Notice
This English translation has no official character. The only authentic texts are the German, French and Italian versions published in the Official Compendium of Federal Law (AS).

Ordinance on certification services in the area of the electronic signature

(Ordinance on the electronic signature, VZertES)

of 3 December 2004 (status: 1 August 2011)

The Swiss Federal Council,

having regard to art. 4, 6 para. 1, 7 para. 3, 8 para. 2, 9 para. 3, 11 para. 4, 13 para. 2, and 20 of the federal act of 19 December 2003 on certification services in the area of the electronic signature (ZertES)[1],
having regard to art. 59*a*, para. 3, of the code of obligations (CO)[2],[3]

decrees:

Art. 1 Recognition bodies

[1] The Swiss Accreditation Service (SAS) of the State Secretariat for Economic Affairs[4] accredits the recognition bodies of certification service providers in accordance with the provisions of the ordinance of 17 June 1996 on accreditation and designation[5].

[2] If no accredited recognition body exists, the Federal Office of Communications (the Office) recognises certification service providers.

Art. 2 Insurance

[1] The certification service provider which intends to obtain recognition must conclude

---

AS **2004** 5101
[1] SR **943.03**
[2] SR **220**
[3] New content according to No. I of the ordinance of 6 June 2011, in force since 1 August 2011 (AS **2011** 3457).
[4] Formerly attached to the METAS.
[5] SR **946.512**

third-party liability insurance for an amount of at least CHF 2 million for each case of insurance and CHF 8 million per year of insurance.

[2] In place of insurance, it may produce an equivalent guarantee.

Art. 3 Signature and signature verification keys

[1] In order to be able to be the subject of qualified certificates, the signature and signature verification keys must be of sufficient length and must implement a recognised algorithm in order to be able to withstand cryptographic attacks throughout the period of validity of the qualified certificate.

[2] The Office shall regulate the details in the technical and administrative regulations and set the requirements applicable to signature-creation devices. It may also set the requirements for the signature verification process.

Art. 4 Qualified certificates

[1] The Office shall regulate the format of qualified certificates.

[2] Certification service providers may issue qualified certificates for themselves as legal entities.

Art. 5 Issue of qualified certificates

[1] Recognised certification service providers must require persons requesting a qualified certificate to present personally a passport, a Swiss identity card or an identity card recognised in order to enter Switzerland.[6]

[2] They must in addition require persons who have specific attributes to present the documents proving these attributes, such as, for example, a power of attorney. When the specific attributes refer to an entry in the commercial register, the following documents must also be presented:

a. a current certified extract from the commercial register;

b. the statement of acceptance:

   1. of the holder, in the case of an individual undertaking;

   2. of the associates, in the case of a company of persons;

   3. of the highest management or administration body, in the case of a legal entity.

[3] Recognised certification service providers may accept a request accompanied by a qualified electronic signature when a person without specific attributes and identified in accordance with para. 1 less than six years previously requests a new qualified certificate.

---

[6] New content according to No. I of the ordinance of 6 June 2011, in force since 1 August 2011 (AS **2011** 3457).

[4] The identity of a person using a pseudonym must be established in accordance with paras 1 to 3.

Art. 6 Ban on copying or conserving duplicates

Recognised certification service providers may neither establish nor conserve duplicates of their clients' signature keys.

Art. 7 Revocation of qualified certificates

[1] Recognised providers shall inform their clients of the manner of requesting revocation of qualified certificates. They must be able to receive revocation requests at all times.

[2] They must guarantee third-party online access to the information relating to the revocation of a qualified certificate up to the expiry of the latter's validity. This information shall include the serial number of the certificate, mention of the fact that it is revoked and the date and time of revocation. It must be authenticated by the qualified electronic signature of the recognised provider.

[3] Recognised certification service providers must be able to provide the information enabling verification of qualified certificates which are no longer valid for eleven years from the expiry of the certificates.

Art. 8 Directory service for qualified certificates

The Office shall determine the requirements which the recognised provider offering a directory service must satisfy.

Art. 9 Activities log

[1] Recognised certification service providers shall archive the entries relating to their activities as well as the corresponding documentation for eleven years.

[2] For activities relating to certificates, the period commences from the expiry of the latter.

[3] For certificates which have been issued on the basis of a request associated with a qualified electronic signature (art. 5 para. 3), the entries and documentation relating to the identification of their holders according to art. 5 para. 1 must be conserved until the end of the eleven-year period which applies to the last of the certificates established in this way.

Art. 10 Cessation of activity

[1] Recognised certification service providers shall announce immediately, but at least 30 days in advance, to the SAS and to the recognition body that they are going to cease their activity.

[2] When no other recognised certification service provider exists to which the SAS could transfer the tasks pursuant to art. 13 para. 2, ZertES, the office shall discharge the following tasks:

a. it shall continue to process requests for revocation of qualified certificates.

b. it shall guarantee third-party online access to the information relating to the revocation of qualified certificates up to the expiry of the latter.

c. it shall update and archive the activities' log and corresponding documentation.

3 It may itself revoke certificates which are still valid.

Art. 11 Security measures

1 The holder of a qualified certificate must retain exclusive access to its signature key. To the extent that it may be required, the holder must keep the signature-creation device in its possession or place it in a secure location.[7]

2 In the event of loss or theft of the signature-creation device, the holder of a qualified certificate must request revocation of the latter within the shortest possible time. The same applies to a holder who knows or has reason to believe that a third party may have had access to the signature key.

3 The signature-creation device activation data (the activation data) must not refer to the personal data of the holder of a qualified certificate.

4 The transcriptions of the activation data must be archived in a secure location and separately from the signature-creation device.

5 The holder of a qualified certificate must modify the activation data when it knows or has reason to believe that a third party has had knowledge thereof. If it is unable to modify the data itself, it must request revocation of the certificate within the shortest possible time.

Art. 12 Commercial register

1 Art. 36 of the ordinance of 7 June 1937 on the commercial register[8] remains reserved as far as the archiving of documentation relating to qualified certificates issued to persons with specific attributes inscribed in the commercial register is concerned (art. 5, para. 2).

2 The entries in the commercial register alone are proof of the specific attributes of persons who are holders of qualified certificates.

Art. 13 Implementation

---

7 New content according to No. I of the ordinance of 6 June 2011, in force since 1 August 2011 (AS **2011** 3457).

8 [AS **53** 573, **1970** 733, **1971** 1844, **1982** 558, **1989** 2380, **1992** 1213, **1996** 2243 No. I 36, **1997** 2230, **2004** 433 annex No. 4 2669 4937 annex No. II 1, **2005** 4557, **2006** 4705 No. II 22 5787 annex 3 No. II 1. AS **2007** 5851 annex No. I]. See currently art. 8 para. 5, 9 para. 4 and 166 of the ordinance of 17 Oct. 2007 (SR **221.411).**

The office shall issue the necessary technical and administrative regulations. It shall take account of pertinent international law and may declare international technical standards applicable.

Art. 14 Abrogation of the law in force

The ordinance of 12 April 2000 concerning electronic certification services (ZertDV)[9] is abrogated.

Art. 15 Entry into force

The present ordinance enters into force on 1 January 2005.

[9] [AS **2000** 1257]