

eCH-0048 Classes de certificats PKI

Titre	Classes de certificats PKI
Code	eCH-0048
Type	Norme de procédure
Stade	définie
Version	V1-0
Statut	approuvée
Validation	2006-12-15
Date de publication	2006-11-17
Remplace	
Langues	Allemand, français
Auteurs	Groupe spécialisé Sécurité Gerold H. Werner, max. consult SA (directeur), max.consult-ag@bluewin.ch Adrian Müller, Dr. Otto Müller Consulting adrian@mueller-consulting.biz Roland Wichtermann, DDPS roland.wichtermann@gst.admin.ch Daniel Messerli, Ergonomics dmesserli@ergonomics.ch
Editeur / Distributeur	Association eCH, Amthausgasse 18, 3011 Berne T 031 560 00 20, F 031 560 00 25 www.ech.ch/ info@ech.ch

Sommaire

1	Statut du document	3
2	Introduction	3
2.1	But de la norme	3
2.2	Objectifs visés par la norme	8
2.3	Cadre réglementaire et délimitation	8
2.4	Avantages	9
3	Vue d'ensemble des classes de certificats	10
4	Profils d'exigences	12
4.1	Classe 1	12
4.2	Classe 2	13
4.3	Classe 3	16
4.4	Certificats d'essai.....	19
5	Remarque finale	20
6	Exclusion de responsabilité – Droits de tiers	21
7	Droits d'auteur	21
	Annexe A – Références & Bibliographie	22
	CH Bases légales Vue d'ensemble http://www.bakom.ch/themen/internet/00467/index.html?lang=fr	22
	Directive UE	22
	Publications ETSI	22
	CEN Workshop Agreements	22
	Norme ISO	23
	ITSEC	23
	Recommandation UIT-T	23
	Normes NIST	23
	pkix RFCs.....	23
	Annexe B – Collaboration & Supervision	23
	Annexe C – Abréviations	24

1 Statut du document

Le présent document a été **approuvé** le 15 décembre 2006 par le Comité d'experts. Il a force normative pour le domaine d'application défini dans les limites de validité fixées.

2 Introduction

Le groupe spécialisé eCH Sécurité est convaincu, tout comme les représentants de l'administration publique et de l'économie participant, que la norme présentée ici est une base utile pour l'implémentation efficace de certificats et de signatures numériques de niveau avancé dans un contexte interopérational de processus électroniques.

Le développement technique et organisationnel des processus électroniques exigera un suivi continu et une adaptation régulière de la norme au cours des prochaines années.

2.1 But de la norme

L'implémentation de processus opérationnels¹ fiables en cyberadministration exige l'identification sûre des partenaires. Les signatures électroniques authentifiées par des certificats de type X.509 se sont imposés sur le plan international. Cette norme technique doit s'accompagner d'un ensemble cohérent de règles organisationnelles et juridiques afin d'assurer une correspondance univoque entre les effets juridiques des documents et la volonté de leurs auteurs au moyen de signatures électroniques, et garantir ainsi les effets juridiques voulus par les partenaires.

Dans l'espace communautaire européen, la directive 1999/93/CE² peut être considérée comme référence transposée en droit national dans la plupart des États membres de l'Union européenne. Cette directive précise (à différents degrés d'explicitation) le cadre réglementaire relatif à trois niveaux de qualité des signatures et certificats numériques :

- Signature électronique
"signature électronique", une donnée sous forme électronique qui est jointe ou liée logiquement à d'autres données électroniques et qui sert de méthode d'authentification ; (Directive, art. 2, 1)
- Signature électronique avancée
"signature électronique avancée", une signature électronique qui satisfait aux exigences suivantes :
 - a) être liée uniquement au signataire ;
 - b) permettre d'identifier le signataire ;
 - c) être créée par des moyens que le signataire puisse garder sous son contrôle exclusif et
 - d) être liée aux données auxquelles elle se rapporte de telle sorte que toute modification ultérieure des données soit détectable ; (Directive, art. 2, 2)

¹ Le terme "processus opérationnels" utilisé dans le présent document désigne aussi bien les activités opérationnelles de l'économie privée que des administrations publiques ainsi que les interfaces des administrations avec l'économie.

² Directive 1999/93/CE du Parlement européen et du Conseil du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques http://europa.eu.int/eur-lex/pri/fr/oj/dat/2000/l_013/l_01320000119fr00120020.pdf

- Signature électronique qualifiée
(signature électronique avancée reposant sur un certificat qualifié)
"certificat qualifié", un certificat qui satisfait aux exigences visées à l'annexe I et qui est fourni par un prestataire de service de certification satisfaisant aux exigences visées à l'annexe II (Directive, art. 2, 10)

Dans les considérants³ et dans les articles déclaratoires⁴ de la directive, il est fait expressément mention de la volonté de faciliter la communication électronique transfrontalière dans l'espace économique communautaire.

Il est précisé qu'un des buts visés est le développement des transactions électroniques de l'administration publique entre les institutions étatiques, les citoyens et l'économie.⁵

Les dispositions législatives et réglementaires en Suisse (SCSE, OSCSE, PTA et autres documents référencés) concernant l'utilisation de signatures électroniques et l'émission de certificats numériques sont axées sur la remise de certificats qualifiés exclusivement à des **personnes physiques** par des prestataires agréés. Le but visé est un équivalent électronique de la signature manuscrite servant à authentifier la volonté du signataire.

Les acteurs intervenant dans les processus d'affaires et de cyberadministration, considérés dans leur ensemble, ne sont toutefois pas seulement des personnes physiques mais aussi des personnes morales, des organisations, des unités organisationnelles, des fonctions, et des éléments d'infrastructure (serveurs, routeurs, ... machines et processus en général).

De ce fait, la signature authentique de personnes physiques ne couvre qu'une partie de la chaîne complexe des processus de l'économie et de la cyberadministration.

Par ailleurs, la grande majorité des processus opérationnels ne sont pas soumis à des règles juridiques exigeant une signature manuscrite, ou son équivalent électronique, la signature électronique qualifiée. Dès lors que la signature électronique est utilisée, il en découle des exigences légales quant à la garantie et à la responsabilité qui ne sont pas toujours appropriées ni souhaitables.

- L'implémentation sûre de chaînes de processus en cyberadministration exige entre autres l'authentification d'identités numériques au moyen de certificats électroniques, tel que le certificat qualifié de signature selon la SCSE.
- Outre la "signature qualifiée", la SCSE vise également la "signature électronique simple" (SCSE art. 2a) et la "signature électronique avancée" (SCSE art.2b), sans préciser suffisamment le cadre réglementaire et les effets juridiques.

³ Considérants 5, 7, 8, 10, 19 et 23

⁴ Directive, art 3 "Accès au marché" et art. 4 "Principes du marché intérieur"

⁵ Considérant 5

- Pour la signature qualifiée, il y a renversement du fardeau de la preuve (CO art. 59a). Dès lors, contrairement aux règles en vigueur dans les transactions sur papier, le signataire (préssumé) doit prouver qu'il n'a pas signé un document. S'agissant des signatures qui ne reposent pas sur un certificat qualifié, il n'existe pas actuellement de dispositions légales.

Le champ d'application des certificats X.509 ne se limite pas à la signature de documents électroniques. Il englobe l'authentification, les signatures en code, le cryptage et d'autres fonctions. La présente norme eCH vise tous les domaines d'utilisation.

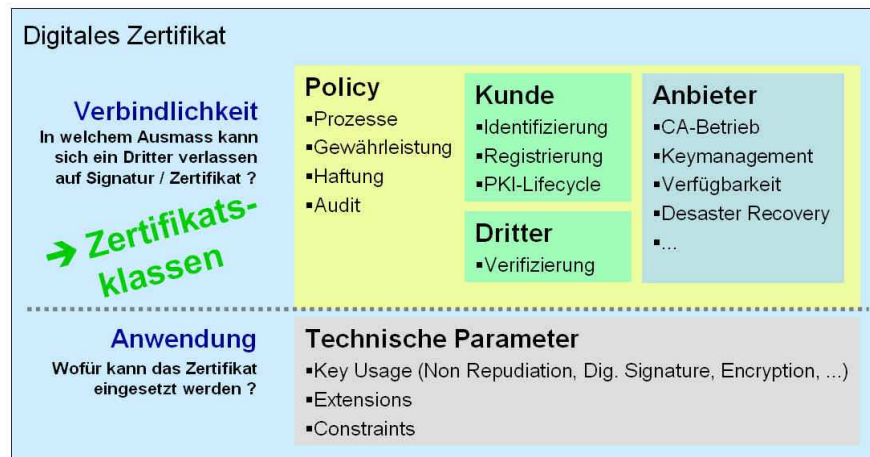
La présente norme eCH distingue deux aspects de base des certificats numériques :

- **Niveau de fiabilité⁶**
des données du certificat relatives au sujet certifié (personne physique ou morale, organisation, machine, processus, fonction). Cet aspect détermine la mesure dans laquelle un partenaire d'affaires peut se fier au contenu du certificat. C'est de lui ainsi que de la réglementation de la responsabilité du prestataire du service de certification et le cas échéant de règles contractuelles complémentaires applicables aux partenaires d'affaires que découle le caractère authentique des processus électroniques auxquels s'applique la signature électronique.
- **Fonction**
du certificat, modulée par la fixation des paramètres techniques (selon X.509). Cet aspect détermine les buts auxquels le certificat peut techniquement servir (signature électronique, irrévocabilité, authentification, cryptage de courrier électronique, authentification de serveurs, signature en code, etc.).

La présente norme part du principe que la fiabilité et la fonction d'un certificat sont deux dimensions indépendantes. La fonction étant déterminée par des paramètres purement techniques du certificat, la présente norme est axée sur les critères techniques et organisationnels dont dépend la fiabilité des données contenues dans le certificat.

⁶ Le niveau de fiabilité est une estimation du degré de confiance qui peut être accordé aux données contenues dans le certificat. Cette fiabilité se base en partie sur des normes techniques reconnues internationalement mais surtout sur la qualité des processus organisationnels assurant l'authenticité et la vérification des données identitaires du certificat.

Dimensionen des X.509 Zertifikates



Un certificat est émis par un prestataire de service de certification (CSP)⁷. Il doit répondre aux critères suivants :

- Garantie des caractéristiques d'une classe de certificats pour les certificats émis
- Implémentation des paramètres techniques pour le domaine d'utilisation déterminé et pour les services de répertoire nécessaires

La combinaison des profils d'exigences découlant de ces critères donne 3 "classes de certificats". Les certificats la classe la plus élevée (Classe 3) sont établis et remis conformément à la SCSE. Ils sont de plus soumis à des règles contractuelles et ne concernent pas exclusivement des personnes physiques. Sur l'ensemble de la chaîne des processus, les certificats peuvent concerner également des personnes morales, des machines ou des processus automatisés et leur conférer ainsi un niveau de fiabilité bien défini.

Selon le degré de protection nécessaire des processus opérationnels il est convenu de définir des niveaux d'exigences afin d'assurer un rapport optimal entre le besoin de protection et les coûts dans les échanges entre la cyberadministration et l'économie.

⁷ CSP, Certification Service Provider : prestataire de service de certification.

eCH-0048: Zertifikatsklassen

Definiert Anforderungen zu:	Class-1 gering	Class-2 hoch	Class-3 sehr hoch	Qualif. sehr hoch
1. Registrierung				
a) Identifizierung	Welche Dokumente beweisen die Identität			
b) Prozess	Wie läuft der Registrierungsprozess ab			
c) Nachvollziehbarkeit	Was wird wie über welchen Zeitraum archiviert			
2. Client PKI-Token				
a) Anforderungen	Software-/Hardwaretoken, Key-Store, Evaluation			
b) Keymanagement	Key-Generierung und -Backup für Client-Token			
3. CA-Betrieb				
a) CA Betrieb	Betriebsumgebung, Prozesse, Personal, Regularien			
b) Policy	Liefer- und Serviceumfang			
c) Revision	Kontrollmechanismen für Betrieb der CA			

Il en résulte une matrice où

- Le propriétaire d'un processus opérationnel détermine, en fonction du besoin de protection des données et des applications, la classe de certificat nécessaire pour permettre l'interaction en ligne avec des tiers
- Le prestataire de service de certification (CSP) peut positionner sa prestation indépendamment de la désignation propre des classes de certificats qu'il propose.

Cette matrice permet de différencier les services offerts selon les conditions du marché et conformément aux variantes autorisées.

La présentation uniforme des offres de certificats sur le marché en fonction des critères de classification facilite la comparaison des offres et permet aux décideurs de s'informer et de choisir en connaissance de cause les produits assurant un déroulement sûr et économique des processus opérationnels.

Vergleichbarkeit Marktangebot

	Class-1 gering	Class-2 hoch	Class-3 sehr hoch	Zert ES
Anbieter A	D	C	B	A
Anbieter B	Grün	Blau		
Anbieter C	1	2	3	
Anbieter D	Silber	Gold	Platin	
etc.	X	Y	Z	CH1

2.2 Objectifs visés par la norme

La norme eCH relative aux certificats numériques vise le management des identités dans les processus opérationnels de la cyberadministration pour différents domaines d'utilisation avec le niveau de sécurité correspondants.

Prémises de la norme eCH pour les classes de certificats :

- Règles complémentaires pour les "signatures électroniques" et les "signatures électroniques avancées" au sens de la SCSE
- Définition de 3 classes de certificats avec niveaux de fiabilité correspondants
- Détermination des exigences relatives à l'émission de certificats
- Non-spécification des paramètres techniques et référencement exclusif des normes pertinentes pour les niveaux de fiabilité
- Conformité à
 - la législation suisse
 - la réglementation des partenaires internationaux (EU en particulier)

2.3 Cadre réglementaire et délimitation

L'accent est mis sur la spécification des exigences permettant de réaliser les différents niveaux de fiabilité (garantie contraignante des données contenues dans le certificat). Les scénarios et les fonctions techniques des certificats lors de leur utilisation sont déterminés par le propriétaire des processus opérationnels et, pour autant que le niveau de fiabilité ne soit pas affecté, ne font pas l'objet de la présente norme eCH.

2.3.1 Authentification, autorisation

La présente norme eCH concerne expressément et exclusivement l'identité ou la représentation de l'identité du détenteur de la clé de signature privée attribuée authentifiée par le certificat.

Même s'il est généralement possible de fixer dans les certificats des attributs autorisant leur détenteur à utiliser des applications ou des services déterminés, la présente norme s'abstient délibérément de le faire pour les motifs suivants :

- Les données d'autorisation ne sont pas propres au détenteur du certificat mais lui sont attribuées par un tiers (propriétaire des processus opérationnels)
- La forme, les effets et le contrôle des données d'autorisation par les applications correspondantes ne sont pas soumis à des normes uniformes et sortent donc du cadre de la définition d'une politique de certification (Certification Policy) et des possibilités de contrôle d'un prestataire de service de certification (Certification Service Provider, CSP).
Il n'est donc pas possible d'assumer la responsabilité de l'utilisation et des informations qui en sont tirées.
- Les données d'autorisation se modifient en règle générale plus souvent que les données d'authentification. Une séparation stricte est appliquée en pratique afin d'éviter la nécessité de délivrer de nouveaux certificats de manière répétée.

Les propriétaires des processus opérationnels (tels que les unités d'organisation, OU) peuvent utiliser librement des données de certificats, par exemple pour gérer des droits d'accès à des applications. Cette utilisation se déroule toutefois en dehors de la politique de certification et peut être soumise à des dispositions contractuelles séparées.

2.3.2 SCSE

La classe des *certificats qualifiés* est expressément exclue de la norme car elle est soumise aux normes légales de la SCSE et de l'OSCSE, pour lesquelles une norme eCH est superflue. Les *certificats qualifiés* ne sont mentionnés dans le présent document qu'à des fins d'information et de délimitation par rapport aux classes de certificats définies ici.

La SCSE – en accord avec la directive européenne – vise les "signatures électroniques" et les "signatures électroniques avancées" pour lesquelles la loi ne spécifie pas les certificats correspondants. La présente norme eCH vise à combler cette lacune par des règles complémentaires et à permettre ainsi l'utilisation de ces signatures sous forme de complément bien défini aux certificats qualifiés dans les processus de la cyberadministration.

2.4 Avantages

Les classes de certificat 1, 2 et 3 offrent une grille de profils d'exigences élémentaires applicables aux certificats numériques qui complète les certificats qualifiés visés par la SCSE de manière à permettre l'identification univoque des acteurs dans toute la chaîne des processus de la cyberadministration.

En outre, la présentation uniforme des profils permet la comparaison des offres des prestataires de service de certification (Certification Service Provider, CSP) quant à leur fonctionnalité, leur qualité et leur fiabilité, assurant ainsi la transparence du marché et favorisant la concurrence.

3 Vue d'ensemble des classes de certificats

	Classe 1	Classe 2	Classe 3	Certificat qualifié
Niveau de fiabilité	Bas	Haut	Très haut	Très haut
Base légale	"signature électronique" SCSE 943.03, art. 2, al. a.	"signature électronique avancée" SCSE 943.03, art. 2, al. b.	"signature électronique avancée" SCSE 943.03, art. 2, al. b.	"signature électronique qualifiée" SCSE 943.03, art. 2, al. c.
Identification	Compte e-mail / compte de domaine / compte technique	---PERSONNE--- Documents personnalisés ---FONCTION, GROUPE, MACHINE--- Mandat du responsable avec preuve d'autorisation	---PERSONNE--- Documents authentifiés (passeport, ID) ---FONCTION, GROUPE, MACHINE--- Mandat du responsable avec preuve d'autorisation étendue	---PERSONNE--- Documents authentifiés (passeport, ID) ---FONCTION, GROUPE, MACHINE--- Non applicable
Nom	Nom librement attribuable (CN) Le nom du compte e-mail ou du compte technique est enregistré dans le certificat	Personne physique désignée par la preuve d'identité. Le certificat peut être établi sous un pseudonyme. Les attributs particuliers (désignation de profession protégée, titre académique ou statutaire, ...) exigent des preuves séparées.		
Enregistrement	Procédure librement définie avec vérification des données de compte	Procédure sécurisée basée sur les preuves d'identité fournies	Procédure sécurisée basée sur une demande personnelle, le cas échéant aussi auprès de tiers	Demande personnelle auprès d'une autorité d'enregistrement agréée.
Archivage des données	Durée : plus de 2 ans	Durée : plus de 5 ans (délai de prescription selon CO)	Durée : plus de 11 ans	
Durée de validité de l'enregistrement	Identique à la durée du certificat	Maximum 6 ans.		

	Classe 1	Classe 2	Classe 3	Certificat qualifié
Durée du certificat	Selon politique de certification			Aucune indication
Clé de client ⁸ (Client Token)	Soft- / Hardware	Soft- / Hardware	Hardware évalué selon - FIPS 140-1/140-2 Level 2 ou - OFCOM PTA	Clé de client selon OFCOM PTA RS 943.032.1 / Annexe
Gestion de clés de client	Key Backup / Recovery par le prestataire CSP pour : - clé de signature : NON - clé de chiffrement seulement dans les infrastructures et les processus sûrs et documentés			Clé de client selon OFCOM PTA RS 943.032.1 / Annexe
Exigences CA (gestion, personnel, processus)	Plan d'exploitation et de sécurité documenté	Plan d'exploitation et de sécurité documenté; contrôle des accès aux systèmes et backups de CA etc.; contrôle annuel par un responsable interne	Plan d'exploitation et de sécurité documenté; contrôle des accès aux systèmes et backups de CA etc.; contrôle annuel par un expert qualifié (interne / externe).	Contrôle annuel selon: ETSI TS 101 456, ch. 6.1, 7.1, 7.4, 7.5, 8.1; Cf. OFCOM PTA RS 943.032.1, CH. 3.2 Organisation et principes opérationnels
Police de certification (CP, CPS)	Déclarations selon RFC-3647 concernant notamment les données certifiées et l'étendue des prestations			Responsabilité: 2 millions CHF par cas
Détenteurs autorisés (sujets)	Aucune indication	<ul style="list-style-type: none"> - personnes physiques - personnes morales, sociétés simples, organisations - groupes, fonctions - machines (SSL, IPsec, etc.) 		- personnes physiques (clients)
Domaine d'application	Toutes les applications sont autorisées			- signature de documents électroniques (manifestation de la volonté de l'auteur)

⁸ Software- oder Hardwaremedium zur Speicherung des/der privaten Schlüssel eines Zertifikates (Bsp. f. Software: Microsoft Certificate Manager im Windows OS; Bsp. f. Hardware: SmartCard, USB-Token, Hardware Security Module)

4 Profils d'exigences

L'attribution d'une "classe de certificat" définit le degré de fiabilité des données contenues dans un certificat et donc le degré auquel un tiers peut se fier à ces données et, en cas de dommage, imputer la responsabilité de l'émetteur du certificat.

La classification en trois classes correspond d'une part à des exigences de sécurité différenciées des processus opérationnels et d'autre part aux schémas usuels du marché.

Bases techniques : X.509v3, PKIX.

4.1 Classe 1

Les certificats de cette classe servent en règle générale aux processus opérationnels pour lesquels l'authenticité des participants est en principe non pertinente ou est assurée par d'autres moyens.

L'intégration de cette classe à bas niveau de fiabilité à la norme eCH se justifie du fait que lorsqu'un prestataire CSP veut émettre de tels certificats il doit le faire selon des règles bien définies.

4.1.1 Enregistrement

4.1.1.1 Identification

Un compte technique suffit comme preuve d'identité, par exemple un compte courriel (e-mail) ou un domaine enregistré. Le nom du compte doit figurer dans le certificat

Les certificats de Classe 1 attestent l'existence d'un tel compte au moment de leur émission. L'attribution du certificat à une personne physique ne peut en être déduite.

4.1.1.2 Noms

Les noms (CN, SAN) peuvent être choisis librement pour autant qu'ils ne soient pas contraires aux bonnes mœurs ou aux droits de tiers. L'usage de titres statutaires ou professionnels protégés n'est pas admissible en raison du manque de preuve

Les noms d'organisations (O:) ou d'unités organisationnelles (OU:) sont fixés par l'autorité de certification CA.

4.1.1.3 Procédure d'enregistrement

Procédure librement définie avec vérification des données de compte (confirmation d'adresse e-mail, code d'accès ou émission liée à un domaine ou à une entrée de répertoire).

Exemples

a) envoi par e-mail du certificat émis ; b) envoi par e-mail d'un code d'accès ; c) attribution d'un certificat à un nom de domaine ou une entrée de répertoire.

4.1.2 Validité de l'enregistrement

Les données d'enregistrement ne sont pas conservées pour le renouvellement du certificat et ne sont valables que pour la seule émission du certificat demandé.

4.1.3 Clé de client de certificat (Client Certificate Token)

Il peut s'agir d'une clé numérique ou d'une clé technique (par exemple USB). Si la clé émise par le prestataire CSP inclut le code personnel d'utilisation du certificat, elle doit être protégée de manière adéquate (mot de passe, code NIP) empêchant l'usage non autorisé.

4.1.4 Emission et remise de certificats

Le prestataire de service de certification doit assurer par des mesures techniques et organisationnelles que la clé secrète d'un certificat ne puisse être vue ou utilisée par des tiers au cours du processus de protection et de livraison. Après la remise de la clé de certificat la responsabilité de la protection de la clé et du code NIP incombe au détenteur du certificat.

4.1.5 Révocation de certificats

Les données relatives aux certificats révoqués doivent être actualisées et publiées par le prestataire CSP.

4.1.6 Gestion de l'autorité de certification CA

Les aspects techniques et procéduraux de la gestion de l'autorité de certification CA doivent être documentés. L'archivage des fichiers de journalisation (log files) pendant deux ans après l'émission du certificat est nécessaire pour satisfaire aux exigences de la traçabilité.

4.1.7 Politique de certification (CP) et déclaration des pratiques (CPS)

Une politique de certification (Certification Policy, CP) sert de contrat cadre entre le prestataire CSP, le détenteur du certificat et les tiers faisant confiance au certificat. Elle précise l'ampleur des prestations et les caractéristiques garanties des produits et services. Elle doit se conformer à RFC-3647 pour assurer la comparabilité et la transparence des offres.

4.2 Classe 2

Dans l'économie et les administrations, certaines procédures se sont imposées au fil des années, bien qu'elles n'offrent pas de sécurité totale quant à l'identité et à la légitimité des participants ou à l'intégrité des données. Exemples : commandes de marchandises par téléphone ou par fax, commandes écrites ou conventions munies de signatures qui ne peuvent pas être authentifiées de manière univoque par le destinataire.

Dans le domaine de la cyberadministration, il arrive aussi souvent que l'on traite des demandes de renseignements, des accords ou des requêtes par téléphone, par la poste, par fax ou par courriel (e-mail) sans que leur authenticité ou leur légitimité soit vérifiée de façon sûre. L'équivalent numérique de cette pratique usuelle correspond aux certificats de la Classe 2.

4.2.1 Enregistrement

4.2.1.1 Identification

a) Personnes physiques

Présentation de documents personnels de tiers avec photo et données officielles :

- permis de conduire
- carte de santé
- carte de légitimation d'entreprise ou de service
- abonnement demi-tarif ou abonnement général

b) Personnes morales, organisations, fonctions, groupes, processus

Mandat du responsable administratif ou hiérarchique avec preuve d'identité et de fonction

Exemple

Commande de certificat signée par un chef de service sur papier à en-tête de l'organisation avec apposition d'une deuxième signature ; l'identification du mandant se fait au moyen d'un document mentionné plus haut sous a).

c) Machines, serveurs, adresses IP publiques

Les certificats de serveurs, routeurs ou autres font l'objet d'une demande par un responsable avec preuve de son identité et de sa légitimité. La légitimité de la demande de certificat pour certains domaines ou pour les adresses IP publiques est en général documentée au moyen d'extraits des registres pertinents.

4.2.1.2 Noms

Tous les noms propres de personnes physiques figurant dans le certificat doivent correspondre aux données des documents d'identité présentés.

Pour les personnes physiques et les noms ne désignant pas des personnes (machines, fonctions, ...) il y a lieu d'indiquer le nom réel du demandeur dans les données d'enregistrement de manière à permettre d'établir l'identité correspondant au pseudonyme.

L'utilisation autorisée de désignations d'entreprise ou d'organisation dans le certificat doit être documentée par des extraits officiels de registre (registre du commerce, registre des associations) ou des pièces officielles analogues.

Les titres professionnels ou académiques protégés figurant dans un certificat doivent également être authentifiés (diplôme ou attestation de l'organisation professionnelle).

4.2.1.3 Procédure d'enregistrement

L'exécution technique et administrative incombe entièrement au prestataire de service de certification. Certains aspects peuvent être confiés sous contrat à des tiers.

La transmission des documents de la demande et des pièces d'identité et de légitimation (données d'enregistrement) peut s'effectuer par télécopieur (fax) ou par voie électronique. Lorsqu'il s'agit de reprendre des données électroniques émanant de tiers, il convient de fixer les processus et les responsabilités par voie contractuelle.

Les données d'enregistrement doivent être archivées avec des copies ou des références des documents d'identité présentés de manière à assurer la correspondance univoque et vérifiable de l'identité numérique des personnes physiques responsables.

La durée d'archivage des données d'enregistrement correspond à la durée de validité du certificat plus 5 ans, conformément au délai de prescription du Code des obligations (CO).

4.2.2 Validité de l'enregistrement

Les documents valables au moment de l'émission du certificat servent de base à l'enregistrement pendant toute la durée de validité du certificat. Si les données d'enregistrement restent inchangées, cette base peut servir aux renouvellements du certificat et à l'établissement d'autres certificats, toutefois pour une durée totale limitée à 6 ans. A l'échéance de ce délai il y a lieu de procéder à un nouvel enregistrement avec présentation de tous les documents.

4.2.3 Clé de client de certificat (Client Certificate Token)

Il peut s'agir d'une clé numérique ou d'une clé technique (par exemple USB). Si la clé émise par le prestataire CSP inclut le code personnel d'utilisation du certificat, elle doit être protégée de manière adéquate (mot de passe, code NIP) empêchant l'usage non autorisé.

4.2.4 Emission et remise de certificats

Le prestataire de service de certification doit assurer par des mesures techniques et organisationnelles que la clé secrète d'un certificat ne puisse être vue ou utilisée par des tiers au cours du processus de protection et de livraison. Après la remise de la clé de certificat la responsabilité de la protection de la clé et du code NIP incombe au détenteur du certificat.

4.2.5 Révocation de certificat

Les données relatives aux certificats révoqués doivent être actualisées et publiées par le prestataire CSP.

4.2.6 Gestion de l'autorité de certification CA

Un plan d'exploitation et de sécurité comprenant le contrôle des accès aux systèmes CA et autres éléments d'infrastructure doit assurer la traçabilité du service de PKI. Un contrôle annuel par des experts (internes ou externes) vérifie le respect des exigences relatives aux composants techniques, au personnel et aux processus.

4.2.7 Politique de certification (CP) et déclaration des pratiques (CPS)

Une politique de certification (Certification Policy, CP) sert de contrat cadre entre le prestataire CSP, le détenteur du certificat et les tiers faisant confiance au certificat. Elle précise l'ampleur des prestations et les caractéristiques garanties des produits et services. Elle doit se conformer à RFC-3647 pour assurer la comparabilité et la transparence des offres.

4.3 Classe 3

Pour les processus économiques ou administratifs exigeant une identification univoque des participants (personnes, organisations, codes de programmes, machines, ...) et l'intégrité des données, il y a lieu de définir un profil correspondant à ces exigences élevées. Ces exigences correspondent de manière générale à celles des certificats qualifiés selon la SCSE, sans se limiter exclusivement aux certificats délivrés à des personnes physiques et au cadre juridique étroit de la loi (responsabilité, renversement du fardeau de la preuve, ...).

Les certificats de Classe 3 permettent de certifier des processus opérationnels multiples selon un niveau comparable à celui du certificat qualifié.

4.3.1 Enregistrement

4.3.1.1 Identification

a) Personnes physiques

Présentation au moment de l'enregistrement d'un document officiel muni d'une photo, tel que

- passeport
- pièce d'identité officielle
- permis d'étranger

Lorsque des données électroniques sont reprises en tant que données d'enregistrement, il y a lieu de garantir de manière traçable que les données électroniques correspondant à une personne ont été établies sur la base d'un contrôle d'identité au sens défini plus haut.

b) Personnes morales, organisations, fonctions, groupes, processus

La commande d'un certificat impersonnel au nom d'une entreprise ou d'une organisation doit être effectuée par un responsable opérationnel ou administratif qui doit prouver son autorisation de signer au moyen d'un extrait officiel de registre. Pour les entreprises il s'agit d'un extrait du registre du commerce. Les autorités et les offices confirment en général la légitimité du mandant par un sceau officiel ou un moyen de preuve similaire. Les autres organisations et les associations doivent aussi fournir des preuves généralement reconnues.

La preuve de l'identité du demandeur doit être fournie conformément aux règles applicables aux personnes physiques.

En pratique les demandes de certificats sont rarement formulées par les fondés de pouvoir mais le plus souvent par des responsables de l'informatique ou d'autres chargés de fonction sans mention au registre du commerce. Pour garantir la cohérence de la chaîne de preuve il faut dans de tels cas qu'un fondé de pouvoir inscrit au registre du commerce autorise par écrit les responsables de l'informatique. La demande formelle peut alors se faire par ces derniers avec preuve de leur identité conformément aux règles susmentionnées. Tous les documents de preuve doivent être joints à la demande..

Exemple 1

Commande de certificat par un chef de section sur papier à en-tête de l'entreprise appuyée par une seconde signature de fondé de pouvoir selon l'extrait du registre du commerce, lequel doit être joint à la demande. Les moyens de preuve visés plus haut sous a) servent à l'identification du mandant.

Exemple 2

Commande de certificat par un responsable de l'informatique avec transmission de données signées numériquement. Le prestataire CSP doit disposer de la procuration délivrée par un fondé de pouvoir en faveur de l'informaticien responsable. Un extrait du registre du commerce doit aussi avoir été présenté. La preuve de l'identité de l'informaticien responsable est fournie conformément aux règles définies sous a).

c) Machines, serveurs, adresses IP publiques

Les certificats de serveurs, routeurs et autres sont demandés par des responsables opérationnels ou administratifs avec preuve de leur identité et de leur légitimation selon les règles définies plus haut. La légitimité d'une demande de certificat pour certains domaines ou adresses IP est en général établie au moyen d'extraits des registres correspondants.

Outre les preuves exigées sous b) il y a lieu, pour les systèmes à accès public, de fournir des preuves appropriées que le demandeur est autorisé à exploiter de tels systèmes.

4.3.1.2 Noms

Tous les noms propres de personnes physiques mentionnés dans un certificat doivent correspondre aux indications des documents d'identité présentés.

S'agissant de personnes physiques et les noms ne désignant pas des personnes (machines, fonctions, ...) il y a lieu d'indiquer le nom réel du demandeur dans les données d'enregistrement de manière à permettre d'établir l'identité correspondant au pseudonyme.

L'utilisation autorisée de désignations d'entreprise ou d'organisation dans le certificat doit être documentée par des extraits officiels de registre (registre du commerce, registre des associations) ou des pièces officielles analogues.

Les titres professionnels ou académiques protégés devant figurer dans un certificat doivent également être authentifiés (acte de remise du titre ou confirmation par l'organisation professionnelle).

4.3.1.3 Procédure d'enregistrement

L'exécution technique et administrative incombe entièrement au prestataire de service de certification. Certains aspects peuvent être confiés sous contrat à des tiers.

Le processus d'enregistrement doit reposer sur une demande personnelle. Le cas échéant cette règle s'applique aussi aux tiers.

La transmission des documents de demande, d'identité et de légitimation (données d'enregistrement) peut s'effectuer

- par remise en mains propres
- par envoi postal
- au moyen de données de tiers signées numériquement

S'agissant de la reprise de données électroniques de tiers, il y a lieu de fixer contractuellement avec ces tiers les processus et les responsabilités. Les données d'enregistrement transmises par voie électronique doivent être signées numériquement par le partenaire contractuel.

Les données d'enregistrement doivent être archivées avec des copies ou des références des documents d'identité présentés de manière à assurer la correspondance univoque et vérifiable de l'identité numérique des personnes physiques responsables.

La durée d'archivage des données d'enregistrement correspond à la durée de validité du certificat plus 11 ans, conformément aux dispositions de la SCSE.

4.3.2 Validité de l'enregistrement

Les documents valables au moment de l'émission du certificat servent de base à l'enregistrement pendant toute la durée de validité du certificat. Si les données d'enregistrement restent inchangées, cette même base peut servir aux renouvellements du certificat et à l'établissement d'autres certificats, toutefois pour une durée totale limitée à 6 ans. A l'échéance de ce délai il y a lieu de procéder à un nouvel enregistrement avec présentation de tous les documents.

4.3.3 Clé de client de certificat (Client Certificate Token)

Les certificats de Classe 3 exigent des clés techniques (USB par exemple) où la clé secrète est protégée par mot de passe ou code NIP contre l'usage non autorisé.

Les clés techniques (hardware) doivent satisfaire aux exigences de FIPS 140-1/140-2 Level 2. Les prescriptions techniques et administratives PTA de l'OFCOM relatives à la SCSE permettent également de déterminer des clés techniques appropriées.

4.3.4 Emission et remise de certificats

Le prestataire de service de certification doit assurer par des mesures techniques et organisationnelles que la clé secrète d'un certificat ne puisse être vue ou utilisée par des tiers au cours du processus de protection et de livraison.

La création des clés s'effectue soit dans les clés de certificat de client elles-mêmes soit sous forme de clés techniques (hardware) analogues.

La transmission de la clé de certificat et du code NIP correspondant s'effectue par remise en mains propres ou par envoi séparé permettant d'assurer la prise en main documentée par le titulaire du certificat.

Après remise de la clé de certificat de client, la responsabilité de la garde au secret de la clé et du code personnel incombe au titulaire du certificat.

4.3.5 Révocation de certificat

Les données relatives aux certificats révoqués doivent être actualisées et publiées par le prestataire CSP au moins une fois par jour.

4.3.6 Gestion de l'autorité de certification CA

Un plan d'exploitation et de sécurité comprenant le contrôle des accès aux systèmes CA et autres éléments d'infrastructure doit assurer la traçabilité du service de PKI. Un contrôle annuel par des spécialistes qualifiés (internes ou externes) vérifie le respect des exigences relatives aux composants techniques, au personnel et aux processus.

4.3.7 Politique de certification (CP) et déclaration des pratiques (CPS)

Une politique de certification (Provider Policy) sert de contrat cadre entre le prestataire CSP, le détenteur du certificat et les tiers faisant confiance au certificat. La politique précise l'ampleur des prestations et les caractéristiques garanties des produits et services. La politique doit se conformer à RFC-3647 pour assurer la comparabilité et la transparence des offres.

4.4 Certificats d'essai

Aucune classe n'a été créée pour des certificats d'essai, et ce pour les motifs suivants :

- Les certificats d'essai sont en général nécessaires dans toutes les applications et chaînes de processus PKI, par exemple pour vérifier la fonctionnalité de l'implémentation et des processus organisationnels au cours de la phase d'introduction.
- Les certificats d'essai ne doivent pas se distinguer dans leur contenu et leur structure des certificats authentiques, sans quoi ils ne pourraient pas remplir leur fonction.
- S'il y a émission systématique de certificats d'essai, il convient de les distinguer des certificats authentiques not pas au niveau du certificat mais à celui de l'autorité de certification (CA).

Une autorité de test (TEST CA) est créée (le cas échéant avec TEST RootCA séparée), dont la désignation indique clairement qu'il s'agit d'une autorité d'essai. Le lien vers la politique (Policy) devrait renvoyer à une politique d'essai (Test Policy) correspondante. En outre une bonne pratique veut que le sujet des certificats de CA ainsi que les certificats de clients émis par elle comportent le terme "TEST".

5 Remarque finale

Il convient pour terminer de constater que même les certificats de Classe 3 ou selon la SCSE, tout comme dans le monde réel, ne peuvent garantir de manière absolue la fiabilité des données certifiées. Des identités numériques falsifiées peuvent survenir par suite de faux documents d'identité présentés par des personnes ayant des intentions délictueuses, à la suite de processus défectueux ou lacunaires lors de l'enregistrement ou en raison de collaborateurs mal intentionnés au sein des autorités d'enregistrement ou de certification.

Les niveaux de qualité des identités numériques dépendent moins des processus ou des algorithmes cryptographiques utilisés que d'une chaîne de processus administratifs et techniques systématiquement axée sur la sécurité et la traçabilité :

- Définition du mandat / Données d'enregistrement
- Vérification d'identité / Journalisation / Archivage
- Transmission des données à l'autorité de certification CA
- Exploitation et gestion des interfaces de l'infrastructure de CA
- Logistique de transmission des certificats, clés, codes NIP
- Actualisation et mise à disposition des données concernant les révocations

En fin de compte la présente norme eCH vise l'uniformisation des exigences et la transparence des processus de manière à assurer la sécurité des procédures d'émission.

6 Exclusion de responsabilité – Droits de tiers

Les normes élaborées par l'Association **eCH** et mises gratuitement à la disposition des utilisateurs, ainsi que les normes de tiers adoptées, ont seulement valeur de recommandations. L'Association **eCH** ne peut en aucun cas être tenue pour responsable des décisions ou mesures prises par un utilisateur sur la base des documents qu'elle met à disposition. L'utilisateur est tenu d'étudier attentivement les documents avant de les mettre en application et au besoin de procéder aux consultations appropriées. Les normes **eCH** ne remplacent en aucun cas les consultations techniques, organisationnelles ou juridiques appropriées dans un cas concret.

Les documents, méthodes, normes, procédés ou produits référencés dans les normes **eCH** peuvent le cas échéant être protégés par des dispositions légales sur les marques, les droits d'auteur ou les brevets. L'obtention des autorisations nécessaires auprès des personnes ou organisations détentrices des droits relève de la seule responsabilité de l'utilisateur.

Bien que l'Association **eCH** mette tout en oeuvre pour assurer la qualité des normes qu'elle publie, elle ne peut fournir aucune assurance ou garantie quant à l'absence d'erreur, l'actualité, l'exhaustivité et l'exactitude des documents et informations mis à disposition. La teneur des normes **eCH** peut être modifiée à tout moment sans préavis.

Toute responsabilité relative à des dommages que l'utilisateur pourrait subir par suite de l'utilisation des normes **eCH** est exclue dans les limites des réglementations applicables.

7 Droits d'auteur

Tout auteur de normes **eCH** en conserve la propriété intellectuelle. Il s'engage toutefois, par une convention écrite spéciale, à mettre gratuitement, et pour autant que ce soit possible, la propriété intellectuelle en question ou ses droits à une propriété intellectuelle de tiers à la disposition des groupes de spécialistes respectifs ainsi qu'à l'association **eCH**, pour une utilisation et un développement sans restriction dans le cadre des buts de l'association.

Les normes élaborées par les groupes de spécialistes peuvent, moyennant mention des auteurs **eCH** respectifs, être utilisées, développées et déployées gratuitement et sans restriction.

Les normes **eCH** sont complètement documentées et libres de toute restriction relevant du droit des brevets ou de droits de licence. La documentation correspondante peut être obtenue gratuitement.

Les présentes dispositions s'appliquent exclusivement aux normes élaborées par **eCH**, non aux normes ou produits de tiers auxquels il est fait référence dans les normes **eCH**. Les normes incluront les références appropriées aux droits de tiers.

Annexe A – Références & Bibliographie

CH Bases légales

Vue d'ensemble <http://www.bakom.ch/themen/internet/00467/index.html?lang=fr>

RS 943.03, SCSE	Loi fédérale du 19 décembre 2003 sur les services de certification dans le domaine de la signature électronique (Loi sur la signature électronique, SCSE) (du 19.12.2003, en vigueur depuis 01.01.2005)
RS 943.032 OSCSE	Ordonnance sur les services de certification dans le domaine de la signature électronique (du 03.12.2004)
RS 943.032.1 PTA Version 2	Prescriptions techniques et administratives, version 2 (Ordonnance de l'OFCOM sur les services de certification dans le domaine de la signature électronique, Annexe) (du 29.07.2005, en vigueur depuis 01.09.2005)
RS 641.201.1 OelDI	Ordonnance du DFF concernant les données et les informations transmises par voie électronique (du 30.01.2002)
RS 221.431 Olico	Ordonnance concernant la tenue et la conservation des livres de comptes (du 24.04.2002)
RS 221.415 Ordonnance FOSC	Ordonnance sur la Feuille officielle suisse du commerce (du 21.02.2006)
RS 431.02 LHR	Loi fédérale sur l'harmonisation des registres des habitants et d'autres registres officiels de personnes (Loi sur l'harmonisation des registres) (23.06.2006)

Directive UE

1999/93/CE	Directive 1999/93/CE du Parlement européen et du Conseil du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques http://europa.eu/scadplus/leg/fr/lvb/l24118.htm http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31999L0093:FR:HTML
------------	---

Publications ETSI

ETSI TS 101 456	Policy requirements for certification authorities issuing qualified certificates
ETSI TS 101 862	Qualified Certificate Profile
ETSI TS 101 733	CMS Advanced Electronic Signatures (CAeS)
ETSI TS 101 903	XML Advanced Electronic Signatures (XAeS)
ETSI TR 102 040	International Harmonization of Policy Requirements for CAs issuing Certificates
ETSI TS 102 042	Policy requirements for certification authorities issuing public key certificates
ETSI TR 102 044	Requirements for role and attribute certificates
ETSI TR 102 045	Signature policy for extended business model
ETSI TS 102 176-1	Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms

CEN Workshop Agreements

CWA 14169	Secure Signature-Creation Devices "EAL 4+"
CWA 24272-5	EESSI Conformity Assessment Guidance - Part 5: Secure signature-creation devices
CWA 24272-6	EESSI Conformity Assessment Guidance - Part 6: Signature-creation device supporting signatures other than qualified

Norme ISO

ISO/IEC 15408	Information technology - Security techniques. Evaluation criteria for IT security
---------------	---

ITSEC

ITSEC	Information Technology Security Evaluation Criteria
-------	---

Recommendation UIT-T

X.509	X.509 : Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks (03-2000) http://www.itu.int/rec/recommendation.asp?type=folders&lang=e&parent=T-REC-X.509
-------	---

Normes NIST

FIPS 140-1 / FIPS 140-2	Security requirements for Cryptographic Modules
----------------------------	---

pkix RFCs

<http://www.ietf.org/html.charters/pkix-charter.html>

3279	Algorithms and Identifiers for the PKI Certificate and CRI Profile
3280	PKI Certificate and CRL Profile
3647	Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework
3739	PKI Qualified Certificates Profile

Annexe B – Collaboration & Supervision

Collaboration	<p>Groupe spécialisé eCH Sécurité</p> <p>Gerold H. Werner, max. consult AG, max.consult-ag@bluewin.ch</p> <p>Adrian Müller, Dr. Otto Müller Consulting adrian@mueller-consulting.biz</p> <p>Roland Wichtermann, VBS roland.wichtermann@gst.admin.ch</p> <p>Daniel Messerli; Ergonomics dmesserli@ergonomics.ch</p>
---------------	--

Annexe C – Abréviations

CA / AC	Certification Authority – Autorité de certification
CEN / ISSS	Comité Européen de Normalisation / Information Society Standardization System (http://www.cenorm.be/iss) – Initiative du CEN pour la normalisation des technologies d'information et de communication (TIC)
CN	Common Name – champ de certificat X.509 : nom du détenteur du certificat
CO	Code des obligations
CP	Certification Policy : politique de certification
CPS	Certification Practice Statement : Déclaration des pratiques de certification
CRL	Certificate Revocation List – Liste des certificats révoqués par un prestataire de service de certification
CSP	Certification Service Provider : prestataire de service de certification
CWA	CEN Workshop Agreement – Accord d'atelier du CEN : spécifications élaborées par les ateliers du CEN
EESC	E-Europe SmartCard Initiative (http://www.eeurope-smartcards.org/) - Groupes de travail : B1 Electronic Identity (e-ID), TB5 E&M Payments with SmartCards
EESSI	European Electronic Signature Standardization Initiative : Initiative européenne pour la standardisation de la signature électronique
ETSI	European Telecommunications Standards Institute – Institut européen des normes de télécommunication (http://www.etsi.org/)
FIPS	Federal Information Processing Standards – normes IT de NIST (sécurité)
HSM	Hardware Security Module : composants assurant la production et le stockage de clés privées (Private Keys) et de toutes les fonctionnalités PKI (signature numérique, hash, cryptage et décryptage, etc.). Les HSM sont intégrés sous forme de crypto-adaptateurs dans le serveur de l'autorité de certification CA ou le serveur de signatures, ou comme élément de réseau de plusieurs serveurs de CA ou de signature. Les processus propres aux HSM. Permettent la sauvegarde (backup) et la restauration (recovery) des clés et des certificats au moyen d'une procédure sécurisée
IETF	Internet Engineering Task Force
ISO	Organisation internationale de normalisation
LRA	Local Registration Authority
NIST	National Institute of Standards and Technology (http://csrc.nist.gov/publications)
OFIT	Office fédéral de l'informatique et de la télécommunication (http://www.bit.admin.ch/)
OSCSE	Ordonnance sur les services de certification dans le domaine de la signature électronique
PKI	Public Key Infrastructure : infrastructure à clé publique
RFC	Request for Comment (document de référence internet)
SAN	Subject Alternate Name – champ optionnel de certificat X.509 pour noms complémentaires de sujet
SCSE	Loi sur les services de certification dans le domaine de la signature électronique (Loi sur la signature électronique)
PTA	Prescriptions techniques et administratives (ordonnance OFCOM / Annexe – voir sous bases légales)
UIT	Union internationale des télécommunications
URL	Uniform Resource Locator : adresse univoque d'une information sur internet