUK 5 times in a row will disable the PUK and thus also the smart card. **Re-enabling PIN using PUK is limited to 6 attempts.**

STARCOS 3.7

Smart card access is PIN-protected as is with payment cards, for example. PIN is a number of 6–8 digits. PIN will be automatically disabled if a wrong PIN is entered three times in a row. PUK is a number of 8 digits. Entering a wrong PUK 5 times in a row will disable the PUK and thus also the smart card. **Re-enabling PIN using PUK is limited to 10 attempts.**

The card's segment named Secure Personal Storage is designed for storing any kind of data. This segment is protected with a special PIN, a secure storage PIN. Use the PUK referred to in the previous paragraph to re-enable the secure storage PIN. The secure storage PIN is a number of 6–8 digits.

2.1 Card initialization

Card initialization means setting a PIN and a PUK. If the user has received the PIN envelope, the card has been initialized already and the PIN and the PUK are enclosed in the envelope. If the PIN envelope has not been received, setting PIN and PUK is required in the first use of the card. The card initialization dialogue is displayed automatically, usually in launching the application with a new smart card for the first time. Please make sure you remember your PIN and PUK

3. Main screen

Fig. 1 – Main screen

	Settings	Diagno	stics				_	- 6	3	×
1. choose object				į	2. personal ce	ertificate detail				
Personal certificates		c	REATE CERTIFICATE	CERTIFICATI	KEY PAIR	KEY REMOVAL WIZARD				
🕭 Partner certificates			REQUEST IMPORT IMPORT							_
Certificate authority certificates			certificate ty	pe standa	ard certificate					_
Personal repository			issued f	or CN=To C=CZ	máš Kout					
Protected personal repository				O=První certifikační autorita, a.s. GN=Tomáš						
Card information			organizationIdentifier=NTRCZ-26439395							
Tomáš Kout, 22.04.2	024		issuer CN=I.CA Public CA/RSA 06/2022 O=První certifikační autorita, a.s.							
SC Tomáš Kout	:			organizationIdentmer=NTRC2-26439395 C=CZ						
💛 — 🔄 QC Tomáš Kou	t		validi	ty from 2	2.04.2024 8:00:33 to 2	2.04.2025 8:00:33				_
—— 🔍 SC key pair			serial number 3202F5 (hex)					-		
🖳 🔍 QC key pair			3277557 (dec)							_
Tomáš Kout, 24.10.2023				DELETE	MARK AS INITIAL		s			
SC Tomáš Kout							<u></u>	CER	LIFICATI	ON
Select a personal certificate, a k	ey pair or a container							- AUT	HORI	ΓY

The main screen is divided into two parts. The left part of the screen displays a list of objects stored on the smart card. The right part of the screen displays the individual details of the object on the smart card. The top bar shows the following options – see Fig. 2.

3.1 Switching between application languages

Click the pertinent flag in the right bottom corner to switch to a different language.

Fig. 2 – switching the language



Fig. 3 – Main bar



Click to display the application's version.





Fig. 4 – Application version

About application					
Application name I.CA Secur Version 7.1.2 Icons designed by Freepik (wv	eStore vw.flaticon.com)				
Copyright První certifikační autorita, a.:	s. 2014 - 2024 OK				

3.3 Settings

Use the Settings option to:

1) Adjust the keypad for entering PIN

Fig. 5 – PIN Keypad



By default, the application is set to "Random button placement on

virtual keyboard for PIN".

The user then enters the PIN on the virtual keyboard with the mouse cursor.



Fig. 6 - Keyboard for PIN entry.

PIN dialog X								
To process this enter PIN PIN:	operation, it is n	ecessary to						
6	7	3						
8	5	4						
2	1	0						
	9	<<<						
Ok Cancel								

The PIN keypad can be set to "Virtual PIN keypad", where the user can then

enters the PIN on the numeric keypad.

Fig. 7 - PIN entry keypad

PIN dialog				\times
To process the PIN:	is operatio	n, it is r	ecessary t	o enter PIN
	Ok		Cancel	



2) PIN CACHE - the time the PIN is stored in memory, by default the value is set to 0.

Fig.	8 -	· PIN	memorization	settings
------	-----	-------	--------------	----------

Settings										
PIN	PIN CACHE	LOG	UPDATE	OTHER						
		PIN C	ACHE							
PIN valid	PIN validity period (in minutes)									
other	0	- +	eSign	0 - +						
rememb	er PIN optior	n (checked /	unchecked)							
other		eSign								
confirm	use of saved	PIN								
other		eSign	\checkmark							
				CANCEL OK						

- a) PIN storage time (in minutes) setting the PIN storage time
- b) **The option to remember the PIN** (selected/not selected) the user can select a time period, for which the user wants to remember the PIN, the setting is separately for:
 - a. Other encryption and authentication keys
 - b. eSign signature keys

Note: The maximum time to remember the PIN for signature keys in eSign is 30 min, for encryption keys there is no time limit. Furthermore, the application allows PIN memorization in relation to the application process.

- c) Confirm the use of the stored PIN a function that allows you to activate the confirmation dialog that appears when the PIN is memorized and a key signature is created on the smart card. In this case, the user will be prompted whether he/she agrees to the use of the key and the creation of the signature
- d) Fig. 9 Confirmation dialogue

SecureStore	
Do you want to allow the application to use the PIN k	ey for a qualified signature?
	Ano Ne



3) **Enable logging** - enable application logging, for possible analysis of technical problem when using the smart card and the application. The application records the so-called audit log, when the latest audit log will be recorded in the audit log as part of the smart card operations. Security-sensitive operations performed, such as key deletion, key generation, etc.

The user can change the path to the saved log file using the button

Fig. 10 – Log

		Sett	ings					
PIN	PIN CACHE	LOG	UPDATE	OTHER				
		LC)G					
enable lo	ogging				\checkmark			
path to t	he log	ramData/I.CA	SecureStore/S	ecureStore.log				
	Open file location Clear log View log							
				CANCE	L OK			

4) **Updates** - the settings can be used to enable/disable online updating of the application. If a new version is released, the user is informed about the new version whenever the application is launched.



Fig. 11 - Application update settings

		Sett	ings		
PIN	PIN CACHE	LOG	UPDATE	OTHER	
		UPD	ATE		
enable p	rogram upda	tes			\checkmark
				CANC	CEL OK

3.4 Diagnostic Tools

I.CA SecureStore includes diagnostic tools to check the status of the CSP providers (cryptographic service providers) registered in MS Windows.

Fig. 12 – Diagnostic Tools

Secure Store Settings			gnostics						-		×
1. choose	e object				2. pe	ersonal ce	ertificate de	tail			
🛃 Personal certi	ificates		CREATE CERTIFIC	REATE CERTIFICATE CERTIFICATE KEY PAIR KEY REMOVAL WIZARD							
Partner certificates			REQUEST	REQUEST IMPORT IMPORT						_	
X Certificate authority certificates			cer	tificate type	standard cer	rtificate					
Personal repository				issued for CN=Tomáš Kout C=CZ O=První certifikační autorita, a.s. GN=Tomáš SN=Kout							
Protected personal repository											
Card informat	Card information			organizationIdentifier=NTRCZ-26439395						_	
Tomáš Kout, 22.04.20	24		issuer CN=I.CA Public CA/RSA 06/2022 O=První certifikační autorita, a.s.								
SC Tomáš Kout					C=CZ	ildentiller=NTRC	2-20439395				
—— 🛃 QC Tomáš Kout				validity from 22.04.2024 8:00:33 to 22.04.2025 8:00:33							
—— 🔍 SC key pair			se	serial number 3202F5 (hex))					
🖳 🔍 QC key pair					3277557 (de	c)					_
Tomáš Kout, 24.10.20	23		DETAIL EXI	PORT	DELETE	MARKAS		REGISTER TO		/5	
SC Tomáš Kout										CERTIEICA	TION
Select a personal certificate, a key								r 😃 🗌	AUTHOR	RITY	



3.5 Selecting smart card reader

If the user has more than one smart card reader connected to the PC, the "Select smart card readers" window even after the application is started.

Fig. 13 - Selecting a smart card reader

Choose card reader	
Alcor Micro USB Smart Card Reader 0 9203090300001862	
INGENICO iHC Smart Card Terminal 1 9203090300000672	
INGENICO iHC Smart Card Terminal 0	
	Cancel

If the user has only one smart card reader connected to the PC, the window is not displayed.

3.6 Toolbar

In the toolbar, see Fig. 14, the options change according to the selected object in the left part of the screen.

SECURESTORE SE	ettings	Diag	nostics						-		×
1. choose obj	ject				2. car	d informati	on				
🔄 Personal certificate	es		RELOAD	CARD CHOOSI	E CARD CHANGE	SHOW AUDIT	CHECK				
8 Partner certificates	8= Partner certificates		DATA	A REAL	DER PIN	LUG	INTEGRITY				_
Certificate authorit	ty certifica	tes		reader	INGENICO iHC Smart	Card Terminal 1					-1
Personal repositor	ry			card number	920309030000672						_
Protected persona	Protected personal repository			card holder							_
Card information		_		company	OPERÁTOR ICARA						
				issued by	06/12/2021						
				card type	ICA Starcos 3.7						
			version of th	ne card application	1.7						
				free card capacity	106160 B						- 1
				empty containers	information is not ava	ailable					
		ļ.		DIN	OV nameining attacks						
Active card details								۵	; I.	CERTIFICA AUTHOP	

Fig. 14 – Toolbar

3.7 Changing PIN

The tool bar example shows the options valid for the *Card Information* object.

Choose *Reload Card Data* to reload data from the smart card. F5 has the same function.

Choose *Change PIN* to change PIN to your card. The change PIN dialogue will ask you to enter your current PIN once and the new PIN twice.

Fig. 15 – Changing PIN

	PIN change
Current PIN new PIN new PIN again	
	CANCEL OK

- a) <u>Starcos 3.0 and 3.5</u> The Change PIN option allows you to change the PIN provided, if the value of the original PIN is known. The Unblock PIN option allows a new PIN value to be set if the user blocks the PIN. A PUK is required to unblock the new PIN setting.
 Unblocking a PIN using a PUK is limited to 5 attempts.
- b) <u>Starcos 3.7</u> The Change PIN option allows you to change the PIN provided, if the value of the original PIN is known. The Unblock PIN option allows a new PIN value to be set if the user blocks the PIN. A PUK is required to unblock the new PIN setting. By entering the PUK, the user activates 3 new attempts to enter the correct PIN.

PIN unblocking with PUK is limited to 10 attempts.

4. Display key pair information

The user can find information about the key pair in the **"Personal certificates"** object.

Fig. 16 - Displaying key pair information

	Settings	Diag	nostics						_		×
1. choos	e object		>			2. key p	oair detail				
🛃 Personal cert	tificates		CREATE CER	RTIFICATE CE	RTIFICATE	KEY PAIR	KEY REMOVAL WIZARD				
8 Partner certif	ficates	-	nequ								
🏅 Certificate au	uthority certifica	ites									
Personal rep	ository		corresp	onding certificate	SC Tomáš K	out					
Protected pe	Protected personal repository			container name Objekt 24/10/2023 14:32:24							
🗐 Card informa	ation		contai	container creation date 24.10.2023 14:32:38							
Tomáš Kout, 24.10.20	023			Key Origin	The key was	generated in th	he smart card				
SC Tomáš Kout				Key Purpose	Exchange ke	2V					
SC key pair				key type	PSA (2049 b)	itc)					
OPRA Tomáš Kout, 03	3.04.2024	- 1		key type	K3A (2046 D	1(5)					
QC OPRA Tomá	áš Kout										
SC OPRA Tomá	š Kout										
💛 🔍 QC key pair											
About application								۵	١.	CERTIFICA	

The storage stores one key pair for the certificate and two key pairs for Twins certificates.

The public/private key generation time is the exact time the key has been generated on the card or imported in the card.

The "Key origin" entry shows how the key was created on the card.

The **"Key purpose"** item indicates whether the key is an encryption or signature key.

The **"Key type"** is also shown, in the example it is a key for the RSA algorithm with a length of 2048 bits.

A key pair can be removed from the card using the **"Remove"** button.

4.1 Deleting a public key

The user finds the option in the **"Personal Certificates"** object, selects the desired public key and uses the **"Delete"** button to perform the deletion.

Fig. 17 - Deleting a public key

	Settings	Diag	nostics						-		×
1. choos	se object					2	. personal c	ertificate detail			
Personal cer	tificates		CREATE CE	RTIFICATE	CER	TIFICATE	KEY PAIR	KEY REMOVAL WIZARD			
🕭 🛛 Partner certi	ficates	-	REQI								
K Certificate au	Certificate authority certificates			certificate t	ype	standa	rd certificate				-1
Personal rep	Personal repository			issued	l for	CN=To C=CZ	máš Kout				- 1
Protected pe	Protected personal repository					O=Prvi GN=To SN=Ko	ní certifikační autorita máš ut	a, a.s.			- 1
Card informa	ation					organiz	ationIdentifier=NTR	CZ-26439395			_
Tomáš Kout, 22.04.2	024			iss	suer	CN=I.C O=Prvr	A Public CA/RSA 06/20 ní certifikační autorita	022 a, a.s.			1
—– 📧 SC Tomáš Kout	t					organiz C=CZ	ationIdentifier=NTR	CZ-26439395			- 1
💛 💽 QC Tomáš Kou	t			vali	dity	from 2	2.04.2024 8:00:33 to 2	2.04.2025 8:00:33			
💛 🔍 SC key pair				serial num	nber	3202F5	(hex)				_
🖳 🔍 QC key pair	— 🔍 QC key pair					327755	7 (dec)				
Tomáš Kout, 24.10.2	023						-				
🗕 🔚 SC Tomáš Kout	📧 SC Tomáš Kout			EXPORT	DE	LETE	MARK AS INITIAI	L REGISTER TO WINDOWS			
Select a personal certificate, a k	key pair or a container								ا 🙂	AUTHO	ATION RITY

4.2 Removing the container

The user finds the option in the **"Personal Certificates"** object, selects the desired container and uses the **"delete container"** button to delete it.

Fig. 18 - Removing a container

	Settings	Diag	nostics					-	-		×
1. choos	e object		>			2. conta	iner detail				
Personal cert	tificates		CREATE CE	ERTIFICATE CEI	RTIFICATE	KEY PAIR	KEY REMOVAL WIZARD				
8 Partner certit	ficates										
🕈 Certificate au	uthority certifica	ates									
Personal rep	ository										
Protected pe	rsonal reposito	ry									
Card informa	ation	·		container name	TwinsSD 2	2/04/2024 07:58:0	5				
🗁 Tomáš Kout, 22.04.20	024		conta	ainer creation date	22.04.2024	7:58:47					
— 📧 SC Tomáš Kout					1						
— 🔄 QC Tomáš Kou	t	1									
—— 🔍 SC key pair											
📃 🔍 QC key pair											
Tomáš Kout, 24.10.20	023										
📧 SC Tomáš Kout											
Select a personal certificate, a k	ey pair or a container							ی 🕒		OERTIFICA AUTHOR	

If the user deletes the container, this session is irreversible and can no longer be signed/decrypted by the certificate!!!



4.3 Deleting a container using the key removal wizard

The user finds the option in the "Personal Certificates" object, selects the desired key pair and runs the

"Key Removal Wizard" function.



Fig. 19 – Key removal wizard

The key removal wizard is divided into 3 tabs based on the type and length of the key. In this example, the key type is an RSA key with a length of 2048 bits.

	Settings	Diag	nostics					-	-		×
1. choos	e object		>			2. key p	oair detail				
🔄 Personal cer	tificates		CREATE CE	ERTIFICATE CER		KEY PAIR	KEY REMOVAL WIZARD				
🛯 🖉 Partner certi	ficates		n.cq								
🎖 Certificate au	uthority certifica	ites									
Personal rep	ository		corres	ponding certificate	QC Tomáš K	out					
Protected pe	ersonal reposito	ry		container name	TwinsOD 22	/04/2024 07:58:	05				
Card information	ation		cont	ainer creation date	22.04.2024 7	:58:28					
Tomáš Kout, 22.04.20	024	1		Key Origin	The key was	generated in t	he smart card				
SC Tomáš Kout	t	- 11		Key Purpose	Key for qual	ified electronic	signature				
QC Tomáš Kou	t			key type	RSA (2048 bi	ts)					
— 🔍 SC key pair		_									
🔍 QC key pair											
Tomáš Kout, 24.10.20	023										
SC Tomáš Kout	t										
Select a personal certificate, a k	key pair or a container							ے 🗧	1.	CERTIFICA AUTHOR	



Fig.	20 -	Key	and	certificate	removal	wizard
------	------	-----	-----	-------------	---------	--------

	Key and certificate removal wizard	
RSA 2048 RSA 4096	ECC	
smart card reader	INGENICO iHC Smart Card Terminal 1	
card number	920309030000672	
Free for QC RSA 2048	0	
container name	TwinsQD 22/04/2024 07:58:05	
creation date	22.04.2024 7:58:28	Key for qualified
certificate for	Tomáš Kout	electronic signature
serial number	BBAEA4 (hex) 12299940 (dec)	Remove container
validity period	from 22.04.2024 8:00:27 to 22.04.2025 8:00:27	
certificate status	valid	
container name	Objekt 24/10/2023 14:32:24	
creation date	24.10.2023 14:32:38	
certificate for	Tomáš Kout	Part Antina
serial number	3109A2 (hex) 3213730 (dec)	Delete certificate
validity period	from 24.10.2023 14:34:01 to 23.10.2024 14:34:01	
certificate status	valid	
		STORNO

The "Remove container" option is the same as in the previous section 4.2.

If the user deletes the container, this session is irreversible and the certificate can no longer be signed/decrypted!!!

The **"Delete certificate"** option is only enabled for commercial certificates and is used to remove only the public key as in 4.1

After clicking on the **"Delete"** option, the user is prompted to enter the PIN, after entering the PIN the marked certificate/container will be deleted.

Fig.	21 -	Entering	the PIN t	o remove	the ce	ertificate/	container
------	------	----------	-----------	----------	--------	-------------	-----------

	Enter PIN	
QC PIN		
	CANCEL	ОК

5. Certificates

5.1 Displaying the certificate

The user can find the certificate display in the **"Personal certificates"** object, where he selects the desired certificate to display. The detail of the certificate is displayed in the right screen of the application in the **"Personal certificate detail"**.

Fig. 22 - Displaying the certificate

	Settings	Diag	nostics						-		×
1. choos	se object		>			2	. personal ce	ertificate detail			
Personal cert	tificates		CREATE CE	RTIFICATE	CER	TIFICATE	KEY PAIR	KEY REMOVAL WIZARD			
8= Partner certi	ficates	-									_
K Certificate au	8 Certificate authority certificates				ype	standa	rd certificate				-1
Personal rep	ository			issued	for	CN=Tor C=CZ	máš Kout				
Protected pe	Protected personal repository					GN=To SN=Ko	ni certifikachi autorita máš ut	, a.s.			- 1
Card information	Card information				organizationIdentifier=NTRCZ-26439395						
Tomáš Kout. 22.04.2	024		I	iss	uer	CN=I.C. O=Prvr	A Public CA/RSA 06/20 ní certifikační autorita)22 , a.s.			
🗕 🔚 SC Tomáš Kout	t					organiz C=CZ	zationidentifier=NTRC	_2-26439395			- 1
🚽 🔄 QC Tomáš Kou	t			vali	dity	from 2	2.04.2024 8:00:33 to 22	2.04.2025 8:00:33			
SC key pair				serial num	ber	3202F5	(hex)				
🖳 🔍 QC key pair						327755	7 (dec)				_
🗁 Tomáš Kout, 24.10.2	023										
SC Tomáš Kout	SC Tomáš Kout			EXPORT	DE	LETE	MARK AS INITIAL	REGISTER TO WINDOWS			
Select a personal certificate, a k	key pair or a container								ا 🕲	AUTHO	

5.2 Working with a personal certificate

Options for working with the certificate stored on the card are available in the toolbar at the bottom of the application.

The user finds the option in the "**Personal certificates**" object and selects the required certificate for the operation using the toolbar.



SECURESTORE Settings	Diag	gnostics			×
1. choose object				2. personal certificate detail	
Personal certificates		CREATE CE	ERTIFICATE CER	IFICATE KEY PAIR KEY REMOVAL WIZARD	
Partner certificates		REQ	UESI II		
Certificate authority certific	ates		certificate type	standard certificate	-1
Personal repository			issued for	CN=Tomáš Kout C=CZ	
Protected personal reposit	ory			O=Prvni certifikačni autorita, a.s. GN=Tomáš SN=Kout	- 1
Card information				organizationIdentifier=NTRCZ-26439395	_
Tomáš Kout, 22.04.2024	1		issuer	CN=I.CA Public CA/RSA 06/2022 O=První certifikační autorita, a.s.	
SC Tomáš Kout				organizationIdentifier=NTRC2-26439395 C=CZ	- 1
🔄 QC Tomáš Kout			validity	from 22.04.2024 8:00:33 to 22.04.2025 8:00:33	_ •
—— 🔍 SC key pair			serial number	3202F5 (hex)	_
—— 🔍 QC key pair				3277557 (dec)	_
Tomáš Kout, 24.10.2023					
📧 SC Tomáš Kout		DETAIL	EXPORT DI	LETE MARK AS INITIAL REGISTER TO WINDOWS	
Select a personal certificate, a key pair or a container					

Fig. 23 - Options for working with a personal certificate in the toolbar

The options for importing a certificate to a smart card are available by clicking on the **"Personal certificates"** object.



SECURESTORE	Settings	Diag	nostics							-		×
1. choos	se object					2	. personal c	ertificate detail				
Personal cer	tificates		CREATE CE REQ	ERTIFICATE	CERT IM	TIFICATE	KEY PAIR IMPORT	KEY REMOVAL WIZARD	1			
8= Partner certi	ficates					_						_
🕈 Certificate au	uthority certifica	ates		certificate	type	standa	rd certificate					_1
Personal rep	ository			issued	d for	CN=To C=CZ	máš Kout					
Protected pe	ersonal reposito	ry				GN=To SN=Ko	ni čertifikačni autorita máš ut	a, a.s.				- 1
Card informa	ation					organia	ationIdentifier=NTR	CZ-26439395				
Tomáš Kout, 22.04.20	024			is	suer	CN=I.C O=Prvr	A Public CA/RSA 06/20 ní certifikační autorita	022 a, a.s.				
🗕 🔚 SC Tomáš Kout	Ę					C=CZ	auomuentiner-in rik	CZ-20433333				- 1
— 🛃 QC Tomáš Kou	t			vali	idity	from 2	2.04.2024 8:00:33 to 2	2.04.2025 8:00:33				
—— 🔍 SC key pair				serial num	nber	3202F5	(hex)					_
🖳 🔍 QC key pair						327755	7 (dec)					
Tomáš Kout, 24.10.2	023	-										
🕭 SC Tomáš Kout	t)		DETAIL	EXPORT	DEI	LETE	MARK AS INITIAI	L REGISTER TO WINDO	WS			
Select a personal certificate, a k	ey pair or a container								> 3		CERTIFICA AUTHOR	



The personal certificate is imported in the storage where the corresponding key pair is saved. Communication partner's certificates can be imported as partner certificates.

Displaying the certificate's bare data is an option for experts to make a visual check of the certificate's data.

5.3. Using CA Root Certificate

A new card contains the required certification authority root certificates, which are saved in **"Certification Authority Certificates"**.

A certificate can only be imported as a CA certificate if it is a certificate of a permitted CA for the given smart card. Certificates of other CAs and new CA certificates issued can be imported as .cmf files. The I.CA certificates as .cmf files can be downloaded from https://www.ica.cz/Rootcertificate

Fig. 25 – Importing a Certification Authority Certificate

	Settings	Diag	nostics							×
1. choos	e object				2. C/	A certificate det	ail			
Personal cert	tificates ficates		CERTIFICA IMPORT	ТЕ						
Certificate au	uthority certifica	ates		certificate type	qualified certificat	e				
Personal rep	ository			issued for	CN=I.CA Test EU Q O=První certifikač	ualified CA-SK/RSA 10/202 ní autorita, s.r.o.	2			
Protected pe	ersonal reposito	ry			organizationIdent C=SK	ifier=NTRSK-54869099				
Card informa	ation			issuer	CN=I.CA Test Root	CA/RSA 04/2022				
8 I.CA Test EU Qualified	d CA-SK/RSA 10/2022	2			organizationIdent C=CZ	ifier=NTRCZ-26439395				
8 I.CA Test EU Qualified	d CA2/RSA 04/2022	1		validity	from 04.10.2022 14	4:21:02 to 01.10.2032 14:21	:02			
8 I.CA Test EU Qualified	d CA1/RSA 0 <mark>4/2022</mark>			serial number	05F5E536 (hex)		0/2#*V			
8 I.CA Test Qualified CA	A/RSA 11/2015				100001078 (dec)					
8 I.CA Test Public CA/R	SA 04/2022			key type	RSA (4096 bits)					
8 I.CA Test Public CA/R	SA 11/2015		DETAIL			DELETE				
8 I.CA Test Qualified 2	CA/RSA 02/2016				DD TO TROSTED					
Select a certificate of a certificat								🕑 📘	AUTHOR	

Root certificates are used to verify the trustworthiness of personal certificates. To work with certificates, root certificates need to be registered in Windows so that Windows can verify the trustworthiness of certificates used for signing or encryption.

If the user is using an older version of Windows and I.CA root certificates are not part of Windows, register the root certificate from the smart card. Use the "**Add to Trusted**" option to register, see Figure 26. Registering the root certificate to Windows requires user consent, then the root certificate is registered to MS Windows as a trusted root certificate.



	Settings	Diag	gnostics						_	C]	×
1. choos	e object					2. CA	A certific	ate detail				
Personal cert	tificates		CERTIFICAT	E								
🛎 Partner certi	ficates		IMPORT									
🚼 Certificate au	uthority certifica	ites		certificate ty	pe	qualified certificate	e					
Personal rep	ository			issued	for	CN=I.CA Test EU Qu O=První certifikačr	ualified CA-SI ní autorita, s.r	K/RSA 10/2022 r.o.				
Protected pe	rsonal reposito	ry				organizationIdenti C=SK	fier=NTRSK-5	54869099				
Card informa	ation			issu	Jer	CN=I.CA Test Root	CA/RSA 04/2	022				
8 I.CA Test EU Qualified	I CA-SK/RSA 10/2022	2				organizationIdenti C=CZ	fier=NTRCZ-2	s. 26439395				
8 I.CA Test EU Qualified	I CA2/RSA 04/2022			valid	lity	from 04.10.2022 14	:21:02 to 01.1	10.2032 14:21:02	 			
8 I.CA Test EU Qualified	CA1/RSA 04/2022			corial numb	-	OFFFFF26 (box)						
I.CA Test Qualified CA	/RSA 11/2015			Senarhumi	Jei	100001078 (dec)						
I.CA Test Public CA/R	SA 04/2022			key ty	pe	RSA (4096 bits)						
I.CA Test Public CA/R	SA 11/2015		DETAIL	EXPORT)				
I.CA Test Qualified 2	CA/RSA 02/2016			EAFORI	AL		DELETE	J				
Select a certificate of a certificat	ion authority								 ٠	AUT	TIFICATI	ON TY

Figure 26 - Registering a certification authority certificate to Windows

5.4. Registering Personal Certificate in Windows

Most applications require that the personal certificate with which the user wants to work be registered in Windows.

Use "Register in Windows" to register each certificate separately.

This option will register the personal certificate from the smart card in the personal Windows storage.

Go to "Personal Certificates" and select the certificate to be registered.

Fig. 27 – Registering personal certificate in Windows

	Settings	Diag	gnostics					_		×
1. choos	e object		>			2. personal cer	tificate detail			
Personal cert	tificates		CREATE C	ERTIFICATE	CERT	TIFICATE KEY PAIR	KEY REMOVAL WIZARD			
🛯 🖉 Partner certi	ficates									
Certificate au	uthority certifica	ites		certificate ty	pe	standard certificate				-1
Personal rep	ository			issued f	for	CN=Tomáš Kout C=CZ				
Protected pe	ersonal reposito	ry				O=První certifikační autorita, a: GN=Tomáš SN=Kout	s.			1
🗐 Card informa	ation					organizationIdentifier=NTRCZ-2	26439395			_
Tomáš Kout, 22.04.20	024			issu	Jer	CN=I.CA Public CA/RSA 06/2022 O=První certifikační autorita, a.	2 S.			
—— 📧 SC Tomáš Kout	:					organizationIdentifier=NTRCZ-2 C=CZ	26439395			
💛 🔄 QC Tomáš Kou	t			valid	ity	from 22.04.2024 8:00:33 to 22.04	4.2025 8:00:33			
— 🔍 SC key pair				serial numb	ber	3202F5 (hex)				_
🖳 🔍 QC key pair						3277557 (dec)				
Tomáš Kout, 24.10.20	023									
SC Tomáš Kout	t		DETAIL	EXPORT	DE	LETE MARK AS INITIAL	REGISTER TO WINDOWS			
Select a personal certificate, a k	key pair or a container							٠	AUTHOP	

6. Personal Repository

Fig. 28 – Personal Repository

	Settings	Diagnostics		- 0	×
1. choos	se object		2. object detail		
🔄 Personal cer	tificates	FILE IMPORT			
🕭 Partner certi	ficates				
😗 Certificate au	uthority certifica	ates			
Personal rep	ository				
F Protected pe	ersonal reposito	ry			
Card informa	ation				
			No object selected		
Select a file in the personal repo	ository	1	ی د	AUT	FICATION HORITY

The user can store small files (a few kB) in the **"Personal repository"** or **"Protected personal repository"** section of the tab. Text as well as binary files can be saved to the tab.



Reading and exporting secure storage files are protected with the secure storage PIN, see Chapter 2.

Fig. 29 - Importing a file into personal repository

	Settings	Diagnostics		-		×
1. choos	e object		2. object detail			
Personal cert	tificates	FILE IMPOR	RT			
8= Partner certi	ficates					
K Certificate au	uthority certifica	ates				
Personal rep	ository					
Protected pe	ersonal reposito	ry				
Card informa	ation					
			No object selected			
Select a file in the personal repo	ository		ے 😜 😉	1.	CERTIFICA AUTHOF	

The user can find the function in the **"Personal Repository"** object and in the details of the **"File import"** object.

Figure 30 - Importing a file into a protected repository

	Settings	Diagnostics			-	×
1. choos	e object			2. object detail		
🖅 Personal cer	tificates	FILE	CHANGE PIN FOR			
🕭 Partner certi	ficates	IMPORT	PROTECTED REPOSITORY		 	
Certificate au	uthority certifica	ates				
Personal rep	ository					
Protected pe	ersonal reposito	ry				
Card information	ation					
				No object selected		
Select a file in the protected rep	oository				C A	



The user can find the function in the **"Protected Personal Repository"** object and in the detail of the **"File import"**

Fig. 31 - Exporting a file from a personal repository

	Settings	Diagnos	stics		-		×
1. cho	ose object			2. personal repository file detail			
🖅 Personal ce	ertificates	FII	LE IMPORT				
🗶 Partner cer	tificates						
🕈 Certificate	authority certific	ates					
Personal re	epository						
f Protected	personal reposito	ory					
Card inform	nation		file name	file.txt			
E file tyt			creation date	27.06.2024 13:29:44			
		_	file length	4 B			
		E	XPORT DELETE				
Select a file in the personal r					e I	AUTHO	

The user can find the function in the **"Personal Repository"** object, after selecting the file to export in the **"Personal Repository File Detail"**, he will click the **"Export"** button.

In order to delete a file in the protected repository, a PIN is required.

7. Application control

The individual functions of the application are implemented using the toolbar. The toolbar is displayed by clicking on the appropriate object on the left side of the application screen.

7.1 Toolbar for card information

The toolbar of the "Card information" object contains basic administrative operations with the card related to PIN and PUK management and repeated loading of data from the card.

Fig. 32 – Toolbar of the "Card information" object

	Settings	Diag	nostics						—		×
1. choos	se object				2. car	d informati	on				
Personal cer	tificates		RELOAD (DATA	CARD CHOOS	E CARD CHANGE DER PIN	SHOW AUDIT LOG	CHECK]			
Certificate a	uthority certifica	ates		reader	INGENICO iHC Smart	Card Terminal 1					
Personal rep	ository			card number	920309030000672						
Protected pe	ersonal reposito	ry		card holder							_
Card inform	ation			company	OPERÁTOR ICARA						_
			<u> </u>	issued by	06/12/2021						
				card type	ICA Starcos 3.7						
			version of th	e card application	1.7						
6	7			free card capacity	106126 B						
				empty containers	information is not ava	ailable					
										CERTIFICA	TION
Active card details										AUTHOP	RITY

7.2 Toolbar for Personal certificates folder

Fig. 33 – Toolbar for the "Personal Certificates" object

	Settings	Diagnostics			-		×
1. choos	e object	>		2. personal certificate detail			
Personal cer	tificates	CREATE	CERTIFICATE CEP QUEST II	ITIFICATE KEY PAIR MPORT IMPORT KEY REMOVAL WIZARD			
8= Partner certi	ficates						_
🕈 Certificate au	uthority certifica	ates	certificate type	standard certificate			
Personal rep	ository		issued for	CN=Tomáš Kout C=CZ			
Protected pe	ersonal reposito	ry		O=První certifikační autorita, a.s. GN=Tomáš SN=Kout			
Card informa	ation			organizationIdentifier=NTRCZ-26439395			_
Tomáš Kout, 22.04.2	024	1	issuer	CN=I.CA Public CA/RSA 06/2022 O=První certifikační autorita, a.s.			
SC Tomáš Kout	:			C=CZ			
💛 — 🔄 QC Tomáš Kou	t		validity	from 22.04.2024 8:00:33 to 22.04.2025 8:00:33			
SC key pair			serial number	3202F5 (hex)			_
🖵 🔍 QC key pair				3277557 (dec)			
Tomáš Kout, 24.10.2	023	DETAIL	EXPORT D	ELETE MARK AS INITIAL REGISTER TO WINDO	ws		
SC Tomáš Kout	ł	DETAIL					17:011
Select a personal certificate, a k	ey pair or a container					AUTHO	RITY

7.2.1 Create certificate request

The "Create certificate request" option will redirect the user to the I.CA website, where they select the desired type of the certificate request to generate a key pair using the on-line generator.

Fig. 34 - Selecting the type of request for generating a key pair using the online generator

	Settings	Diag	gnostics						-		×
1. choos	e object					2	2. personal c	ertificate detail			
Personal cert	tificates		CREATE CE REQU	RTIFICATE	CER	TIFICATE //PORT	KEY PAIR	KEY REMOVAL WIZARD			
8= Partner certif	ficates										-
🎖 Certificate au	thority certifica	ates		certificate	type	standa	ard certificate				_
Personal rep	ository			issue	d for	CN=To C=CZ	máš Kout				
Protected pe	rsonal reposito	ry				O=Prvi GN=To SN=Ko	ní certifikační autorita omáš out	, a.s.			
🗐 Card informa	ation					organi	zationIdentifier=NTR(Z-26439395			_
Tomáš Kout, 22.04.20)24			is	suer	CN=I.C O=Prvi	A Public CA/RSA 06/20 ní certifikační autorita)22 , a.s.			
SC Tomáš Kout						C=CZ	zationIdentifier=NTR0	.2-26439395			
— 🔄 QC Tomáš Kout	t			val	idity	from 2	2.04.2024 8:00:33 to 2	2.04.2025 8:00:33			
—— 🔍 SC key pair				serial nur	nber	3202F5	ō (hex)				
🖵 🔍 🔍 QC key pair						327755	57 (dec)				
🗁 Tomáš Kout, 24.10.20	023		DETAIL	EXPORT	DE	ETE					
SC Tomáš Kout			DETAIL	EXI OKI							
About application										AUTHOR	

After selecting the type of applicant and certificate request, the user will be redirected to the I.CA on-line generator, where it is necessary to pass the system test (have the necessary components installed to run the on-line generator).

Fig. 35 - Selecting the type of certificate applicant



Fig. 36 - Data entry - on-line generator

AUTHORITY	CONNECTED) WITH TRUST		S # S
		CREATE A QUALIFIED CE	RTIFICATE REQUEST	
1. Test system	2. Entering data	3. Verification	4. Saving request	5. Completion
Information ab	out the applicant		Sh	ow other options >>
Degree (before name)		Degree (after name)		
Thomas		Corner	Czech Republic	v 🔞
test@ica.cz	0	test@ica.cz	+420 ¥ Pho	ne number
Insert optional ide	ntifier for individuals			
Key type		RSA 2048 🗸		
Revocation password		1234		0
Key Repository Type (CSP)	Microsoft Smart Card Key Storage Pr	ovider	v
 Certificate contain 	ing IC MLSA for communicatio	n with the public authorities 🛛 🛛		
Certificate sent in	the ZIP format			
Save the request t	o the card			
			Advanced (Certificate Options >>
	Copyright I CA Al	Continue	rita. a.s. Contarts 09.20.00	
	copyright I.CA Al	r nights neserveu rivni cerunkdolli dub	onte, e.s. contacts 09.20.00	

Fig. 37 - Data check – on-line generator

			s 🕀 💿
		LIFIED CERTIFICATE REQUEST	
1. Test system	2. Entering data 3. Verificatio	4. Saving request	5. Completion
	Information abo	ut the applicant	
	Full name	Thomas Corner	
	First name	Thomas	
	Surname	Corner	
	E-mail in the certificate	test@ica.cz	
	Country	Czech Republic	
	Certificat	e setting	
	Type of the certificate	Qualified certificate	
	Type of applicant	Current user (individual - non-entrepreneu	rial)
Certificate containing	IC MLSA for communication with the public authorities	Yes	
	Revocation password	1234	
	E-mail for contact with I.CA	test@ica.cz	
	Certificate sent in the ZIP format	Yes	
	Period of validity	365 days	
	Certificate signing algorithm	pkcs#1 1v5	
	Key Repository Type (CSP)	Microsoft Smart Card Key Storage Provider	,
	Key type / Algorithm thumbnails / Key length	RSA / sha256Algorithm / 2048	
	Usage setting key	Non Repudiation / Digital Signature	
	Extended usage setting key	id-kp-emailProtection	
	Encoding type	UTF8_STRING	
	Cont	inue -	

Generating key pairs and signing the request - on-line generator

If the user has more than one smart card connected to the PC, the user selects in the dialog box which key pair should be generated. After selecting the smart card, the system prompts the user to enter the PIN.



Fig. 38 - Generating a private key

CREATING A CERTIFICATE REQUEST
₽. Example 1 and
Please wait, key generation and creation of the certificate
request.

Fig. 39 - Selecting a smart card reader

Choose your card		- 0 X
Card list: Reader name Alcor Micro USB Smart Card Reader 0 BIT4ID miniLector-S 0 INGENICO iHC Smart Card Terminal 1	Card name ICA Starcos 3.7 eSign ICA Starcos 3.7 eSign ICA Starcos 3.7 eSign	Provider Microsoft Smart Card Key Stor Microsoft Smart Card Key Stor Microsoft Smart Card Key Stor
	OK Cancel	

Fig. 40 - Entering the PIN to generate the key pair and signing the request

PIN dialog				×
To process thi PIN:	is operatio	on, it is r	necessary t	o enter PIN
	Ok		Cancel	



Fig. 41 – Saving the request – on-line generator

	W			
1 . Test system	2. Entering data	3. Verification	4. Saving request	5. Completion
Save to the I.CA	Selec	ct how to save your ce	rtificate request	
Save on local dis	k or external storage	Save to the I.CA	server	
		own on the picture and press the	The specified phone number will	be sent the request identification

Choosing a way to save a certificate request.

When choosing **"Save to I.CA server"**, a six-digit numeric code of the saved request on the I.CA server will be sent to the user's contact e-mail specified in the certificate request.

When **"Save to local disk or external storage"** is selected, a file with the generated request called cert****.req is saved.



Fig. 42 - Completion – on-line generator

AUTHORITY	CONNECTED	WITH TRUST		• # •			
		CREATE A QUALIFIED	CERTIFICATE REQUEST				
1. Test system	2. Entering data	3. Verification	4. Saving request	5. Completion			
	Your request has	been successfully	stored on the I.CA	server.			
	Ident	ification code of y	our request is				
	I	944152					
With this id	lentification code v	isit selected regis	tration authority w	hich completes the			
	i	ssuance of your c	ertificate.				
		Find the registration	authority				
		Exit guide					

Copyright I.CA All Rights Reserved | První certifikační autorita, a.s. | Contacts | 09.20.00

With the six-digit numerical code for the request stored on the I.CA server or with the req. file on a portable USB medium, the user then visits the registration authority, which can be searched for using the **"Find registration authority"** button.

7.2.2. Importing a personal certificate

This function allows you to import a personal certificate from disk to smart card. The certificate is imported in cer./der. format. The user can find the function in the **"Personal certificates"** object.

Fig. 43 - Importing a personal certificate

	Settings	Diag	nostics	nostics						
1. choos	se object		>			2. personal certificate detail				
🔄 Personal cert	tificates		CREATE CE	CREATE CERTIFICATE CERTIFICATE KEY PAIR REQUEST IMPORT IMPORT KEY REMOVAL WIZARD						
🗶 🗧 Partner certi	ficates									
X Certificate au	X Certificate authority certificates			certificate type standard certificate						
Personal repository				issued for CN=Tomáš Kout C=CZ						
Protected personal repository				O=Prvni certifikačni autorita, a.s. GN=Tomáš SN=Kout						
🗐 Card informa	ation					organizationIdentifier=NTRCZ-26439395				
Tomáš Kout, 22.04.20	024	1	issuer CN=I.CA Publi O=První certi		suer	CN=I.CA Public CA/RSA 06/2022 O=První certifikační autorita, a.s.				
SC Tomáš Kout	t i i i i i i i i i i i i i i i i i i i				C=CZ					
—— 🖭 QC Tomáš Kou	t			validity from 22.04.2024 8:00:33 to 22.04.2025 8:00:33						
—— 🔍 SC key pair		- 1	serial number		nber	3202F5 (hex)				
🖳 🔍 QC key pair		- 1				3277557 (dec)	_			
Tomáš Kout, 24.10.20	023	- 1	DETAIL	EXPORT						
SC Tomáš Kout	+	_	DETAIL	EAPORI	DE	LETE WARK AS INITIAL REGISTER TO WINDOWS				
Select a personal certificate, a k	key pair or a container									

The imported certificate is stored in the storage on the smart card that contains the keys to the certificate.

If there is no storage on the smart card containing the appropriate keys, the certificate will be stored in the part of the card marked "Partner Certificates".

Fig. 44 - Selecting a certificate file to be imported to the card

Select a personal certificate to impo	ort				×
\leftarrow \rightarrow \checkmark \uparrow \square > Ploch	a > Secure Store		~ C Pro	hledat: Secure Store	م
Uspořádat 🔻 Nová složka				≣ •	•
> 🔷 OneDrive - Personal	Název	Datum změny	Тур	Velikost	
	🙀 certificate.cer	16.07.2024 9:03	Certifikát zabezpe	3 kB	
🛄 Plocha 🔹 🖈					
📑 Dokumenty 🔹 🖈					
🔀 Obrázky 🖈					
🔁 Fotky 🖈					
🕖 Hudba 🔹 🖈					
🛂 Videa 🛛 🖈					
🛓 Stažené soubory 🔹 🖈					
Název souboru:	certificate.cer		~ cer	tificate (*.pem *.der *.c	er*.p ∨
				Otevřít 🛉 Z	rušit

7.2.3 Importing a key pair from a backup (PKCS#8) and importing keys (PKCS#12)

This option imports the keys that were saved to disk during the process of generating the encryption certificate request (PKCS#8) onto the smart card. The user can find the function in the **"Personal Certificates"** object. In the same way, keys with a certificate that are stored in PKCS#12 format on disk can be imported to the smart card.

	Settings	Diag	nostics						-		×
1. choos	e object		>	2. personal certificate detail							
Personal cert	tificates		CREATE CE	CREATE CERTIFICATE CERTIFICATE KEY PAIR REQUEST IMPORT IMPORT KEY REMOVAL WIZARD							
A= Partner certif	ficates										_
Certificate au	Certificate authority certificates			certificate type standard certificate							
Personal repository				issued for CN=Tomåš Kout C=CZ							
Protected personal repository			O=První certifikační autorita, a.s. GN=Tomáš SN=Kout		a, a.s.						
🗐 Card informa	ation		organizationIdentifier=NTRCZ-26439395								
Tomáš Kout, 22.04.20	024		issuer		suer	r CN=I.CA Public CA/RSA 06/2022 O=První certifikační autorita, a.s.					
SC Tomáš Kout	:			C=CZ		(2-20439395					
💛 🔤 QC Tomáš Kou	t			vali	idity	from 22.04.2	2024 8:00:33 to 2	22.04.2025 8:00:33			
—— 🔍 SC key pair		- 11	serial number			r 3202F5 (hex)					
🖳 🔍 QC key pair	QC key pair					3277557 (de	c)				
Tomáš Kout, 24.10.20	Tomáš Kout, 24.10.2023		DETAIL	EXPORT							
SC Tomáš Kout		_	DETAIL	EAPORT	DE		ART AS INITIA	L REGISTER TO WINDOWS		OFPTIFIC	71011
Select a personal certificate, a k	ey pair or a container									AUTHOR	

Fig. 45 - Importing a key pair from a backup (PKCS#8) and a key pair (PKCS#12)

7.2.4 Set the certificate as the default for logging into Windows

This option allows you to mark the selected certificate as the default for Windows login. The selected certificate will be used when logging into Windows.

The user can find the function in the **"Personal certificates"** object, where he selects the certificate intended for this function and confirms it with the "Mark as default" button.

Fig. 46 - Mark certificate as default for Windows login

	Settings	Diagnostics				_		×		
1. choos	e object		2. personal certificate detail							
🔄 Personal cert	tificates	CREATE C	CREATE CERTIFICATE CERTIFICATE KEY PAIR REQUEST IMPORT IMPORT KEY REMOVAL WIZARD							
8 Partner certif	ficates							_		
🕈 Certificate au	uthority certifica	ates	certificate type standard certificate							
Personal rep		issued for CN=Tomáš Kout C=CZ								
Protected pe	ry	O=První certifikační autorita, a.s. GN=Tomáš SN=Kout								
🗐 Card informa	Card information			organizationIdentifier=NTRCZ-26439395						
Tomáš Kout, 22.04.20	024		issuer CN=I.CA Public CA/RSA 06/2022 O=První certifikační autorita, a.s.							
- 📧 SC Tomáš Kout	:		organizationIdentifier=N C=CZ		CZ-26439395					
QC Tomáš Kout	t		validity from 22.04.2024 8:00:33 to 22.04.2025 8:00:33							
— 🔍 SC key pair			serial number 3202F5 (hex)					_		
🖵 🔦 QC key pair				3277557 (dec)				_		
Tomáš Kout, 24.10.20	023	DETAIL	EXPORT							
SC Tomáš Kout		DETAIL	EAPORI DI	ELETE IVIARK AS INITIA	REGISTER TO WINDOWS			TION		
Select a personal certificate, a k	ey pair or a container					ت ا	- AUTHOR	RITY		

8. Definitions

Certification authority – an independent trusted entity that issues certificates to clients. The certification authority guarantees that the link between a client and his certificate is unique.

Registration authority – a contact workplace for communication with clients. The primary job of a registration authority is to receive certificate applications and deliver certificates to clients. Registration authorities verify certificate applicant's identity and whether applications match the documents submitted. Registration authorities issue no certificates, they only submit certification applications to the I.CA central office.

Cryptographic operations – operations using a key to encrypt and decrypt. Asymmetric cryptography is used for the smart cards – encryption and decryption are done with a pair of keys and an electronic signature is created and verified.

Electronic signature - electronic data attached to or logically linked with a data message that permits verifying the signed person's signature in relation to the signed message.

Data for creating an electronic signature- unique data used by the signing person to create their electronic signature (in the meaning of the Electronic Signature Act); it is the private key of the relevant asymmetric cryptographic algorithm (RSA in this instance).

Smart card - a device providing secure storage of the user's private key and allowing the user to create electronic signature. The smart card contains private keys, client's certificates and certification authority certificates, and can also hold other data.

PIN and PUK – a means to protect access to the card, that is, writing on the card and using the private keys saved on the card. These protective codes can be set in the card beforehand, with the user receiving the codes in the PIN envelope, or it is the client who sets his PIN and PUK for his card.

PIN envelope – the letter a client may receive along with his card. A PIN envelope belongs to a specific card and contains the card's unique identification and PIN and PUK values. Some cards may be supplied without a PIN envelope.

Repository – memory space on a medium, such as disk or smart card, where the key pair and the certificate are saved. A single smart card may have as many as 8 different storage compartments at a time. The smart card repository has its unique name. SIGNATURE type storage does not permit creating key backups when generating a certification request. Any certificate for which keys are backed up thus must be saved in OTHER storage.

Certification request – is completed by filling a form with applicant data. The applicant's public key is attached to the information filled in the request form and all this structure is signed with the applicant's private key. Certification request is digital data that include all the data required for the certificate to be issued

Certificate – proof of identity analogous to personal identity card, client uses his certificates to prove his identity in electronic communication. The procedure for getting the certificate is very similar to that for getting a personal identity card. I.CA provides these services through a network of points of contact – registration authorities, which implement client's requests. A certificate is uniquely tied to a pair of keys, which the user uses in electronic communication. The key pair consists of the public key and the private key.

Public key - the public part of the user's key pair, it is intended for electronic signature authentication and possibly for encryption.

Private key - the secret part of the user's key pair, it is used for creating an electronic signature and possibly for decryption. Due to the use of a private key, the highest possible security must be provided for it. For this reason, a smart card is used to store the key. The private key used for decryption needs to be kept for the lifetime of the encrypted documents and messages. The user can store this key on the card and it is recommended to keep it on a backup medium at the same time.

Certificate validity – every certificate is issued for a definite period of time (1 year). The term of validity is specified in each certificate. The certificate used for electronic signature becomes useless after expiration. The encrypting certificate has to be kept beyond the term of validity to decrypt earlier messages.

Commercial certificate – is issued to natural persons or legal entities and is suitable for regular use. Commercial certificates are issued in the **Standard** version (the private key is stored in Windows) or the **Comfort** version (the private key is stored in the smart card).



Qualified certificate – is strictly subject to EU Regulation 910/2014 and designed solely for electronic signatures. Creating, managing and using qualified certificates are governed by relevant certification policies. Qualified certificates are issued in the **Standard** version (the private key is stored in Windows) or the **Comfort** version (the private key is stored in the smart card).

Certification authority certificate – is used to verify the correctness and trustworthiness of client certificates. By installing it on your PC, the user declares to the operating system his trust in such a certificate authority. In practice, this means that if the user receives a message that is electronically signed with a certificate issued by that particular certification authority, it is seen as trustworthy by the system. In other cases, the message appears to be untrusted.

Windows login certificate - must contain specific information. Therefore, you cannot use any certificate to log in to Windows. The I.CA registration authority will provide the correct certificate for logging in upon request. The storage on the card containing the login certificate must be marked for authentication. Only one storage on the card can be marked for authentication.

List of public I.CA (commercial) certificates - a list of certificates issued by I. CA, for which their owners have agreed to make them public. This does not include "test" certificates and certificates for which the owner has not agreed to disclose.

The list of public commercial and qualified I.CA certificates can be found here:

https://www.ica.cz/List-public-certificates

Certification authorities supported by the card - each smart card issued by I.CA has a defined list of supported certification authorities whose certificates can be stored on the card.

Subsequent certificate - is issued to the client on the basis of an electronic request sent during the validity of the initial certificate. A subsequent certificate is issued only if the client does not request to change the items of the previous certificate. If it is requested, it is not a subsequent certificate, but another initial one. When issuing a subsequent certificate before the expiry of the initial certificate, the presence of the client at the I.CA registration authority is no longer necessary. The client simply sends an electronically signed request for the issuance of a subsequent certificate in a standardized electronic form using a valid certificate.

Key usage

- DigitalSignature (digital signature) This flag (bit) is primarily set if the certificate is to be used in connection with a digital signature, except for nonrepudiation, certificate signatures, and CA invalidated certificate lists. Usage: this bit is currently to be set in cases where the user intends to use his private key associated with the issued certificate for the creation of a digital signature in general (e.g. when using the certificate in secure e-mail).
- NonRepudiation this flag is set if the public key (through digital signature verification) is to be used to prove accountability for a particular action by the signer.
 Usage: this bit is currently to be set especially in cases of qualified certificates where the user intends to use his private key associated with the issued certificate to create an electronic signature.
- KeyEncipherment this flag shall be set if the public key is to be used to transmit cryptographic keys. Usage: this bit shall be set if the user intends to use the certificate for encryption purposes within secure electronic mail. In MS Outlook, this bit must also be set if the user does not have another certificate that can be used for encryption.

The PKCS#12 format of the RSA keys and the certificate can be stored in a single file in the so-called PKCS#12 format, which is defined by the PKCS#12 standard. In this format, it is possible, for example, to export the RSA key certificate from Windows storage if private key export is enabled. The content of the file is password protected. The file has the extension pfx or p12.