



Qualified Certification Authority

Manual for Clients – Nonentrepreneurial Natural Persons

version 1.0.4

Operational Documentation

August 2007

Manual for Clients - Nonentrepreneurial Natural Persons version 1.0.4

Version	Date	Author	Note
1.0.3	09/NOV/2006	M.Šlancar	first version
1.0.4	18/AUG/2007	M.Šlancar	list of personal document in chapter 6 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 Table of contents

1 Table of contents	3
2 Definitions of the Terms used	5
3 Introduction	6
3.1 Foreword.....	6
3.2 Briefly about making a contract and issuing of the certificate.....	6
3.3 Sources of information on QCA.....	7
4 Prior to making a contract	7
4.1 Shall I apply for a qualified or commercial certificate?.....	7
4.2 Shall I use the certification service as a representative/employee of the organization, a person independently gainfully employed or nonentrepreneurial natural person?.....	7
4.3 What kinds of certificates issued by QCA will I need?.....	7
4.4 Where can I get the necessary things done?.....	8
4.5 Shall I have the MWSA Identification Sign assigned?.....	8
4.6 Shall I allow publication of my certificate?.....	9
5 Preparation for making a contract	9
5.1 How to obtain the forms.....	9
5.2 How to fill in the order form.....	9
5.3 How to fill in the client form.....	10
5.3.1 Client form for certificates for the verification of the electronic signature of the natural person.....	10
5.3.2 Client form for certificates for the verification of the electronic mark of the natural person.....	10
5.3.3 Change client form for certificates for the verification of the electronic signature of the natural person.....	11
5.3.4 Change client form for certificates for the verification of the electronic mark of the natural person.....	11
5.4 Keys and electronic certificate request generation.....	12
6 Contract conclusion and issuing of the certificate	12
6.1 Order acceptance by the Czech Post.....	12
6.2 First client form acceptance by the Czech Post.....	13
6.3 Issuing of the certificate.....	13
6.4 Installation of the issued certificate.....	13
6.5 Revocation of the certificate.....	13
6.6 Delivering of another client forms.....	14
6.7 Change of the concluded contract with the Czech Post.....	14
7 Other	15
7.1 Invoicing.....	15

7.2 Validity of the certificate and its renewal..... 15

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.

Contact place is the office of CP, which issues and revokes certificates. Also nonentrepreneurial natural persons make their contracts there. **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.

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.

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.

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 nonentrepreneurial natural persons will be described.

3.2 Briefly about making a contract and issuing of the certificate

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

Suggested principles presuppose immediate issuing of the certificate after making a contract. Nonentrepreneurial natural persons are completely attended to at the contact places.

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

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. Download the appropriate version of this document.

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.

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 natural persons may be issued under these policies:

**Certificates for the verification of the electronic signature of the natural person,
Certificates for the verification of the electronic mark of the natural person.**

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. Natural persons will not, in most cases, need these certificates.
- 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 the nonentrepreneurial natural persons contain the data „name and surname of a person“ (or name of the marking device), optionally also the data „address of the natural person“ and „e-mail address“.
- 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 natural persons is now **mandatory**.

4.4 Where can I get the necessary things done?

Nonentrepreneurial natural persons can get all the necessary things done at a contact place.

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 client form.

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 Preparation for making a contract

Natural persons will apply in most cases for certificates for the verification of the electronic signature. However, this manual will describe also the applying for certificates for the verification of the electronic mark.

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. The client gives also the filled client form to the Czech Post. Immediately after making a contract a certificate is issued to the client.

5.1 How to obtain the forms

The client downloads the order form and client form 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 your name and address.
- 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 your personal data for the purposes of marketing and advertising of products and services of CP. By checking the box you indicate that you withhold your consent.
- In point **5** fill in your identification data, place and date.

Print the filled in form in two copies. Do not sign the order for the time being.

5.3 How to fill in the client form

In the client form, you specify the kind and content of certificates that will be issued to you. There are various types of client forms:

- client forms for certificate issuing according to the certification policies,
- change client forms to maintain your personal data and issued certificates (change of your personal data or certificate data, locking or removing from the QCA system, stopping the certificate issuing).

The client forms are filled in using these instructions:

5.3.1 Client form for certificates for the verification of the electronic signature of the natural person

- Enter the contract number. This data can be found on the concluded contract, it has been added by the contact place. Leave the field blank, if the contract was not yet concluded.
- Enter your identification data into the first table – name and surname and identification number.
- Enter mandatory certificate data into the second table. State your name and surname into the CN field. State your e-mail address as another mandatory data.
- Still in the second table, you can fill in one optional data – address of your residence.
- 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 you have checked that you require the MWSA Identification Sign you have to fill in the second page of the form. There is a form in which you give your consent with the provision of your personal data for MWSA. Filling in and undersigning the form is a necessary condition for the assignment of the MWSA Identification Sign.

Print the client form but don't sign it yet. The form for MWSA must be printed on the separate paper, do not use the double-side print.

5.3.2 Client form for certificates for the verification of the electronic mark of the natural person

- Enter the contract number. This data can be found on the concluded contract, it has been added by the contact place. Leave the field blank, if the contract was not yet concluded.
- Enter your identification data into the first table – name and surname and identification 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 one optional data – address of your residence and e-mail address. 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).

Print the client form but don't sign it yet.

If the name of the certificate contains the so called domain name (e.g. **cpost.cz** or **mydomain.com**) you must prepare the declaration of domain owner. You declare there that you own specified domain. The declaration form can be downloaded from web pages of QCA.

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

5.3.3 Change client form for certificates for the verification of the electronic signature of the natural person

- Enter the contract number. This data can be found on the concluded contract, it has been added by the contact place. Leave the field blank, if the contract was not yet concluded.
- Enter your identification data 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 Client data maintenance part, you can change your personal data, lock, unlock or completely remove yourself 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. If you request inserting the MWSA Identification Sign to the certificate you must fill in the third page of the form. There is a form in which you give your consent with the provision of your personal data for MWSA. Filling in and undersigning the form is a necessary condition for the assignment of the MWSA Identification Sign.

Print the client form but don't sign it yet.

5.3.4 Change client form for certificates for the verification of the electronic mark of the natural person

- Enter the contract number. This data can be found on the concluded contract, it has been added by the contact place. Leave the field blank, if the contract was not yet concluded.
- Enter your identification data 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 Client data maintenance part, you can change your personal data, lock, unlock or completely remove yourself 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.

Print the client form but don't sign it yet.

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**) you must prepare the declaration of domain owner. You declare there that you own specified domain. The declaration form can be downloaded from web pages of QCA.

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

5.4 Keys and electronic certificate request generation

Since after making a contract the issuing of the certificate follows, you have to generate a key pair and electronic certificate request on your 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.

6 Contract conclusion and issuing of the certificate

You come to the contact place with:

- printed order forms,
- printed client form,
- electronic certificate request,
- **two** personal documents:
 - primary document:* passport issued by home country, foreign passport, 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 as primary document.)
 - secondary document:* passport issued by home country, foreign passport, traveling identity card, stay permit issued by Czech authority or driving license of the European Union
(Citizens of any country can also submit an identity card issued by home country as secondary document.)

You will sign the orders in the presence of the employee of the Czech Post.

6.1 Order acceptance by the Czech Post

RA operator checks your identity using both personal documents. He (she) copies your personal documents because of the consequent issuing of the certificate under the Law No 227/2000 Coll. on the electronic signature.

RA operator checks the data in the order form and, if correct, accepts it. You will get one copy of the undersigned order from the operator. The operator then enters your personal data in the QCA system.

6.2 First client form acceptance by the Czech Post

You will sign the client form(s) in the presence of the RA operator.

The operator then uses the client form to enter the necessary data in the QCA system. Then the issuing of the certificate can begin.

6.3 Issuing of the certificate

Written certificate request is printed and you approve it by your signature.

On the written request you state the so called revocation passphrase which relates to the process of the certificate revocation (see chapter 6.5). This passphrase is determined by you. You do not have to remember it since it will be stated in the certificate issuing protocol. The password should be different from other passwords, which you use.

After the issuing of the certificate you 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.

You have 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 you refuse the issued certificate a new one cannot be issued right away. You must generate a new key pair and certificate request and you must visit the contact place again.

6.4 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.

6.5 Revocation of the certificate

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

Revocation request can be submitted at the contact place. You can visit the place in person or contact it by phone or e-mail. To enable the identification of the appropriate certificate you must tell the operator the serial number of your certificate or its name and issuing date. You will find these data in the certificate issuing protocol. Specify which certification authority issued this certificate - whether QCA or VCA.

You further tell the operator the revocation passphrase, which is, again, stated in the certificate issuing protocol. By this process it is verified whether you are entitled to ask for the revocation of the given certificate. If the passphrase is incorrect, you must come to the contact place in person (bring two personal documents) 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 your personal documents. These documents are again copied in the same way as by the issuing of the certificate. At the end of this process you will get the certificate revocation protocol.

After working hours of the contact places you 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 you the visit to the contact place during working hours.

6.6 Delivering of another client forms

Preparing of another client forms can be necessary due to these reasons:

- you want to issue new certificates containing different data
- you need to change data in the currently issued certificates or stop issuing of the certificates
- a change of your personal data happened
- you want to remove yourself from the QCA system

You deliver the client form(s) to the contact place in person and sign the documents in presence of the CP employee.

RA operator uses the client form to enter the changes in the QCA system. Then a new certificate or certificate with changed data can be issued.

6.7 Change of the concluded contract with the Czech Post

In case of change of your personal data or another stipulations in the contract the clause to the contract is concluded with the business place in appropriate region. More details on concluding the clause are negotiated with the business place (e.g. sending the clause by post or signing the clause on the contact place).

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. The issued certificate is paid for in cash at the contact place. Payment order is included in the certificate issuing protocol.

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 your personal data or certificate data occurred, it is possible go to contact place to issue the certificate – procedures in chapters 5.4, 6.3 and 6.4 will be performed.

In addition to personal visit you can also apply for the subsequent certificate by the electronic way. Send an undersigned e-mail containing the request for subsequent certificate to electronic registry of PostSignum.

If a change of data occurred, submit the change client forms to contact place. Contact place performs the necessary changes in the QCA system and then informs you. Then you can come to the contact place to issue the certificate.

Certificate renewal is invoiced, again. The price for the certificate is invoiced under the valid price list and contract. You pay for certificate issued on contact place in cash; the subsequent certificate is paid in advance by sending the payment to a special account of Czech Post. You receive the account number by e-mail.