



Qualified Certification Authority

Manual for Clients – legal entities

version 1.0.5

Operational Documentation

August 2007

Version	Date	Author	Note
1.0.3	09/NOV/2006	M.Šlancar	first version
1.0.4	24/MAR/2007	M.Šlancar	Authorized person can now ask for the certificate revocation also on the contact place.
1.0.5	18/AUG/2007	M.Šlancar	list of personal document in chapter 6.2 updated

Approved by:

Version	Approved by	
1.0.3	Manager QCA	manager.postsignum@cpost.cz
1.0.4	Manager QCA	manager.postsignum@cpost.cz
1.0.5	Manager QCA	manager.postsignum@cpost.cz

1 Table of contents

1 Table of contents.....	3
2 Definitions of the Terms used.....	5
3 Introduction.....	7
3.1 Foreword.....	7
3.2 Briefly about making a contract and issuing of the certificate.....	7
3.3 Sources of information on QCA.....	7
4 Prior to making a contract.....	8
4.1 Shall I apply for a qualified or commercial certificate?.....	8
4.2 Shall I use the certification service as a representative/employee of the organization, a person independently gainfully employed or nonentrepreneurial natural person?.....	8
4.3 What kinds of certificates issued by QCA will I need?.....	8
4.4 Where can I get the necessary things done?.....	9
4.5 Shall I have the MWSA Identification Sign assigned?.....	10
4.6 Shall I allow publication of my certificate?.....	10
5 Making a Contract.....	10
5.1 How to obtain the forms.....	10
5.2 How to fill in the order form.....	10
5.3 Order delivery to the business/contact place.....	11
5.3.1 Delivery by post.....	11
5.3.2 Delivery by the personal visit of the authorized person of the client.....	11
5.4 Order acceptance by the Czech Post.....	12
5.4.1 In case of the delivery by post.....	12
5.4.2 In case of the delivery by the personal visit of the authorized person of the client.....	12
5.5 How to fill in the list of applicants.....	12
5.5.1 The introductory page of the list of applicants.....	13
5.5.2 Appendix to the list of applicants for certificates for the verification of the electronic signature of the employee.....	13
5.5.3 Appendix to the list of applicants for certificates for the verification of the electronic mark of the organization.....	14
5.5.4 Change appendix to the list of applicants for certificates for the verification of the electronic signature of the employee.....	14
5.5.5 Change appendix to the list of applicants for certificates for the verification of the electronic mark of the organization.....	15
5.6 Delivery of the first list of applicants to the business or contact place.....	15
5.7 Delivery of the other lists of applicants.....	16
5.8 Change of the concluded contract with the Czech Post.....	16
6 Issuing of the certificates to applicants.....	16
6.1 Keys and electronic certificate request generation.....	16

6.2 Issuing of the certificate to the employee of the organization.....17
6.3 Installation of the issued certificate.....17
6.4 Revocation of the certificate.....18
7 Other..... 19
7.1 Invoicing..... 19
7.2 Validity of the certificate and its renewal..... 19

This document is a widely recommended strategy for the clients of the Certification Authority PostSignum QCA. We suggest that you consult minor differences from this strategy (as well as possible problems) with the concrete business or contact place.

2 Definitions of the Terms used

Since we are going to use a lot of terms in this text, we want to explain them first. We strove to explain these individual terms so that general public can easily understand them.

To denote the Qualified Certification Authority of the Czech Post - **PostSignum QCA** – the abbreviation **QCA** will be used in the text. „Qualified Certification Authority“ may appear as well.

Commercial Certification Authority of the Czech Post - **PostSignum VCA** – is an affiliated Authority to QCA. A little bit unusual abbreviation **VCA** is used to denote a commercial authority. It is derived from the Czech term.

For the Czech Post, national enterprise, the abbreviation **CP** will be used in the text.

Business place is the office of CP, where the contract between the client (legal entity) and CP can be made. This office also enters the clients and applicants to the QCA system, which must be realized before the certificate issuing. **Operator of the business place (BP Operator)** is the term denoting the service person at the business place.

Contact place is the office of CP, which issues and revokes certificates. Also the contract can be concluded there (especially in case of nonentrepreneurial natural persons, persons independently gainfully employed and small organizations). **Operator of the Registration Authority, or RA Operator**, is the term denoting the service person at the contact place.

Client is a natural person (individual), a person independently gainfully employed or legal entity (organization), who entered into a contractual relation with CP by making a contract on the provision of certification services of CP.

Legal Representative of the Organization is a person authorized to act on behalf of the specific organization. This person has been entered into, for example, Commercial Register, or any other Register. Legal Representative is, therefore, the director of the organization, city mayor, head of the association, etc. The Legal Representative signs the Certification Services Order for the QCA.

Authorized Person is the representative of the organization (one or more) who defines for the QCA which employees may ask for which certificates. The Authorized Person may be the Legal Representative, but it is better, especially for the organizations with a more complex organizational structure, to define a different person, for example the heads of the personnel department of the individual organizational units.

The term **Applicant** indicates a person who comes to the contact place to obtain the certificate. It can be either natural persons or employees of organizations. Also the legal representative and authorized person can be the applicant, of course.

The MWSA Identification Sign is a unique number of each person, allocated by the Ministry of Work and Social Affairs. The applicant for the certificate may ask for this number being included in his certificate. The MWSA Identification Sign in the certificate may be

required for the communication with the state authorities. Allocation of the Identification Sign is free of charge.

MWSA is the abbreviation of the Ministry of Work and Social Affairs.

Electronic Signature presents certain data that are bound to the given message. The electronic signature is generated by the specific person and enables to check the fact that the message has been signed by this person and the message has not been altered.

Electronic Mark is, to put it simply, the electronic signature generated automatically by the technical device. Electronic mark is subjected to different legal regulations and a different term has to be used.

A **private key/public key** pair is the basis of the operations of data decryption/encryption and electronic signature generating/verification. While the private key must remain in the possession of the given person, the public key of this person may be accessible to everybody.

Electronic Certificate Request is a data structure (in a file), used for the requesting for the certificate. The certificate request contains the public key, which will be "stored" in the issued certificate.

Certificate is a data structure bound to the certain person. Using this certificate it is possible to identify this person beyond any doubt. Using this certificate it is possible to verify the electronic signature of the given person. The issued certificate contains information about its holder, validity period, purpose of usage, public key and any other. Issuing certification authority signs the content of the certificate so that it is possible to prove that it has been issued by this authority.

Qualified Certificate is a certificate used for the verification of the electronic signature. It differs from a „common“ certificate since it was issued by the Qualified Certification Authority.

Qualified System Certificate is a certificate used for the verification of the electronic mark. Again it is issued by the Qualified Certification Authority.

Certification Policy is a document determining the purpose of the certificates issued under this policy. It further defines the conditions of certificate issuing, certificate revocation, etc.

Revocation of the certificate is a process in which the validity of the certificate is terminated before the date of real certificate expiration. The certificate must be revoked when it is impossible to use it any longer (for example because of disclosure, computer crash, etc.). After its revocation the certificate is placed into the certificate revocation list.

The Certificate Revocation List (CRL) is a data structure (in a file) containing the list of certificates that have been revoked. This list is accessible to public so that everybody can check whether his certificate (or, for example, the certificate of his partner in communication) is still valid.

3 Introduction

3.1 Foreword

Thank you for your interest in the services of the Qualified Certification Authority of the Czech Post, **PostSignum QCA**. The purpose of this document is to give you, in a comprehensive form, all the necessary information needed for the successful issue of the certificate for you or the employees of your organization.

Certification Authority **PostSignum QCA** has been, from the very beginning, prepared for the provision of services for the two very different groups of clients – organizations and nonentrepreneurial natural persons without ID No.

In the following chapters the processes concerning only organizations will be described.

3.2 Briefly about making a contract and issuing of the certificate

The Client makes a contract with the Czech Post on the provision of certification services in accordance with the common business practice.

In the order form of the certification services the authorized persons are stated. After making a contract the authorized persons deliver the Lists of Applicants to the business place, these applicants are then entered into the QCA system. From this time on the individual applicants may come to the contact place and have the certificate issued. It causes certain delay between making a contract and issuing of the certificate. On the other hand these procedures prevent the necessity of dealing with each certificate request by the Legal Representative of the client. The applicants also submit a minimum of required materials for the issuing of the certificate.

In the following chapters we are going to describe the whole process containing the order preparation, making of a contract and the final issuing of the certificate to an applicant in a great detail.

Note:

Organizations communicate, in the period of the validity of the contract, with the business place at which the contract has been made. If the contract has been made at the contact place, the organizations communicate with business place which supervises this contact place.

3.3 Sources of information on QCA

Questions of clients concerning the process of making a contract, certificate issuing and revocation will be answered by every contact or business place. If you have more complicated questions, contact user support.

You can find most information on QCA on the web link <http://qca.postsignum.cz>. We will be often referring to these pages later in the text.

4 Prior to making a contract...

4.1 Shall I apply for a qualified or commercial certificate?

Qualified certificate can be used for the communication with the state authorities. There is one disadvantage of these certificates, i.e. they can be used only for data signing while commercial certificates can be used also for data encryption.

If you want to communicate mainly with the state authorities, it is better for you to apply for the qualified certificate.

If you want to use certificates for data encryption, you will have to get the commercial certificate. In that case you should download the corresponding client manual from the web pages of PostSignum VCA.

4.2 Shall I use the certification service as a representative/employee of the organization, a person independently gainfully employed or nonentrepreneurial natural person?

If you want to use the issued certificate for the performance of duties for your employer, you will be in the position of the employee of the organization in relation to QCA.

If you want to communicate with your partners (for example state authorities) as a natural entrepreneurial person, you will be in the position of an independently gainfully employed person in relation to QCA. Download the appropriate version of this document.

If you want to use the issued certificate for your private purposes, you will be in the position of a nonentrepreneurial natural person in relation to QCA. Download the appropriate version of this document.

4.3 What kinds of certificates issued by QCA will I need?

Each Certification Authority offers quite specialized services. The client should decide in advance what kind of certificate he/she will need. Appropriate information on the issued certificates is stated in the certification policy, which can be found on the web pages of QCA. In this chapter we will try to state the most important advices, which should help you in choosing the right kind of certificate. We will further state important information concerning the issuing of certificates.

- QCA certificates are always issued on the basis of the electronic certificate request. Your application should be able to generate the certificate request together with your key pair. On the web pages of QCA it is possible to generate the key pair and the electronic certificate request; key pair with the certificate can then be imported into your application.
- Certificates for employees of organizations may be issued under these policies:
Certificates for the verification of the electronic signature of the employee,
Certificates of the organization for the verification of the electronic mark.

Certificates issued under the first policy are qualified certificates designed for persons. Certificates issued under the second policy are qualified system certificates and are designed for the technical devices (applications on servers).

- Certificates for the verification of the electronic signature can be used in communication with the state authorities. Especially if you want to communicate with the Ministry of Work and Social Affairs, it is important to include the MWSA Identification Sign in your certificate. Other state authorities may require this number in certificate in the future.
- Requests for the certificates for the verification of the electronic mark will be submitted mostly by the state authorities that intend to operate the so called electronic registry.
- According to the law the certificates issued by QCA cannot be used for data encryption. In that case consider the use of commercial certificates issued by the affiliated authority **PostSignum VCA**.
- Certificates issued for organizations contain the data „ identification number and a (business) name of the organization“ and the name of the employee (or the name of the marking device), optionally also the data „the name of the organizational unit“, „e-mail address“ and „the position of the employee in the organization“.
- Even if we talk about an e-mail address as an optional data we recommend that you have the certificate issued with the e-mail address. The certificate without a (correct) e-mail address cannot be used for sending the undersigned e-mail messages. E-mail address in qualified certificates for employees is now **mandatory**.

4.4 Where can I get the necessary things done?

The following table gives the list of activities and office where you can get the necessary things done. These activities are explained later in the text.

Activity	Business place	Contact place
Making a contract	yes	yes
Entering the basic information about the client into the QCA system	yes	yes
Entering the data from the lists of applicants into the QCA system	yes	yes*
Entering the data from other lists of applicants into the QCA system	yes	no
Changes in the contract / lists of applicants	yes	no
Certificate issuing	no	yes
Certificate revocation	no	yes

* Valid only during the so called fast entering of the client into the QCA system at the contact place:

- An authorized person delivers in person the order together with the list of applicants to the contact place.
- The list of applicants may contain just the appendix for the issuing of the certificate for the verification of the electronic signature of the employee without the filled in certificate data „OU (organizational unit)“

- *After entering the data into the system the issuing of the certificate for authorized person may follow (if this person is specified on the list of applicants as an applicant).*

This limitation is valid only for the first hand-over of the list of applicants. In other lists of applicants it is possible to apply for the certificates for the verification of the electronic mark and certificates containing organizational units.

4.5 Shall I have the MWSA Identification Sign assigned?

The MWSA Identification Sign is a number assigned by the Ministry of Work and Social Affairs (MWSA), which quite unequivocally identifies you as a person. It is similar to your Personal Identification Number but it is impossible to derive the date of birth and sex from the MWSA Identification Sign.

The MWSA Identification Sign may be required for the communication with some state authorities. That is why we recommend you to apply for its assignment and placing to the issued certificate. Assignment of the MWSA Identification Sign is free of charge.

4.6 Shall I allow publication of my certificate?

Allowing or prohibiting the publication of the certificate is set in the list of applicants.

It means that you may agree with providing access to your certificate to all users who can upload download it from the web pages or address directory services of PostSignum QCA.

Since the certificate is, in fact, a public data entity, refuse its publication only for really serious reasons.

5 Making a Contract

The process of making a contract is aimed at organization with a more complex organizational structure. Some procedures may be simplified for “smaller” organizations (definition of the authorized persons, making a contract, delivery of the lists of applicants and issuing a certificate during one visit tot the contact place).

Making a contract consists in the order preparation by the client that becomes a contract on the provision of certification services after the acceptance by CP. An authorized person further delivers a prepared list of applicants to the Czech Post. The list can be delivered together with the order or separately after the conclusion of a contract.

5.1 How to obtain the forms

The client downloads the order form and list of applicants from the web pages of QCA. These documents may also be sent to him by the business or contact place.

5.2 How to fill in the order form

Fill in the form following these instructions:

- In point **1** in the section **Provider** the data on the organizational unit of CP you will be making a contract with are set automatically. Check the address to make sure you have the correct version of the order. In the **Client** section enter the business data of your organization.

- In point **2** check whether you want to make a contract for the definite or indefinite period. It is more common to make a contract for the indefinite period.
- In point **3** check which certificates you want to apply for (qualified and/or commercial). You can check one or both boxes.
- In point **4.4** choose whether you intend to give consent to the use of the contact data of your organization for the purposes of marketing and advertising of the products and services of CP. By checking the box you indicate that you withhold your consent.
- In point **5** fill in identification data of your legal representative, place and date.
- In **Appendix 1** to the order state the list of authorized persons who will act on behalf of the organization with QCA. Specify the name and surname of each authorized person and his/her identification number.

Print the filled in form in two copies. The authorized persons will sign the appendix to the order to confirm that the Czech Post is authorized to process their personal data. The legal representative signs both copies of order and appendix to order.

No authorization of the signature (by the notary or other way) is required.

Note:

In case of organizations with a small number of employees the authorized person may be the legal representative (and probably the only one). In “larger” organizations it is most appropriate to choose someone else as an authorized person, for example the employee of the personnel department in each organizational unit of the organization.

5.3 Order delivery to the business/contact place

5.3.1 Delivery by post

Send the filled in and signed order to the business or contact place.

If your organization **is entered in the Commercial Register**, attach to the order:

- original of the entry from the Commercial Register (not older than 3 months), *or*
- copy of the entry from the Commercial Register verified by the notary (original must not be older than 3 months).

If your organization **is not entered in the Commercial Register**, attach to the order:

- original of other document in which the legal representative and ID No of the organization are stated, *or*
- copy of other document in which the legal representative and ID No of the organization are stated (copy must be verified by the notary).

5.3.2 Delivery by the personal visit of the authorized person of the client

Much more convenient and faster method of delivery is a personal visit of the authorized person of the client to the business or contact place.

The authorized person brings the filled in and signed form.

If your organization **is entered in the Commercial Register**, attach to the order:

- original of the entry from the Commercial Register (not older than 3 months), *or*
- copy of the entry from the Commercial Register verified by the notary (original must not be older than 3 months).

If your organization **is not entered in the Commercial Register**, attach to the order:

- original of other document in which the legal representative and ID No of the organization are stated, *or*
- copy of other document in which the legal representative and ID No of the organization are stated (copy must be verified by the notary).

If the authorized person does not intend to come twice to the business/contact place, he/she may bring the lists of applicants as well (see chapters 5.5 and 5.6).

5.4 Order acceptance by the Czech Post

5.4.1 In case of the delivery by post

If the BP/RA Operator receives documents for the making a contract from the client by post, he/she checks the data in the documents, and if these are correct, accepts the order. Then he/she informs the authorized person of the client of the fact that the contract has been made and the client may bring the filled in lists of applicants (see chapters 5.5 and 5.6). The client receives the signed acceptance of the order by post.

5.4.2 In case of the delivery by the personal visit of the authorized person of the client

If the documents for the making a contract were brought by the authorized person of the client, BP/RA Operator checks the data in the documents and, if correct, accepts the order. The authorized person will get one copy of the undersigned order from the BP/RA Operator. If the authorized person brought the lists of applicants, the procedure described in chapter 5.6 follows.

5.5 How to fill in the list of applicants

You indicate in the list of applicants which certificates will be issued to which employees. The form of the list of applicants consists of several files, which contain

- the introductory page of the list of applicants,
- appendixes for the issuing of the certificates to the applicants under the individual certification policies.
- change appendixes for the administration of the applicants and issued certificates (change of applicant's personal data or certificate data, locking or removing the applicant from the QCA system, stopping the certificate issuing).

The introductory page and an arbitrary number of appendixes form the part of the resulting list of applicants.

The lists of applicants are filled in using these instructions:

5.5.1 The introductory page of the list of applicants

- Enter the contract number. This data can be found on the concluded contract, it has been added by the business or contact place. Leave the field blank, if the contract was not yet concluded.
- In point 1 fill in the information on your organization (the same as on the order).
- In point 2 fill in the identification data of the authorized person who prepares the list of applicants.
- In point 3 fill in the number of the produced appendixes to the list of applicants.

The introductory page is finally printed. The authorized person does not sign it for the time being.

5.5.2 Appendix to the list of applicants for certificates for the verification of the electronic signature of the employee

- First fill in the appendix number.
- Next, enter the contract number. This data can be found on the concluded contract, it has been added by the business or contact place. Leave the field blank, if the contract was not yet concluded.
- Enter applicant's identification data into the first table – name and surname and identification number.
- Enter mandatory certificate data into the second table. State applicant's name and surname into the CN field. State the number of the applicant in organization into the OU field. If you do not use employee numbers in your organization (or if you do not want to include it in the certificate), create a special numbering system for this purpose. Each employee must have a unique number assigned, there must not be two employees with the same number. State applicant's e-mail address as last mandatory data.
- Still in the second table, you can fill in the optional data – name of the organizational unit (the name of the section or branch) and position in the organization (i.e. position at work). You can also leave the optional data empty.
- Choose under the tables whether the certificate is to be published on the web pages and on the LDAP server QCA. Checking the box indicates that the certificate will not be accessible to the general public. But we recommend you to allow the publication of the certificate (i.e. leave the box empty).
- You also check whether the certificate should contain the MWSA Identification Sign. If you want to communicate with the state authorities we recommend you to check the box. Assignment of the MWSA Identification Sign is free of charge.
- If the applicant has checked that he/she require the MWSA Identification Sign he/she has to fill in the second page of the form. There is a form in which he/she gives the consent with the provision of personal data for MWSA. Filling in and undersigning the form is a necessary condition for the assignment of the MWSA Identification Sign.

The appendix to the list of applicants is printed and undersigned by the appropriate applicant. The form for MWSA must be printed on the separate paper, do not use the double-side print.

5.5.3 Appendix to the list of applicants for certificates for the verification of the electronic mark of the organization

- First fill in the appendix number.
- Next, enter the contract number. This data can be found on the concluded contract, it has been added by the business or contact place. Leave the field blank, if the contract was not yet concluded.
- Enter applicant's identification data into the first table – name and surname, identification number and the number of the applicant in the organization. If you do not use employee numbers in your organization (or if you do not want to include it in the certificate), create a special numbering system for this purpose. Each employee must have a unique number assigned, there must not be two employees with the same number.
- Enter mandatory certificate data into the second table. State the name of marking device into the CN field.
- Still in the second table, you can fill in the optional data – name of the organizational unit (the name of the section or branch) and e-mail address. You can also leave the optional data empty. We strongly recommend you to enter the e-mail address!
- Choose under the tables whether the certificate is to be published on the web pages and on the LDAP server QCA. Checking the box indicates that the certificate will not be accessible to the general public. But we recommend you to allow the publication of the certificate (i.e. leave the box empty).

The appendix to the list of applicants is printed and undersigned by the appropriate applicant.

If the name of the certificate contains the so called domain name (e.g. **cpost.cz** or **mydomain.com**) the authorized person must prepare the declaration of domain owner. He/she declares there that the organization owns specified domain. The declaration form can be downloaded from web pages of QCA.

(However, we expect that clients need no system qualified certificates containing the domain names in most cases.)

5.5.4 Change appendix to the list of applicants for certificates for the verification of the electronic signature of the employee

- First fill in the appendix number.
- Next, enter the contract number. This data can be found on the concluded contract, it has been added by the business or contact place. Leave the field blank, if the contract was not yet concluded.
- Enter identification data of applicant for the certificate into the first table – name and surname and identification number.
- In the second table fill in the current values of mandatory and optional data of the corresponding certificate.
- In the Applicant's data maintenance part, you can change applicant's personal data, lock, unlock or completely remove him/her from the QCA system.

- In the Certificate data maintenance part, you can change the certificate data, publication of the certificate, inserting the MWSA Identification Sign to the certificate or completely stop the issuing of the certificate to applicant. If you request inserting the MWSA Identification Sign to the certificate the applicant must fill in the third page of the form. There is a form in which he/she gives the consent with the provision of personal data for MWSA. Filling in and undersigning the form is a necessary condition for the assignment of the MWSA Identification Sign.

The printed appendix is undersigned by the applicant. Also the authorized person can undersign the appendix in some cases, which is specified on the appendix.

5.5.5 Change appendix to the list of applicants for certificates for the verification of the electronic mark of the organization

- First fill in the appendix number.
- Next, enter the contract number. This data can be found on the concluded contract, it has been added by the business or contact place. Leave the field blank, if the contract was not yet concluded.
- Enter identification data of applicant for the certificate into the first table – name and surname, identification number and the number of the applicant in the organization.
- In the second table fill in the current values of mandatory and optional data of the corresponding certificate.
- In the Applicant's data maintenance part, you can change applicant's personal data, lock, unlock or completely remove him/her from the QCA system.
- In the Certificate data maintenance part, you can change the certificate data, publication of the certificate or completely stop the issuing of the certificate to the applicant.

The printed appendix is undersigned by the applicant. Also the authorized person can undersign the appendix in some cases, which is specified on the appendix.

If there is a change of certificate name and the new name contains the so called domain name (e.g. **cpost.cz** or **mydomain.com**) the authorized person must prepare the declaration of domain owner. He/she declares there that the organization owns specified domain. The declaration form can be downloaded from web pages of QCA. (However, we expect that clients need no system qualified certificates containing the domain names in most cases.)

5.6 Delivery of the first list of applicants to the business or contact place

The delivery of the lists of applicants depends on the chosen way of verification of the signature of the authorized person:

- The authorized person signs the list of applicants in the presence of the notary (signature verified by the notary). The list of applicants is sent to the **business place** by post. In this case you pay to the notary for the verification of the signature.
- The authorized person brings the list of applicants to the **contact or business place** in person and signs it in the presence of the CP employee (signature verified by the CP employee). In that case the signature verification is free of charge.

- If the authorized person owns the certificate issued by the certification authority of the Czech Post (i.e. PostSignum QCA or PostSignum VCA), he/she can send the signed electronic version of the list of applicants to the **business place** by e-mail. But he/she must also mail the signed original of the list of applicants on paper (because of the written consent with the processing of the personal data by the Czech Post).

The business place takes over the lists of applicants and enters the applicants into the QCA system. During this process the presence of the authorized person is not necessary, he/she will be notified about the entering of all applicants into the QCA system by e-mail or phone. Then the applicants concerned may come to the contact place and have the certificate issued.

The contact place may process the list of applicants only in case of the so called fast entering of the client into the system (see the chapter 4.4). In other cases the contact place can only send the document for the processing to the business place.

5.7 Delivery of the other lists of applicants

Preparing of another lists of applicants can be necessary due to these reasons:

- organization wants to have certificates to new applicants issued
- organization wants to change the data in the already issued certificates or terminate their issuing to the applicants
- personal data of the current applicants have changed
- remove of the applicants from the QCA system

Again, the authorized person has three options of lists of applicants delivery that depend on the chosen way of verification of the signature of the authorized person. See chapter 5.6.

Other lists of applicants may be processed only by the business place, that is why the document is sent to the business place after the verification of the signature of the authorized person by the CP employee at the contact place, which may cause delay.

The authorized person is informed about the entering of all applicants to the QCA system by e-mail or phone.

5.8 Change of the concluded contract with the Czech Post

In case of change of business data of organization, list of authorized persons or another stipulations in the contract the clause to the contract is concluded with the business place in appropriate region.

6 Issuing of the certificates to applicants

6.1 Keys and electronic certificate request generation

Prior to issuing the certificate the applicant must generate a key pair and electronic certificate request on his computer. Appropriate tools for this purpose are offered on the web pages of

QCA. You can also download manuals describing the procedures of key generation in these tools from the pages.

6.2 Issuing of the certificate to the employee of the organization

The applicant for the certificate brings to the contact place the diskette with the electronic certificate request and one valid personal document:

- passport issued by home country, foreign passport, stay permit, traveling identity card or stay permit issued by Czech authority (Citizens of selected European states can also submit an identity card issued by home country.)

During the process of the certificate issuing the RA Operator checks the identity of the applicant. He/she copies the personal document of the applicant in accordance with the law No. 227/2000 Coll. on the electronic signature.

Written request for the certificate is printed which the applicant approves by his/her signature. On the request there is stated the so called revocation passphrase which relates to the process of the certificate revocation (see chapter 6.4). This passphrase is determined by the applicant. There is no need to remember it since it will be stated in the certificate issuing protocol. The passphrase should be different from other passwords which the applicant uses.

After the issuing of the certificate the applicant will accept the issued certificate. Then the certificate issuing protocol is produced. The issued certificate, certificates and CRLs of the certification authorities and certification policy under which the certificate has been issued are copied on the diskette.

The applicant has also the right to refuse the issued certificate. In that case the certificate non-issuing protocol is printed and the certificate is revoked.

Attention! In case of the applicant refuses the issued certificate a new one cannot be issued right away. The applicant must generate a new key pair and certificate request and must visit the contact place again.

6.3 Installation of the issued certificate

The certificate is installed into the application in which the keys have been generated. If this application serves only for the key generation the key export to the file following the import to the target application is realized.

Together with the issued certificate it is necessary to install also the certificates of the certification authorities of PostSignum QCA into the target application. You will find them on the diskette with the issued certificate or on the web pages of PostSignum QCA.

Note: In case of e-mail clients Outlook/Outlook Express it is necessary to install all certificates (and keys) into the OS Windows; in other cases probably directly to the target applications.

Procedures of the installation of the issued certificate and certificates of the certification authorities form parts of the manuals describing the key and certificate request generation. These manuals may be downloaded from the web pages of QCA.

6.4 Revocation of the certificate

It may happen that the applicant cannot use his/her keys and issued certificate, for example for the reasons of disclosure of the private key (i.e. the computer is stolen, etc.), but also because of the computer crash. In that case it is necessary to ask for the revocation of your certificate corresponding to the disclosed (lost) private key.

Revocation request is submitted at the contact place. The applicant can visit the place in person or contact it by phone or e-mail. To enable the identification of the appropriate certificate the applicant must tell the operator the serial number of his/her certificate or its name and issuing date. These data can be found in the certificate issuing protocol. The applicant must specify which certification authority issued this certificate - whether QCA or VCA.

The applicant further tells the operator the revocation passphrase which is, again, stated in the certificate issuing protocol. By this process it is verified whether the applicant is entitled to ask for the revocation of the given certificate. If the passphrase is incorrect or the applicant does not know it, he/she must come to the contact place in person (with one valid personal document) and fill in the written request for the revocation of the certificate (sample request may be downloaded from the web pages of QCA). The certificate is revoked after the verification of the personal document. The document is again copied in the same way as by the issuing of the certificate.

At the end of this process the applicant will get the certificate revocation protocol.

After working hours of the contact places the applicant can contact the so called nonstop revocation service via phone or e-mail (contact data are stated on the web pages of QCA). Also in that case it is necessary to give the same certificate data and revocation passphrase. If the revocation passphrase is not verified, the operator will recommend the visit to the contact place during working hours.

Also the **authorized persons** can ask for the revocation of certificates issued to applicants (employees of organization). Authorized person prepares the certificate revocation request; the sample form can be downloaded from the web pages of QCA. The request is delivered to the Czech post by one of these ways:

- Authorized person prints and signs the request. He/she delivers it in person to the nearest contact place where the certificate revocation will be performed. The personal document of authorized person is also required.
- Authorized person prints and signs the request. He/she sends it to the QCA center by post or fax. (After the working hours of QCA center, send the request to a fax number of the nonstop revocation service.)
- Authorized person sends the prepared electronic document to the e-mail address of QCA center via the electronically signed e-mail. (The authorized person must own „personal“ certificate issued by PostSignum QCA or PostSignum VCA certification authority.)

The verification of the signature on the written request (by the notary or any other way) is **NOT** required.

Contact data of the QCA center, nonstop revocation service and contact places are available on the web pages of QCA.

7 Other

7.1 Invoicing

The price list of QCA services forms a part of the contract. Current version of the price list can be obtained on the web pages of QCA.

The price for the QCA services is invoiced under the valid price list and contract according to the number of issued certificates. The invoice is not issued in case no certificates have been issued. The invoice is sent to the address stated in the contract.

7.2 Validity of the certificate and its renewal

The validity of the certificate lasts one year. After that time it is necessary to ask for the new certificate.

If no change of applicant's personal data or certificate data occurred, it is possible go to contact place to issue the certificate – procedure in chapter 6 will be performed.

In addition to personal visit it is also possible to apply for the subsequent certificate by the electronic way. The applicant sends an undersigned e-mail containing the request for subsequent certificate to electronic registry of PostSignum.

If a change of data occurred, the authorized person submits the change lists of applicants to business place. Business place performs the necessary changes in the QCA system and then informs the authorized person. Then the applicants can come to the contact place to issue the certificate.

The certificate renewal is, again, subject to payment by invoice. The price of the certificate is determined under the valid price list.