Decree on electronic certification services (OSCert)

784.103

of 12 April 2000

The Swiss Federal Council,

having regard to Arts. 28, 62 and 64 of the Law of 30 April 1997 on telecommunications (LTC)[1];

and having regard to Arts. 10, 14 and 15 of the Federal Law of 6 October 1995 on the technical barriers to trade (LTBT)[2],

orders as follows:

Chapter 1 General provisions

Art. 1 Object and aim

[1] This decree defines, in the form of an experimental regulation, the conditions under which certification service providers may be recognised on a voluntary basis and regulates their activities in the field of electronic certificates.

[2] Its aim is to promote the provision of secure electronic certification services to a wide public, to encourage the use and legal recognition of digital signatures and allow for international recognition of certification service providers and their services.

[3] The regulations under private law relating to the conclusion of contracts and the representation of legal persons remain unaffected.

Art. 2 Definitions

For the purposes of this decree:

a. *certification service provider* means a legal or natural person or federal, cantonal or municipal administrative entity which certifies information in an electronic environment and which issues electronic certificates for this purpose;

b. *electronic certificate* means a set of electronic data which link a public key and a legal or natural person or an administrative entity and which are authenticated by the digital signature of a certification service provider;

c. *private key* means a secret cryptographic key;

RO **2000** 1257
[1] RS **784.10**
[2] RS **946.51**

d. *public key* means a cryptographic key corresponding to a private key and made available to the public;

e. *cryptographic key* means a parameter used with a mathematical algorithm to convert, validate, authenticate, encrypt and decipher data;

f. *digital signature* means an electronic code attached to or logically associated with other electronic data and encrypted by means of a private key which, after being deciphered using the corresponding public key, permits verification that the data comes from the holder of the private key and that it has not been modified since being signed;

g. *recognition body* means an accredited certification body in accordance with the decree of 17 June 1996 on accreditation and designation[3] which assesses and recognises certification service providers.

Chapter 2 Recognition of certification service providers

Art. 3 Recognition

[1] Certification service providers who are in a position to issue and manage electronic certificates in accordance with the requirements of this decree may be recognised.

[2] The recognition bodies accredited for the sphere covered by this decree shall be competent to recognise certification service providers.

[3] If there is no recognition body, the Swiss Accreditation Service (SAS) of the Federal Office of Metrology shall recognise certification service providers.

Art. 4 Conditions for recognition

[1] In order to be recognised, certification service providers must fulfil the following conditions:

a. be listed in the commercial register or be part of an administrative unit of the Swiss Confederation, a canton or a municipality;

b. employ personnel who possess the necessary specialist knowledge, experience and qualifications;

c. use reliable computer systems and products;

d. possess sufficient financial resources and guarantees;

e. take out the necessary insurance to cover their liability and expenses arising from the measures laid down in Art. 15, paras. 2 and 3;

f. accept liability in their general terms and conditions of business, including towards third parties, for damages arising from an erroneous electronic

[3] RS **946.512**

certificate or from the infringement of obligations of disclosure, unless they can prove that no fault lies with them;

g. ensure that the applicable law is complied with, in particular this decree and its implementing provisions.

2 The conditions shall be laid down in more detail in the implementing provisions.

Art. 5 List of recognised certification service providers

1 The recognition bodies shall notify the SAS of the certification service providers that they recognise.

2 The SAS shall make the list of recognised certification service providers available to the public.

3 Each recognised certification service provider shall publish the list of all the other recognised certification service providers and their public keys. It shall authenticate the list with its digital signature. Further details of the type and scope of publication shall be laid down in the implementing provisions.

Chapter 3 Essential requirements

Section 1 Generation and use of cryptographic keys

Art. 6

The issues associated with the generation of cryptographic keys which may be the subject of electronic certificates in the sense of this decree and with the creation and verification of the digital signature shall be dealt with in the implementing provisions, the aim of which is to ensure a high degree of security in keeping with technological change.

Section 2 Electronic certificates

Art. 7

1 Any electronic certificate issued in accordance with this decree must contain at least the following information:

a. its serial number;

b. an indication that it has been issued in accordance with this decree;

c. an indication of any restrictions on its use;

d. the name of the holder of the certified public key and an indication as to whether this is a natural person, legal person, administrative entity or a pseudonym;

e. the certified public key;

f. its period of validity;

g. the name and digital signature of the issuing certification service provider.

2 The format of the certificates shall be laid down in the implementing provisions.

Section 3 Certification service providers

Art. 8 Issuing of electronic certificates

1 Recognised certification service providers must require persons requesting an electronic certificate to establish their identity and their authority by presenting in person the following documents:

a. an identity card or passport for natural persons;

b. a power of attorney and an identity card or a passport for persons acting for administrative entities;

c. an extract from the commercial register and an identity card or passport for persons authorised to act on behalf of legal persons.

2 Where a person or administrative entity identified in accordance with para. 1 less than ten years previously requests a new electronic certificate, recognised certification service providers may accept a request with the digital signature generated by the private key corresponding to the public key for which the certificate is to be renewed.

3 On request, the electronic certificate may bear a pseudonym in place of the name of the holder of the certified public key. The identity of the latter must be established in accordance with paras. 1 and 2.

Art. 9 Duty to disclose information

1 Recognised certification service providers must make their general contractual conditions and information about their certification policy available to the public.

2 They must advise their customers of the consequences of divulging or losing their private keys, at the latest when issuing the electronic certificates. They must advise customers of appropriate measures to take to keep their keys secret.

Art. 10 Keeping private keys

Recognised certification service providers may not keep copies of their customers' private keys.

Art. 11 Cancellation of electronic certificates

1 Recognised certification service providers shall cancel electronic certificates immediately when requested to do so by their holders.

2 They must ensure that the person requesting the cancellation is entitled to do so. This requirement is deemed to be satisfied where the request comes with the digital signature generated using the private key corresponding to the public key for which the certificate is to be cancelled.

3 Recognised certification service providers are required to cancel electronic certificates they have issued immediately if there is reason to believe that the latter were obtained fraudulently or that they no longer guarantee a link between a person or an administrative entity and a public key.

4 They can temporarily suspend electronic certificates for a maximum of three days. Once this period expires, they must finally cancel the certificates or re-establish their validity. In the first case, cancellation shall take effect from the moment the certificate is suspended; in the second case, suspension shall have no effect on the validity of the certificate.

5 Recognised certification service providers must advise holders of electronic certificates immediately of the cancellation or suspension of the latter.

Art. 12 Directory of electronic certificates and list of cancelled or suspended certificates

1 Recognised certification service providers shall keep a directory of the electronic certificates they issue in which their customers may have their electronic certificates registered.

2 They must keep an up-to-date list of all cancelled or suspended certificates even if they have not been registered in the directory. This list shall indicate only the serial number of the electronic certificate, the fact that it is cancelled or suspended and the date and time of cancellation or suspension. It shall be authenticated by the digital signature of the recognised certification service provider.

3 Recognised certification service providers must ensure that third parties have on-line access at all times to the directory of electronic certificates and to the list of cancelled or suspended certificates, free of charge apart from the use of public telecommunications services.

4 The details relating to the keeping of directories of electronic certificates and lists of cancelled or suspended certificates and access to the directories and lists shall be laid down in the implementing provisions.

Art. 13 Keeping electronic certificates

1 Recognised certification service providers must keep expired or cancelled electronic certificates and lists of cancelled certificates and allow them to be consulted for eleven years after the certificates have expired or been cancelled.

2 In the first six years, on-line consultation must be ensured at all times, free of charge apart from the use of public telecommunications services.

Art. 14 Journal of activities

[1] Recognised certification service providers shall keep a journal of their activities in connection with the issuing, cancellation and suspension of electronic certificates.

[2] They shall keep the journal entries and the relevant evidence for the same period as they are required to keep the last renewed certificate in accordance with Art. 8, para. 2.

Art. 15 Cessation of trading

[1] Recognised certification service providers shall notify the SAS that they are about to cease trading 30 days in advance. They shall notify the SAS immediately of any bankruptcy notice served on them.

[2] In the case of voluntary cessation of trading, recognised certification service providers must cancel the non-expired electronic certificates they have issued. The SAS shall charge another recognised certification service provider with keeping the list of cancelled certificates and with keeping expired or cancelled certificates, the journal of activities and the relevant evidence.

[3] If a recognised certification service provider goes bankrupt, the SAS shall charge another recognised certification service provider with cancelling the non-expired electronic certificates it has issued, keeping the list of cancelled certificates and keeping expired or cancelled certificates, the journal of activities and the relevant evidence.

Art. 16 Data protection

[1] Recognised certification service providers may collect and process personal data only in so far as necessary for the performance of their tasks.

[2] The data protection legislation shall apply.

Chapter 4 Supervision of recognised certification service providers

Art. 17

[1] Recognised certification service providers shall be supervised by the recognition bodies in accordance with the rules of the law of accreditation.

[2] If a recognition body withdraws recognition from a certification service provider, it shall notify the SAS of this immediately. Art. 15, para. 3 shall apply.

Chapter 5 Recognition of foreign certification service providers

Art. 18

The SAS shall make available to the public the list of foreign certification service providers which are recognised under the international agreements concluded by the Federal Council by virtue of Art. 14 LTBT.

Chapter 6 Attestation of the conformity of a digital signature with this decree

Art. 19

[1] On request and on payment of a fee, the SAS shall attest in writing that the digital signature in an electronic document was applied by means of the private key corresponding to a public key for which an electronic certificate has been issued by a recognised certification service provider and that the certificate was valid at a certain point in time.

[2] The Federal Department of Justice and Police shall determine the amount of the fee.

[3] Attestations in the sense of para. 1 may also be provided by other bodies provided they have the necessary qualifications.

Chapter 7 Final provisions

Art. 20 Implementation

The Federal Office for Communications shall issue the implementing provisions provided for in this decree, in collaboration with the Confederation's Information Technology Strategy Unit and the SAS. In doing so, it shall take account of international standards and provisions in this field.

Art. 21 Entry into force and period of effectiveness

[1] This decree shall come into force on 1st May 2000.

[2] It shall have effect until a relevant law comes into force, but not after 31 December 2009.