

CREATING A SUBSEQUENT CERTIFICATE REQUEST

A request for a subsequent certificates must be created on the same PC, where the original certificates is installed.

AUTHORITY První certifikační autorita A.s.	Issue of renewal certificate
Dear client, to ensure correct functionality of web meets the minimum software requirements to suc software components, in this case, please accept	application for issuing a renewal certificate, your computer will be inspected, whether it cessfully complete the renewal process. In tests, you may be asked to update certain the update components. To start the verification process, press Begin software analysis .
Copyright L	Begin software analysis CA 2000-2014 All Right Reserved <u>První certifikační autorita, a.s.</u> <u>Contacts</u>

Choose Begin software analysis.

		Prviji verifikačni nutarlia, a.s., (L.CA) was founded at the begi of own expertise and experience gained in implementation	Í
AUTHORITY	První certifikační autorita A.s.	Issue of renewal certificate	1
		The most important step forwards was a successful completion in present sense: of Law 227/2000 about electronic signature and conest i refiers, we Office	

After the tests finnish, press Start the issue of the renewal certificate near the bottom of the website (bellow the test results).

All tests were successful, the computer is ready for correct functionality of the web-based application.				
State	Test's description	Test resul	t Details	
√	Operation system version	ок	Your operating system Win8 is supported	
\checkmark	Browser type and version	ок	Your browser IE version 10.0 is supported.	
\checkmark	JavaScript scripting ability	ОК	JavaScript enabled.	
\checkmark	Java Runtime Environment (JRE) support	OK	Java Runtime Environment (JRE) installed. Manufacturer: Oracle Corporation (Version: 1.7.0_55)	
\checkmark	Java Applet jlCApki functionality	ок	Java Applet jlCApki initialized	
\checkmark	Support for the storage of cookies	ОК	Storage of cookies enabled.	

Start the issue of the renewal certificate

Copyright I.CA 2000-2014 All Right Reserved | První certifikační autorita, a.s. | Contacts

After the tests finnish, choose Start the isme of the renewal certificate



CERTIFICATION AUTHORITY První certifikační autorita AS. Issue of renewal certificate	Ð
The most important data factorial week and the second state of the	at on provins in the Offic Vice
Select the certificate for which you want to issue a renewal certificate.	
Choose where is your certificate stored (registered)	
The personal certificate store in Windows	
Other storage (eg I.CA smart card)	
David Jančík [2015-04-23][1DD111](I.CA - Standard Certification Authority, 09/2009)	
Continue	
Copyright I.CA 2000-2014 All Right Reserved Prvni certifikačni autorita, s.s. Contacts	
Doplněk Java(tm) Plug-In SSV Helper od vydavatele Oracle America, Inc. je připraven k použití. <u>N</u> epovolit <u>N</u> epovolit	×

Choose where is your certificate stored. Next, select "Povolit" (Enable) Java to use an.

Heading	Your information	Description
Certificate		
Commercial certific	1954065 (1DD111 hex)	
Not a	23. 4. 2015 12:02:31	
ls:	I.CA - Standard Certification Authority, 09/2009	
Cou	CZ	
Common ni	David Jančík	
Organiza Casial Nus	Prvni certitikacni autorita, a.s.	
Subject alternative name of commer	10A - 705671	
certific		
E-mail (rfc822Na	jancik@ica.cz	
Revocation passw		The password for invalidation must contain only numbe and letters without diacritics. The password must contait 4 to 32 characters. If you do not enter a new password, the password for certificate invalidation valid for the currently valid certificate will be used.
Key Repository Type (C	Microsoft Enhanced RSA and AES Cryptographic Provider	
Allow export of the private	V	This option allows you to export the certificate including the private key. You will be able to transfer the private key between repositories. The key management require special attention because of the high risk of theft/misus?
Allow the strong private key protec	v	Before each use of the private key, you will be warned that your key is to be used. You can choose between th following warnings: Medium - you will always be notifier (only by a warning message); Strong - your password will be requested before every use.
dit the e-mail address		
ption allows you to delete the e-mail address of t	e certificate. This change is irreversible and in some applications may ca	use functional limitations certificate (eg e-mail).
iancik@ic.	Delete	

You will see items of your certificate. These items can not be changed. Fill the item Revocation password.

Doplněk Java(tm) Plug-In SSV Helper od vydavatele Oracle America, Inc. je připraven k použití.

Next, select "Povolit" (Enable) Java to use an.

×

Povolit <u>N</u>epovolit



AUTHORITY au	torita As. Issue of renewal certificate	
	The most impletive stap forward, was a proceeded completes, forward, the proceeded completes, forward, the proceeded	
	Law, 27/2000 Road Alexandria and minimum and minimum and minimum and minimum and minimum and minimum and and an	
Please check the information below.	. If everything is correct, a request for renewal certificate may be generated.	
Data overview		
Heading	Filled Value	
Period of validity	365	
Key Repository Type (CSP)	Microsoft Enhanced RSA and AES Cryptographic Provider	
Algorithm thumbnails	sha256WithRSAEncryption	
Allow export of the private key	Yes	
Allow the strong private key protection	Yes	
Key length	2048	
tems of the subject	Commercial certificate	
Country	CZ	
Common name	David Jančík	
Organization	První certifikační autorita, a.s.	
Serial Number	ICA - 765871	
Extended certificate items	Commercial certificate	
E-mail (rfc822Name)	jancik@ica.cz	
Key usage	Commercial certificate	
Non Repudiation	Yes	
Digital Signature	Yes	
Key Encipherment	Yes	
Data Encipherment	Yes	
Rey Agreement	Tes	
ancik@ica.cz	Addition issuing the renewal cellulicate will be sent to the e-main (e-mains).	
nformation on issuing the renew	al certificate will be sent in the language: Czech	
f you want to change the e-mail o	or the language in which you will be sent information about issuing the renewal certificate click <u>here</u>	
Update information		
Certificate sent in the ZIP format:		
C)Yes	
) a	
	INO	
Market Market and		
make the request		
	Copyright I.CA 2000-2014 All Right Reserved <u>Prvni certifikační autorita, a s.</u> <u>Contacts</u>	

Here is a recap of the request, please check the information provided here. Choose Make the request.

Aplikace vytváří chráněnou po	ložku.	
Privátní klíč CryptoAPI		
Je nastavena střední úroveň	<u>N</u> astavit úroveň z	abezpečení.

Confirmation the program Crypto API. The program creates a new RSA key for signature. Choose button OK.



Program vytváří nový klíč RSA pro výměnu.
Aplikace vytváří chráněnou položku.
Privátní klíč CryptoAPI
Je nastavena střední úroveň <u>N</u> astavit úroveň zabezpečení
OK Stomo Podrobnosti

The program creates a new RSA key for exchanging. Choose button OK.

	Zabezpečení systému Windows	×
Aplikace Ta	ato aplikace potřebuje použít kryptografický	
klíč.		
Kliknutím na t Kliknutím na t	lačítko OK udělíte oprávnění. lačítko Storno oprávnění odepřete.	
Název klíče: Tr Popis klíče: Ne	winsQD 27/05/2014 16:24:00 ení k dispozici.	
6	Chcete udělit přístup ke klíči?	
	OK Storno	
	OK Storio	

You give permission for the use of cryptographic keys. Choose button OK.





Request for the issuance of a renewal commercial certificate: ----BEGIN CERTIFICATE REQUEST-----MIIDVDCCAjwCAQAwgdQxCzAJBgNVBAYTAkNaMRcwFQYDVQQDDA5QZXRyIEphbm91xaFlazEO MAwGA1UECAwFUHJhaGExKTAnBqNVBAcMIFByYWhhLCBTbGF2xJt0w61uc2vDoSA1LzUsIDE5 MDE0M50wKwYDVQQKDCRQcnZuw60gY2VydGlmaWthxI1uw60gYXV0b3JpdGEsIGEucy4xHjAc BgNVBAsMFVbDvXZvam92w6kgb2RkxJts2W7DrTELMAkGA1UEKwwCUEoxFTATBgNVBAUTDE1D QSAtIDeSNDYxODCCASIwDQYJKoZIhveNAQEBBQADggEPADCCAQeCggEBAM4bQ%pgf9WRDK6B ZC+vOn572PcOsgHlxUjbg6Cj8FyOLY9ROKuBpq+y/3U4+bk8KbgM1VDvZe6DopULfOTu70k7 pAGANAFVWdbW6VKJA3pwd4Qy6IFMREDe9YMJR246mAWmE8E9EwhHjHamPwI12hfpVK56e2p cVP2kHEw/b/hhqhDf5F6rDq/HAwoH+ka5DPLNBpliBH31wqp0RUamRKQcOATUam98G1MJgxA dAq8zf/oots9Y0Y43/yndKjrtFIN6bDABncJyENfqsA7Dt4yFVfE2c0w2RX2UER6Q1H660IJ on3vnZueqRDOLLe+kKz3Oa0YyHR5b61g8zShtu0CAwEAAaA@MDgGCSqGS1b3DQEJDjErMCkw CwYDVR0PBAQDAgN4MBoGA1UdEQQTMBGBD2phbm91c2VrQG1jY35jejANBgkqhkiG9w0BAQ=F AAOCAQEAB8Gg=PT31CrcOcXGFRYRyNRFiY9KxihEI3tgBBGRuIro3KIh3wh3N+HGJNs5vsjX BcEORZHNdm9jiFarWm0lc75WFCafUckNpun6DJTyEnf5RY4zpWbL/74UddYYyx6Qz2Pc6VIB jj0lvVXETXjX5gTjy6Fz20HVdWrqNcfbiYW2c4qQUt0ZTQYDmGHcBBLy1w8ecmgYfW4yn144 QcD37hk2f+jJdzKwQmS0eRyebQ7M15zHM9YFKO2J=SD=0SjN1NTMOtEReYyujGz6v87eMW9J XTKLLJjBe35LwQX0gN18+IDkXnt45t6Z1M/Dw73fDqi2VSxd9PPqf4LE+SN51A== ---- END CERTIFICATE REQUEST-Send the request to be processed We Advised to that you make a backup of the private key Pollow the instructions here: http://www.ica.cz/Private-key-backup Please be aware that administration your private key is always fully responsible applicant for a certificate. Possible loss of private key can not be considered a fault the services provided by I.CA and there is no reason to issue a new certificate free of charge. If you wish to save the generated request on your hard disk, click Save the request to the disk. Save request to the disc Parameters of the key by which the request for renewal certificate will be signed: Key Repository name (CSP): Microsoft Enhanced RSA and AES Cryptographic Provider Key Repository Type (CSP): PROV_RSA_AES Key name: 20140110135024 Key type: AT_SIGNATURE

Copyright I.CA 2000-2014 All Right Reserved | Prvni certificačni autorita, a.s. | Contacts

Request for Renewal certificate has been successfully generated. Choose Send the request to be processed.

Confirmation	×
lessage:	
xml version="1.0" encoding="UTF-8"?	^
<ica> <request product_name="Certification Authority" product_version="8.01"> <header></header></request></ica>	
<type version="4">renewalrequest</type>	
<body></body>	
<keyandrequestdata></keyandrequestdata>	
IIIC6TCCAdECAQAwbDELMAkGA 1UEBhMCQ 10xFzAVBgNVBAMMDkRhdmlkIEphbsSNw61rMS0w	
WYDVQQKDCRQcnZuw60gY2VydGlmaWthxI1uw60gYXV0b3JpdGEsIGEucy4xFTATBgNVBAUT	
DEIDQSAtIDc2NTg3MTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBALpqxJduv5A9	~
The sha1 hash result:	
F78E 6A2D 563A 7C34 C1B0 616C 5974 E8CD 23A6 EE5C	
ign by the certificate:	
=CZ, CN=David Jančík, O="První certifikační autorita, a.s.", SERIALNUMBER=ICA - 765871	
gn by the certificate: =CZ, CN=David Jančík, O="První certifikační autorita, a.s.", SERIALNUMBER=ICA - 765871	

Confirm by clicking button Yes.



Крс	odpisu dat je použit váš privátní klíč pro podpis.	×
	Aplikace žádá o přístup ke chráněné položce.	
	<u>H</u> eslo pro: Privátní klíč CryptoAPI	
	OK Storno Podrobnosti	

The signature data is must be used your private key. Choose button OK.

AUTHORITY Autorita AS.	Issue of renewal certificate	B
The request for renewal certificate was successfully received	1.	
Request ID for the qualified Certificate: 5708610227963	0040007000	
Request ID for the commercial Certificate: 5708600134568	5610227363.	
You can track the status of your application with ID 5708	3600134568.	
Time of receipt: 27.05.2014 16:28:07		
Another request		
Copyright 1.0	CA 2000-2014 All Right Reserved Prvni certifikačni autorita, a.s. Contacta	

The request for renewal certificate was successfully received.

The recovered certificate with the tax document is sent to your e-mail system after payment of a pro-forma invoice, which is sent to a certification authority for the processing of the request for renewal of the certificate. To automatically submit certificate occurs in the moment of crediting payments to our account. In the e-mail message and the installation instructions for the relaunching of the PC or on the certificate to a smart card.

For the correct assignment of your payment, enter the payment order to the Message for payer number proforma invoice.

Have any problems contact our support - support@ica.cz.