

# Ordonnance sur l'infrastructure à clé publique suisse (OICP)

du ...

Projet du 03.06.99

---

*Le Conseil fédéral suisse,*

vu les articles 28, 62 et 64 de la loi du 30 avril 1997<sup>1</sup> sur les télécommunications (LTC);  
vu les articles 10, 14 et 15 de la loi du 6 octobre 1995<sup>2</sup> sur les entraves techniques au commerce (LETC),

*arrête:*

## Section 1: Dispositions générales

### Art. 1 But et objet

<sup>1</sup> La présente ordonnance a pour but de garantir la fourniture de services de certification sûrs à un large public, de promouvoir l'utilisation et la reconnaissance juridique de la signature numérique en Suisse et d'assurer la reconnaissance internationale des fournisseurs de services de certification et de leurs prestations.

<sup>2</sup> Elle règle la reconnaissance, sur une base volontaire, des fournisseurs de services de certification de clés publiques.

### Art. 2 Définitions

Au sens de la présente ordonnance, on entend par:

- a. *signature numérique*: donnée sous forme électronique jointe ou liée logiquement à d'autres données électroniques, qui est chiffrée à l'aide d'une clé privée et qu'un tiers peut vérifier en la déchiffrant à l'aide de la clé publique correspondante afin de s'assurer que les données émanent bien de la personne qui est censée détenir la clé privée et qu'elles n'ont pas été modifiées depuis l'instant où elles ont été signées;
- b. *certificat électronique*: données électroniques attestant le lien entre une clé publique et une personne déterminée par apposition de la signature numérique de l'entité qui les émet;
- c. *fournisseur de services de certification*: personne physique ou morale qui certifie des informations dans un environnement électronique et qui émet à cette fin des certificats électroniques.

## Section 2: Reconnaissance des fournisseurs de services de certification

### Art. 3 Reconnaissance

<sup>1</sup> Les organismes de certification accrédités dans le domaine couvert par la présente ordonnance et au sens de l'ordonnance du 17 juin 1996 sur l'accréditation et la

<sup>1</sup> RS 784.10

<sup>2</sup> RS 946.51

désignation<sup>3</sup> sont compétents pour reconnaître les fournisseurs de services de certification.

<sup>2</sup> Pour être reconnus, les fournisseurs de services de certification doivent remplir les exigences essentielles fixées par la présente ordonnance.

<sup>3</sup> S'il n'existe aucun organisme de certification accrédité, le Service d'accréditation suisse (SAS) reconnaît les fournisseurs de services de certification. Il évalue la conformité aux exigences essentielles en désignant des experts.

#### **Art. 4** Enregistrement

<sup>1</sup> L'Office fédéral de la communication (OFCOM) enregistre les fournisseurs de services de certification reconnus.

<sup>2</sup> Les organismes de certification accrédités annoncent à l'OFCOM les fournisseurs de services de certification qu'ils reconnaissent.

<sup>3</sup> L'OFCOM tient à la disposition du public la liste des fournisseurs de services de certification reconnus.

### **Section 3: Exigences essentielles pour la reconnaissance des fournisseurs de services de certification**

#### **Art. 5** En général

Les fournisseurs de services de certification doivent:

- a. employer du personnel possédant les connaissances, l'expérience et les qualifications nécessaires;
- b. utiliser des systèmes et des produits informatiques fiables;
- c. posséder des ressources et des garanties financières suffisantes, notamment en contractant une assurance appropriée couvrant leur responsabilité;
- d. respecter le droit applicable en la matière, notamment la présente ordonnance et ses dispositions d'exécution.

#### **Art. 6** Emission des certificats électroniques

<sup>1</sup> Les fournisseurs de services de certification délivrent des certificats électroniques à des personnes physiques ou morales.

<sup>2</sup> Ils doivent s'assurer de l'identité et des pouvoirs des requérants en exigeant qu'ils se présentent personnellement, munis des documents officiels suivants :

- a. carte d'identité ou passeport pour les personnes physiques;
- b. extrait du registre du commerce et carte d'identité ou passeport des représentants pour les personnes morales.

<sup>3</sup> Lorsqu'une personne demande un certificat électronique pour en représenter une autre, cette dernière doit également justifier de son identité en se présentant personnellement ou en faisant parvenir au fournisseur de services de certification un message

<sup>3</sup> RS 946.512

électronique muni d'une signature numérique répondant aux exigences de la présente ordonnance et attestant des pouvoirs de représentation du requérant.

4 Les fournisseurs de services de certification enregistrent et conservent les informations recueillies lors de l'identification des personnes.

5 Ils peuvent faire figurer dans le certificat électronique un pseudonyme en lieu et place du nom de la personne.

#### **Art. 7** Devoir d'information

1 Les fournisseurs de services de certification doivent publier leurs conditions générales.

2 Au plus tard lors de l'émission des certificats électroniques, ils doivent rendre leurs clients attentifs aux conséquences que peut avoir la divulgation ou la perte de leur clé privée. Ils doivent leur indiquer les mesures appropriées pour maintenir secrète leur clé privée.

#### **Art. 8** Génération et sauvegarde des clés privées

Les fournisseurs de services de certification ne peuvent en aucun cas générer ni sauvegarder eux-mêmes les clés privées de leurs clients qui servent à la signature numérique.

#### **Art. 9** Révocation des certificats électroniques

1 Les fournisseurs de services de certification révoquent immédiatement les certificats électroniques à la demande des personnes en faveur desquelles ils ont été émis.

2 Ils doivent s'assurer de la légitimité de la demande de révocation.

3 Ils sont tenus de révoquer sans tarder les certificats électroniques qu'ils ont émis s'il s'avère que ceux-ci ont été obtenus de manière frauduleuse, qu'ils comportent des indications fausses ou que, de toute autre manière, ils ne sont plus aptes à garantir le lien entre une personne déterminée et sa clé publique.

#### **Art. 10** Annuaire des certificats électroniques et liste des certificats révoqués

1 Les fournisseurs de services de certification doivent, à la demande de leurs clients, faire figurer dans un annuaire les certificats électroniques qu'ils émettent.

2 Ils doivent faire figurer dans une liste tous les certificats révoqués, même ceux qui n'ont pas été publiés, dès le moment de leur révocation.

3 Ils doivent en tout temps garantir l'accès à l'annuaire des certificats électroniques et à la liste des certificats révoqués, par des moyens de télécommunication publics et sans autres frais supplémentaires.

#### **Art. 11** Conservation des certificats électroniques

1 Les fournisseurs de services de certification offrant des services liés à la signature numérique doivent conserver les certificats électroniques échus ou révoqués et permettre leur consultation pendant onze ans au moins à compter de la date d'échéance ou de révocation.

<sup>2</sup> Durant les six premières années, la consultation doit être garantie aux mêmes conditions que celles découlant de l'article 10, alinéa 3.

**Art. 12** Journal des activités

Les fournisseurs de services de certification consignent dans un journal leurs activités relatives à l'émission et à la révocation des certificats électroniques.

**Art. 13** Cessation d'activité

<sup>1</sup> En cas de cessation d'activité volontaire, les fournisseurs de services de certification offrant des services liés à la signature numérique doivent transférer les certificats électroniques qu'ils ont émis et dont la période de validité ou de conservation n'est pas échue à un ou plusieurs autres fournisseurs de services de certification reconnus offrant des services liés à la signature numérique.

<sup>2</sup> En cas de faillite ou de révocation de la reconnaissance d'un fournisseur de services de certification offrant des services liés à la signature numérique, l'OFCOM charge un autre fournisseur de services de certification reconnu offrant des services liés à la signature numérique de révoquer les certificats électroniques non échus qu'il a émis, de tenir la liste des certificats révoqués et de conserver les certificats échus ou révoqués.

<sup>3</sup> L'OFCOM fixe de cas en cas le montant du dédommagement auquel a droit le fournisseur désigné. Ce montant est supporté par les fournisseurs de services de certification reconnus offrant des services liés à la signature numérique au pro rata du nombre de certificats électroniques qu'ils ont émis et qui sont valables le jour où la faillite est prononcée ou la reconnaissance révoquée.

<sup>4</sup> Les fournisseurs de services de certification offrant des services liés à la signature numérique annoncent sans tarder à l'OFCOM qu'ils cessent leurs activités ou qu'ils font l'objet d'une procédure de poursuite par voie de faillite.

**Art. 14** Protection des données

Les fournisseurs de services de certification doivent assurer la protection des données personnelles de leurs clients conformément à la loi fédérale du 19 juin 1992<sup>4</sup> sur la protection des données.

**Art. 15** Prescriptions de l'OFCOM

L'OFCOM édicte les prescriptions de détail relatives aux exigences essentielles, d'entente avec l'Office fédéral de l'informatique et le SAS.

<sup>4</sup> RS 235.1

## **Section 4:** **Certification électronique primaire des fournisseurs de services de certification reconnus**

### **Art. 16** *Tâches de l'OFCOM*

*1 Lors de l'enregistrement des fournisseurs de services de certification reconnus offrant des services liés à la signature numérique, l'OFCOM certifie leur clé publique au moyen de sa propre signature numérique. Il publie sa clé publique dans la Feuille fédérale.*

*2 Il révoque la certification électronique du fournisseur de services de certification dont la reconnaissance a été retirée par un organisme de certification accrédité.*

*3 Il peut certifier, sur une base réciproque et dans le cadre d'un accord international conclu par le Conseil fédéral, la clé publique d'organes étrangers ayant des compétences semblables ou, en l'absence de tels organes, la clé publique de fournisseurs de services de certification étrangers officiellement reconnus offrant des services liés à la signature numérique.*

*4 Pour le reste, il est soumis aux dispositions des sections 2 et 3 et de l'article 19, alinéa 1.*

### **Art. 17** *Obligations des fournisseurs de services de certification*

*Les fournisseurs de services de certification reconnus dont la clé publique est soumise à la certification électronique de l'OFCOM ne peuvent pas reconnaître d'autres fournisseurs de services de certification.*

### **Art. 18** *Emoluments*

*1 L'OFCOM perçoit des émoluments pour la certification électronique des fournisseurs de services de certification reconnus offrant des services liés à la signature numérique ainsi que pour la révocation de la certification électronique.*

*2 Le Département fédéral de l'environnement, des transports, de l'énergie et de la communication fixe le montant des émoluments.*

## **Section 5:** **Surveillance et responsabilité des fournisseurs de services de certification reconnus**

### **Art. 19** *Surveillance*

*1 La surveillance des fournisseurs de services de certification reconnus est assurée par les organismes de certification accrédités.*

*2 Lorsqu'un organisme de certification accrédité retire la reconnaissance d'un fournisseur de services de certification, il l'annonce immédiatement à l'OFCOM.*

#### **Art. 20** Responsabilité

<sup>1</sup> La responsabilité des fournisseurs de services de certification reconnus est régie par les dispositions du Code des obligations<sup>5</sup>. Ceux-ci répondent en particulier de l'exactitude du lien entre une personne déterminée et sa clé publique au moment de l'émission du certificat au sens de l'article 6, alinéa 2.

<sup>2</sup> Lorsqu'ils limitent leur responsabilité à un montant déterminé ou à certaines utilisations du certificat électronique, les fournisseurs de services de certification reconnus doivent l'indiquer dans le certificat électronique.

<sup>3</sup> Aucune limitation de responsabilité ne peut être stipulée quant aux obligations découlant de la présente ordonnance.

### **Section 6: Fournisseurs de services de certification étrangers**

#### **Art. 21**

L'OFCOM tient à la disposition du public la liste des fournisseurs de services de certification étrangers reconnus par le Conseil fédéral dans le cadre d'accords internationaux.

### **Section 7: Attestation de la conformité d'une signature numérique avec la présente ordonnance**

#### **Art. 22**

<sup>1</sup> Sur demande et contre paiement d'un émolument, l'OFCOM atteste que la signature numérique figurant sur un document électronique a bien été apposée au moyen de la clé privée correspondant à la clé publique faisant l'objet d'un certificat électronique émis par un fournisseur de services de certification reconnu et que ce certificat était valable à un moment donné.

<sup>2</sup> Le Département fédéral de l'environnement, des transports, de l'énergie et de la communication fixe le montant de l'émolument.

### **Section 8: Dispositions finales**

#### **Art. 23** Exécution

L'OFCOM est chargé de l'exécution de la présente ordonnance et édicte les prescriptions techniques et administratives nécessaires.

#### **Art. 24** Entrée en vigueur

La présente ordonnance entre en vigueur le 1<sup>er</sup> janvier 2000.

<sup>5</sup> RS 220

...

Au nom du Conseil fédéral suisse:  
La Présidente de la Confédération,  
Le Chancelier de la Confédération,