EIDGENÖSSISCHE FINANZKONTROLLE
CONTRÔLE FÉDÉRAL DES FINANCES
CONTROLLO FEDERALE DELLE FINANZE
CONTROLLA FEDERALA DA FINANZAS

# Office fédéral de l'informatique et de la télécommunication

## Dans quelle mesure l'infrastructure Admin PKI répond-elle aux objectifs définis à l'origine ainsi qu'aux besoins de l'administration fédérale et des cantons ?

**Texte original en allemand**

11 juin 2007

**Table des matières**

**Abréviations et glossaire**

| | |
|---|---|
| OFIT | Office fédéral de l'informatique et de la télécommunication |
| Admin | Administration fédérale |
| CA | Autorité de certification (Certification Authority) |
| CSP | Fournisseur de services de certification (Certification Service Provider) |
| DFS | Tachygraphe numérique (projet de l'OFROU) |
| CDF | Contrôle fédéral des finances |
| e-dec | Déclaration en douane électronique |
| E-Gov | Cyberadministration (communication électronique avec les autorités) |
| e-pass | Passeport suisse contenant des informations lisibles électroniquement telles que la photo passeport, empreintes digitales, etc. ; certificat visant à éviter les falsifications |
| DFJP | Département fédéral de justice et police |
| CI | Conseil de l'informatique de la Confédération |
| USIC | Unité de stratégie informatique de la Confédération |
| CA | Comptabilité analytique |
| LRA | Autorité locale d'enregistrement (Local Registration Authority) |
| NMC | Nouveau modèle comptable incluant une comptabilité analytique pour l'administration fédérale |
| PKI | Infrastructure à clé publique (Public Key Infrastructure) |
| RA | Autorité d'enregistrement (Registration Authority) |
| ROI | Retour sur investissement (Return on Investment) |
| SCMS | Système de gestion des cartes à puce (Smart Card Management System) |
| CSI | Conférence suisse de l'informatique |
| Portail SSO | Portail Single-Sign-On permettant d'authentifier de manière centralisée les usagers externes (essentiellement en provenance des cantons) sur les applications du DFJP |
| SCSE | Loi fédérale sur les services de certification dans le domaine de la signature électronique ; RS 943.03 |

# 1 Résumé du contrôle effectué

Le CDF a procédé auprès de l'Office fédéral de l'informatique et de la télécommunication (OFIT) à un examen portant sur l'infrastructure et les prestations de base servant à l'infrastructure Admin PKI - et permettant d'émettre des certificats. Le contrôle a surtout consisté à examiner l'évolution du projet, son fonctionnement actuel et les perspectives d'avenir. L'infrastructure Admin PKI comprend tous les processus ainsi que les logiciels et le matériel qui permettent d'émettre des certificats correspondants à différents niveaux de qualité.

Après des débuts et quelques tentatives ardus et parfois malheureux (cf. chap. 4), l'OFIT a finalement réussi à créer les infrastructures et les processus permettant de fournir des certificats pour les applications de l'administration fédérale, des cantons et aussi des communes. Outre les certificats de classes A à D définis pour l'administration fédérale, l'OFIT peut proposer des certificats spécifiques, adaptés aux besoins des clients et de leurs applications. Avec la certification par KPMG qui devrait intervenir durant le second trimestre de 2007 et concerner les services de certification de classe A (SCSE), l'infrastructure Admin PKI et partant, l'OFIT, auront prouvé leurs capacités et qualités à un niveau élevé. Côté pratique, la pièce de résistance a été d'émettre 25 000 certificats à l'intention des cantons en 2006. Au moment de la révision, plus de 40 000 certificats de différents niveaux de qualité étaient en fonction.

Aujourd'hui, l'OFIT est reconnu par tous les cantons et par la Conférence suisse sur l'informatique (CSI) comme fournisseur primaire de certificats. Outre le portail SSO, il existe d'autres applications transversales telles que le système d'information en matière de placement et de statistique du marché du travail (PLASTA), la déclaration en douane électronique (e-dec), la distribution de courriers électroniques cryptés et signés (secure-messaging), etc. fonctionnels ou en voie de l'être. Le prix de ces certificats n'est pas au centre de nos préoccupations vu qu'il évolue dans une marge concurrentielle et acceptable. Compte tenu des débuts assez chaotiques de l'infrastructure actuelle Admin PKI, il est compliqué de procéder à un calcul de rentabilité correct concernant les investissements consentis jusqu'à présent et se montant à 12 millions de francs. Ce sont en principe le client, ou plus spécifiquement les applications qui tirent profit d'une PKI, puisque des moyens simples permettent d'obtenir un niveau élevé de sécurité. Le potentiel en matière d'émission d'autres certificats est donc important. La vente de certificats devrait couvrir les frais courants de l'entreprise et ceux générés par les développements techniques nécessaires. Certes, d'autres solutions en matière de sécurité seraient parfois plus avantageuses mais compliqueraient cependant, de par leur hétérogénéité, d'importantes solutions de cyberadministration. La technologie PKI disponible à l'OFIT permet de recourir à des solutions standard communes à tous les échelons de l'administration, mais également à tout le pays en raison de la collaboration qui s'est instaurée avec d'autres entreprises certifiées SCSE comme p. ex. La Poste et le produit IncaMail. Les cantons peuvent également acquérir des certificats auprès d'autres fournisseurs; toutefois, il est fort probable qu'ils utiliseront à plusieurs reprises les certificats déjà fonctionnels de l'infrastructure Admin PKI. Quant aux fournisseurs certifiés SCSE présents sur le marché suisse (Quo Vadis, Swisscom et La Poste-SwissSign), ils sont des partenaires potentiels de l'OFIT, puisque plusieurs solutions de cyberadministration sont envisageables avec la reconnaissance mutuelle des certificats.

Plusieurs études ont porté sur les besoins en solutions PKI en Suisse. Cependant, il n'est pas possible d'avoir une vue d'ensemble à l'échelon du pays concernant les classes A à D définies par l'administration fédérale, étant donné que les autres fournisseurs ont défini leurs propres classes. De par leur large diffusion dans les administrations publiques, les certificats deviendront avec le temps une évidence, pour autant que l'administration fédérale donne l'impulsion nécessaire à leur utilisation. Les coûts vont rester constants, mais se répartiront sur beaucoup plus de certificats qu'actuellement. Les certificats de la classe A sont pour l'instant les seuls à être régis par une loi en Suisse. Leur utilisation potentielle est cependant considérée comme moindre, étant donné le faible nombre d'affaires juridiques exigeant la signature manuscrite (p. ex. vente avec paiements préalables) qui équivaut à la signature électronique qualifiée. Le certificat en tant que tel - c'est-à-dire de qualité labellisée via la certification – sert cependant à instaurer la confiance de manière générale entre les fournisseurs. Partant, le CDF considère comme parfaitement approprié de la part de l'OFIT de proposer cette classe de certificat.

Les attentes et la confiance mises dans l'OFIT concernant ses certificats sont actuellement très grandes. A l'avenir, les exigences les concernant ne seront pas définies sur la base d'un savoir central commun mais au contraire en fonction des souhaits des clients. L'OFIT a montré qu'il était en mesure de répondre aux exigences organisationnelles et techniques inhérentes à un fournisseur de services de certification (CSP). La certification SCSE concerne non seulement l'infrastructure Admin PKI mais a également des répercussions sur tout l'OFIT (processus, documents, infrastructure, etc.). Des prestations solides, une disponibilité élevée et une qualité avérée contribuent à étayer la confiance déjà réelle des clients. C'est à ce niveau que reposent les chances futures de l'infrastructure Admin PKI aussi bien dans l'optique du marché qu'en matière de financement.

Les recommandations émises par le CDF dans le présent rapport sont suivies à chaque fois des **prises de position de l'OFIT**. Lors de sa cinquième séance qui s'est tenue en août 2007, la **Délégation des finances** a pris connaissance du rapport du CDF.

# 2 Mandat et déroulement de l'examen

## 2.1 Mandat

Conformément aux art. 6 et 8 de la loi fédérale sur le Contrôle fédéral des finances (LCF ; RS 614.0), le CDF a soumis en avril 2007 l'infrastructure Admin PKI à un examen. Le mandat consistait à examiner dans quelle mesure le développement et l'exploitation de l'infrastructure Admin PKI répondaient aux objectifs définis à l'origine ainsi qu'aux besoins de l'administration fédérale et des cantons.

L'examen a avant tout consisté à:
- mettre en lumière l'historique du projet depuis 2001 et les principales décisions;
- évaluer le niveau d'avancement actuel, l'implémentation et l'exploitation actuelles;
- évaluer les coûts consentis jusqu'à présent et à l'avenir, compte tenu de la rentabilité;
- constater l'avancement de la certification par KPMG ;
- juger des besoins actuels et futurs des partenaires (cantons) et clients ainsi que de la satisfaction des clients.

Les évaluations se sont basées sur les documents de projet disponibles à partir de 2001 ainsi que les données financières accessibles au moment de la révision.

## 2.2 Fondements juridiques

- Loi fédérale du 28 juin 1967 sur le Contrôle fédéral des finances (état au 20 juillet 1999) (RS 614.0)
- Loi du 7 octobre 2005 sur les finances de la Confédération (Loi sur les finances, LFC, RS 611.0)
- Ordonnance du 5 avril 2006 sur les finances de la Confédération (OFC ; RS 611.01)
- Loi fédérale sur les services de certification dans le domaine de la signature électronique (Loi sur la signature électronique, SCSE, RS 943.03)
- Ordonnance sur les services de certification dans le domaine de la signature électronique (Ordonnance sur la signature électronique, OSCSE, RS 943.032)
- Prescriptions techniques et administratives concernant les services de certification dans le domaine de la signature électronique (RS 943.032.1 / Annexe)
- Ordonnance du DFF concernant les données et les informations transmises par voie électronique (OelDI, RS 641.201.1)
- Ordonnance du 26 septembre 2003 sur l'informatique et la télécommunication dans l'administration fédérale (Ordonnance sur l'informatique dans l'administration fédérale, OIAF, RS 172.010.58)

## 2.3 Etendue de l'examen et principes prévalants

Les vérifications ont été effectuées par les réviseurs informatiques Peter Bürki, Stefan Wagner et Cornelia Simmen (responsable de la révision). Afin de satisfaire au mandat d'audit, il s'est agi de consulter une documentation volumineuse et de procéder à des interviews de personnes en charge des différents projets partiels à l'OFIT ainsi que dans plusieurs autres services impliqués

(USIC, CSI, cantons d'AG et de ZH, SG DFF). Les détails concernant le genre et l'étendue des contrôles effectués découlent des documents de travail.

### 2.4 Documents et renseignements fournis

Toutes les personnes sollicitées ont fourni très rapidement et ouvertement les renseignements demandés. Les documents exigés, parfois très volumineux, ont été mis à disposition de l'équipe en charge de la révision rapidement et dans leur intégralité.

### 2.5 Priorité donnée aux recommandations du CDF

Du point du vue du mandat de révision, le CDF juge l'importance des recommandations et des remarques selon 3 priorités (1 = élevée, 2 = moyenne, 3 = faible). Tant le facteur **risque** [par exemple, volume des conséquences financières, resp. importance des constatations; probabilité de survenance d'un dommage; fréquence de cette lacune (cas isolé, plusieurs cas similaires, généralité) et répétition; etc.] que le facteur **urgence de la mise en œuvre** (court, moyen et long terme) sont pris en compte.

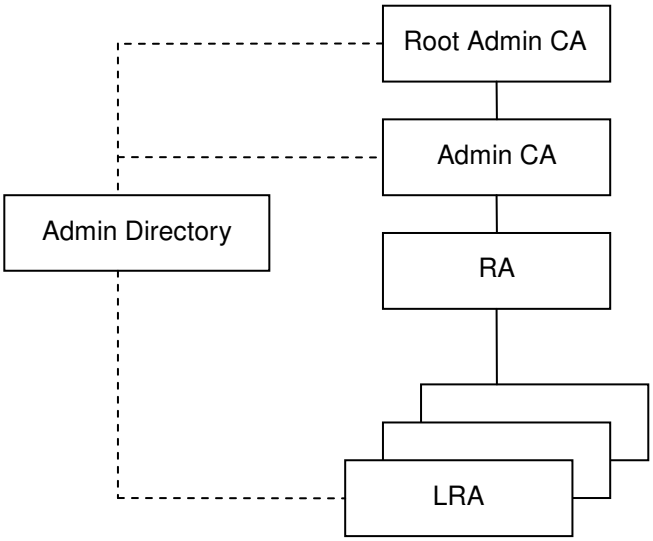
## 3 Introduction

En raison de la mise en réseau des composants informatiques, la transmission électronique des données est en constante progression. Néanmoins, dans les cas juridiquement contraignants, il faut être sûr que les données transmises (p. ex. courrier électronique, commande ou confirmation) proviennent effectivement de l'expéditeur supposé, que le contenu n'ait pas été modifié lors de la transmission ou de l'enregistrement et qu'il existe une traçabilité au niveau de la transmission. Satisfaire à ces nombreuses exigences de sécurité implique différentes réglementations, soit:

- des bases juridiques (lois, ordonnances) régissant l'égalité de traitement entre le courrier électronique et le courrier écrit;
- des fondements organisationnels garantissant la sécurité des processus afin qu'il y ait traçabilité de la livraison, à l'instar d'un courrier postal en recommandé, et instaurant les conditions d'un exercice justifié de toutes les activités entrant dans ce contexte;
- des bases techniques garantissant l'identifiabilité et l'invariabilité, standardisées et reconnues aussi bien au plan national qu'international.

Des notions telles qu'infrastructure à clé publique (Public Key Infrastructure [PKI]), autorité de certification (CA), certificats, authentification, signature et cryptage électroniques sont en lien direct avec les bases juridiques, électroniques et organisationnelles.

Par **infrastructure à clé publique** (PKI), on entend tous les processus, architectures, serveurs, postes de travail et logiciels servant à l'émission de certificats. Une infrastructure PKI est structurée hiérarchiquement et comprend les principaux éléments suivants:




- **L'autorité de certification Root Admin (Root Admin Certification Authority** [CA]) est responsable de la validation et des listes concernant les certificats adjugés, donc du contrôle de l'Admin CA
- L'**Admin CA de l'OFIT** est responsable de l'émission, de la gestion et de la publication des certificats
- L'**autorité d'enregistrement** (RA) **de l'OFIT** gère les demandes de certificats
- L'**autorité locale d'enregistrement** (LRA) décentralisée est compétente pour l'identification d'un requérant de certificats, pour générer les paires de clés et pour les reporter sur les cartes à puce
- Enfin l'**Admin-Directory** enregistre de manière contraignante et publie tous les certificats autorisés et bloqués.

Les besoins liés à la mise en œuvre de **certificats** découlent des exigences de sécurité des applications. En fonction des domaines, les exigences d'authentification, de signature et de cryptage varient de manière indépendante ou en interagissant entre elles. Les certificats peuvent se présenter sous forme de matériel (p. ex. carte à puce, token) ou de logiciel (soft certificate). A l'image du passeport suisse, le certificat est garant d'une exigence morale concernant la crédibilité de celui qui l'émet et d'exigences techniques concernant la sécurité, donc son caractère infalsifiable.

Quatre classes de certificats ont été définies dans l'administration fédérale:

- **Classe D**, qualité moyenne, pour authentifier de manière sûre des personnes ou des machines, soft certificate, utilisation p. ex. pour accéder à des réseaux externes à partir d'applications fonctionnant sur le réseau de la Confédération
- **Classe C**, qualité moyenne, permet l'authentification, le cryptage et la signature de manière sûre, soft certificate, utilisation p. ex. pour crypter le courrier électronique (secure-messaging) au sein de l'administration fédérale

- **Classe B**, qualité très élevée, renforce l'authentification, le cryptage et la signature, certificat personnel sur carte à puce, octroyé uniquement après identification personnelle sur présentation d'un passeport ou d'une carte d'identité valable
- **Classe A**, exigences de qualité très élevées, réglées légalement, signature électronique qualifiée équivalent à une signature manuscrite reconnue au plan juridique, cf. chap. 5.6

Pour satisfaire à des exigences spécifiques en matière d'authentification, de cryptage et de signature, l'OFIT peut fournir des certificats spéciaux créés sur mesure en se référant aux classes définies ci-dessus.

# 4 Historique de l'infrastructure Admin PKI

Ayant pris connaissance du rapport « Création d'une infrastructure de certification pour l'administration fédérale », le Conseil fédéral a donné le mandat en janvier 1999 d'élaborer une infrastructure de certification pour l'administration fédérale. Il a chargé le DETEC de coordonner les travaux, le DFF d'élaborer les bases techniques et le DFJP de préparer tout le volet concernant le caractère juridiquement contraignant des signatures électroniques.

## 4.1 Coordination et bases techniques

Il est impossible de se prononcer concernant les tâches de coordination du DETEC étant donné qu'il n'y a aucun document correspondant dans les dossiers examinés et que cette coordination ne faisait pas non plus l'objet du contrôle réalisé.

Sur la base du volume financier du projet estimé entre 3 et 5 millions de francs à l'époque, un appel d'offres OMC a été lancé en 1999 pour le projet „Secure Messaging“ (FOSC, no 123, 29.6.1999). Lorsqu'en 2000, le coup d'envoi a été donné, une solution de courrier électronique sécurisée dans toute l'administration fédérale avait été retenue. Cette solution se basait sur des certificats de l'entreprise Swisskey, qui, une année plus tard, au milieu du projet, abandonnait le marché. L'OFIT a donc dû décider en 2001, soit de s'adresser à des fournisseurs étrangers pour les certificats liés au projet secure messaging, soit de faire le pas et de produire lui-même des certificats. La variante interne a été retenue et fin 2001 l'OFIT a pu présenter une infrastructure Admin PKI fonctionnelle, c'est-à-dire que les propres certificats étaient produits, publiés et gérés, tandis qu'un local à cet effet était aménagé et sécurisé. Néanmoins, le projet secure messaging est resté au stade de projet pilote, la solution choisie n'ayant pas réussi à s'imposer, trop peu de certificats ayant été générés.

Dès 2002, les obstacles se sont accumulés. D'une part, l'Unité de stratégie informatique de la Confédération (USIC) s'est opposée à la mise en place d'un CA spécifique à la Confédération, arguant qu'il n'y avait aucun besoin au sein de l'administration fédérale ou des cantons, que cette tâche n'entrait pas dans les attributions-clés de la Confédération et que les certificats pouvaient être achetés. Or, l'OFIT avait été mandaté par le Conseil fédéral pour émettre des certificats. Par ailleurs, l'OFIT a longtemps jugé que la seule manière correcte de satisfaire à tous les besoins en matière de sécurité consistait en une solution matérielle unique avec des certificats pour les fonctions d'authentification, de cryptage et de signature. Cela a eu pour résultat que les autres projets PKI ont plutôt stagné de 2001 à 2004. Cette situation a fait que durant le même laps de temps les cantons ont cherche à trouver eux-mêmes des solutions en matière de certificats.

En 2003 a eu lieu l'appel d'offres puis la réalisation des certificats actuels de classe B. Cependant l'acquisition d'un système de gestion des cartes à puce (Smartcard Management Systems [SCMS]) a été suspendue étant donné la faible quantité des certificats émis. En août de la même année, le CI a donné son accord de principe à une infrastructure à clé publique (Admin PKI) gérée exclusivement par l'OFIT. Puis en octobre et décembre, il a été décidé que les prestations de l'Admin PKI d'alors devraient être également proposées aux cantons pour les classes 2 et 3 (classes B et C actuelles). En revanche, à ce moment-là, rien n'a été réglé de manière explicite pour savoir qui assumerait les investissements déjà consentis et futurs ainsi que l'exploitation. Les dépenses liées à l'infrastructure Admin PKI ne peuvent être suivies dans le compte d'Etat qu'à partir de 2004. Rétrospectivement, il faut concéder que sans la ténacité de l'OFIT, l'infrastructure Admin PKI (représentant alors déjà des investissements de plus de 2 millions de francs) n'aurait pas vu le jour.

En 2004, l'USIC a mené une enquête auprès de l'administration fédérale et des cantons pour connaître les besoins en certificats. Ces résultats ont contribué au fait que le CI décide le 24 mai 2004 de mandater „officiellement" l'OFIT pour l'exploitation de l'infrastructure Admin PKI afin d'émettre des certificats des classes B, C et D au titre de prestation transversale bénéficiant des moyens transversaux adéquats. Cette décision a notamment contribué au fait qu'il a été possible de comparer les solutions lancées dans l'intervalle par d'autres services (p. ex. le canton de Zurich) avec celles de l'infrastructure Admin PKI.

Le projet de réorganisation „Change BIT" de 2005 a permis de régler différemment les responsabilités concernant l'infrastructure Admin PKI. On a alors reconnu à l'OFIT les atouts que présentaient des projets tels que l'e-pass, le DFS et le portail SSO. Via une communication notablement améliorée et une meilleure dotation en personnel de l'équipe PKI, l'infrastructure Admin PKI s'est lentement mais régulièrement développée. Le CI a donné en outre à l'OFIT le feu vert à la certification par KPMG, de manière qu'il soit également possible d'émettre des certificats de la classe A selon SCSE, à condition toutefois que ceux-ci ne soient pas financés par des moyens transversaux.

C'est finalement en 2006 que l'infrastructure Admin PKI a vraiment pu décoller, déployant quelque 25 000 certificats de classe B pour le portail SSO du DFJP, démontrant ainsi une large reconnaissance des solutions de l'OFIT par les cantons. Cette expérience a notablement contribué au niveau et au savoir-faire actuels de l'équipe PKI à l'OFIT. Cette mise à l'épreuve axée sur la pratique s'est déroulée parfois dans une ambiance confuse ; cependant dans l'ensemble on peut la considérer comme réussie. Ce succès et les expériences qui en ont découlé ont également contribué à réactiver les projets „Relaunch Secure Messaging (RSM)" et „Smart Card Management System (SCMS)".

Conformément à la décision du CI, l'OFIT a soumis en 2006 les certificats de classe A à la certification de KPMG. Concernant ce projet, d'emblée l'émission de certificats n'a jamais été privilégiée, l'OFIT souhaitant au contraire obtenir de la sorte un label de qualité répondant aux normes nationales et internationales, devant servir à asseoir la confiance pour toute l'infrastructure Admin PKI et donc également pour l'OFIT.

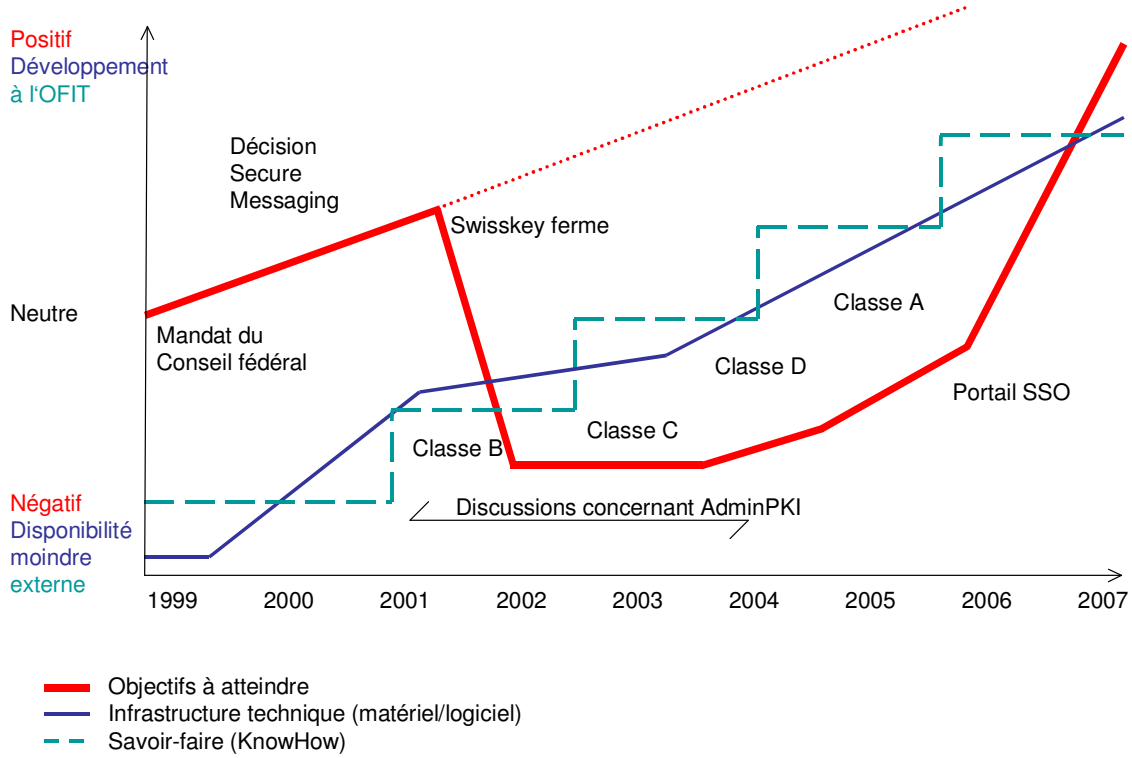
L'évolution du marché des certificats montrera dans quelle mesure l'infrastructure Admin PKI arrivera à se profiler et sera influencée par le secteur économique.

### 4.2 Bases légales

Les dispositions réglementaires nécessaires au niveau juridique ont été considérées comme généralement remplies. Il est de notoriété que les documents signés maintenant de manière numérique égalent juridiquement des documents papier, à condition toutefois que les conditions prescrites par la loi soient remplies. Les lois et ordonnances ont donc été adaptées en conséquence, envoyées en consultation et sont depuis quelques années en vigueur.

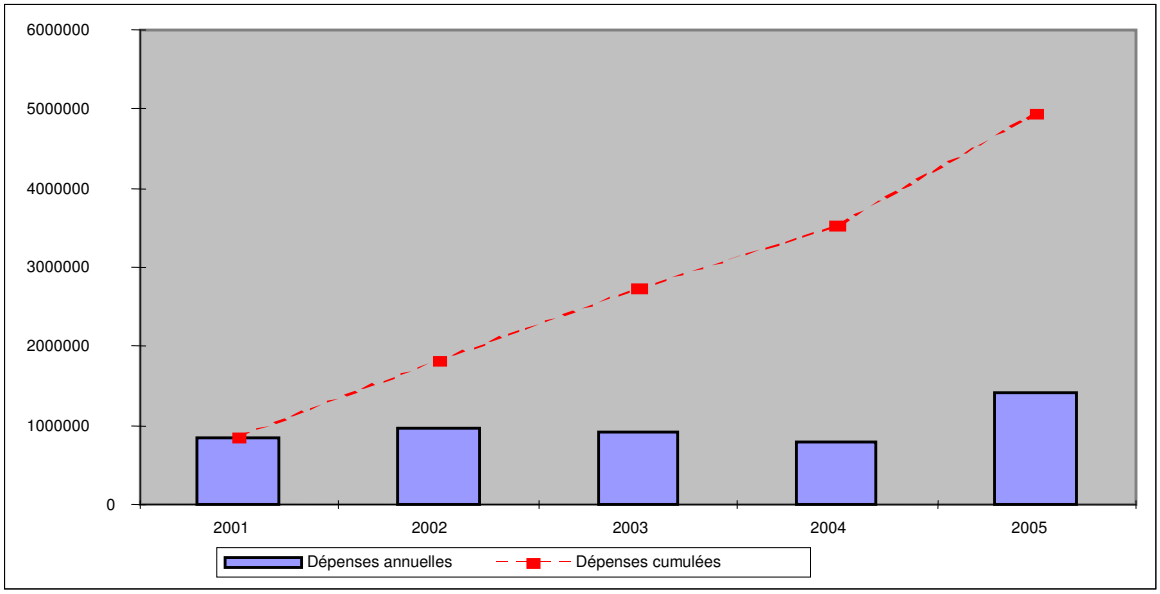
### 4.3 Aperçu graphique des différentes étapes

La ligne **rouge** indique le niveau atteint concernant les objectifs à atteindre. Depuis le mandat initial du Conseil fédéral, la progression s'est faite dans le cadre prévu. La disparition de Swisskey a sensiblement freiné le projet. La réalisation des certificats des classes B, C et D a permis une amélioration continue, leur utilisation pour le portail SSO donnant le véritable coup d'envoi.
La ligne **bleue** montre l'évolution de l'infrastructure technique (matériel et logiciels).
Quant à la ligne **verte**, elle représente le savoir-faire acquis suite au développement de l'infrastructure ainsi que les expériences obtenues.



### 4.4 Aperçu graphique des finances

Le graphique ci-dessous se réfère à un résumé du CDF concernant les factures examinées. Il ne saurait être considéré comme exhaustif, ne comprenant que les coûts externes.




## 5 Situation actuelle

### 5.1 Situation dans les faits

Ainsi que le montre l'histoire de l'infrastructure Admin PKI, cette dernière a dû surmonter bon nombre de difficultés initiales avant de pouvoir s'implanter. Rétrospectivement, un temps précieux a été gaspillé alors que des moyens financiers ont été dépensés à perte. Toutefois, la responsabilité n'en incombe pas uniquement à l'OFIT. En effet, ni l'administration fédérale, ni le marché suisse n'étaient véritablement prêts entre 2001 et 2004 pour une mise en œuvre de certificats au niveau national. La demande inexistante en certificats a conduit à la faillite des entreprises comme Swisskey. Les avantages et possibilités des certificats étaient alors encore trop peu reconnus et appréciés.

Avec la décision du DFJP de créer un portail Single-Sign-On-Portal pour renforcer l'authentification de tous les utilisateurs de ses applications spéciales, l'infrastructure Admin PKI a revêtu une nouvelle importance et pris un nouvel essor. Finalement, au dernier moment, l'OFIT a réussi en 2005 à concrétiser ce mandat exigeant grâce à une nouvelle équipe et à donner sa vitesse de croisière à l'infrastructure Admin PKI actuelle. La mise à disposition avant la fin de l'année de plus de 20 000 certificats de classe B a posé des exigences élevées à tous les intervenants qui évoluaient dans un univers plutôt hostile étant donné que dans la phase initiale il y a souvent eu des réactions de mécontentement de la part des clients.

Finalement, l'équipe actuelle a réussi à donner une nouvelle vie à l'infrastructure Admin PKI et à passer l'épreuve, connaissant certes au début des difficultés mais concluant avec de bonnes notes. Cette expérience a aussi permis d'acquérir de nouvelles informations capitales. Bien qu'à

l'heure actuelle, des classes standard de certificats sont définies dans le catalogue des produits de l'OFIT, elles ne sont plus vendues de manière aussi rigide. De manière croissante, des certificats spécifiques aux applications sont développés et fournis. Grâce au savoir-faire acquis, l'équipe PKI est suffisamment préparée pour réagir de manière ponctuelle et optimale aux souhaits des clients. Ceux-ci peuvent consulter à l'adresse Internet http://internet.bit.admin.ch/adminpki/ non seulement des descriptifs des produits mais également de nombreuses publications : directives, normes, listes de contrôle, etc. Dans ce domaine également, de grands progrès ont été réalisés.

Du côté des clients, il y aura toujours des réactions plus ou moins positives étant donné qu'une infrastructure PKI ne sera jamais totalement complète et fermée, nécessitant sans cesse des nouveautés, des adaptations et des extensions au niveau technique. L'équipe en charge de la révision a cependant reçu bon nombre d'échos positifs et considère que l'infrastructure Admin PKI actuelle a atteint un bon niveau. L'OFIT a prouvé que du travail de qualité pouvait aussi trouver preneur en dehors de l'administration fédérale. Il est vrai que certains points faibles connus devront être améliorés, voire éliminés. Dans l'ensemble, il existe cependant une base solide sur laquelle l'OFIT peut s'appuyer pour les développements futurs et avoir ainsi de bonnes chances de devenir l'un des principaux fournisseurs de certificats en Suisse.

### 5.2 Cantons

La mise en œuvre de certificats pour accéder aux applications de l'administration fédérale est un thème récurrent entre les cantons et l'OFIT. Plusieurs enquêtes effectuées aussi bien par la CSI que par l'USIC révèlent que les besoins en certificats sont très variés. Afin de préparer sa mission, l'équipe en charge de la révision s'est renseignée auprès des cantons de Zurich et d'Argovie à l'aide d'un bref questionnaire pour savoir quel étaient alors les besoins en la matière.

Les hésitations de l'OFIT entre 2001 et 2004 ont fait que le canton de Zurich a développé sa propre infrastructure PKI et que Swisscom était en pourparlers en tant que fournisseur de certificat. Finalement, la balance a penché en faveur de l'infrastructure Admin PKI. Le canton d'Argovie indique avoir d'emblée eu confiance dans ce projet. Pour l'essentiel, ils sont satisfaits de la solution technique, un canton a relevé des lacunes au niveau organisationnel auxquelles l'OFIT est en mesure de remédier.

Indiscutablement, les cantons se sont par le passé montrés résistants concernant l'utilisation de certificats basés sur le matériel. Pour eux et leurs organes associés, de tels certificats représentaient un facteur de coûts important car il fallait mettre en place les processus organisationnels correspondants et acquérir l'infrastructure technique. Inversement, l'OFIT ne pouvait pas toujours fournir les prestations requises dans les délais. Les échanges de courrier attestent de délais de réponse et de livraison inacceptables. Cependant, au fur et à mesure que le projet de portail SSO se concrétisait, le vent a tourné en faveur de l'OFIT. Entre-temps, les critiques se sont faites moins dures et, selon la CSI, les cantons sont aujourd'hui pour la plupart satisfaits de l'offre de l'OFIT. Selon une statistique, à mi-avril 2007, du total des 26 580 certificats de classe B, quelque 24 000 étaient utilisés dans les cantons. Entre-temps plusieurs cantons ont admis que ces certificats pouvaient aussi être utilisés pour leurs propres applications ; des projets allant dans ce sens sont en cours (p. ex. pourparlers entre l'OFIT et le Verwaltungsrechenzentrum AG St-Gall concernant l'utilisation de certificats). Le tout n'entraînera cependant aucune recette supplémentaire pour l'OFIT.

Avec l'introduction d'autorités locales d'enregistrement (LRA) dans les cantons mais également au sein de la Confédération, le processus d'émission des certificats s'est rapproché des clients finaux. Une LRA – 80 fonctionnent actuellement – est un lien important dans tout le système de sécurité d'une PKI. C'est pourquoi, il faut travailler à ce niveau en respectant strictement les directives de l'OFIT. Un audit demandé par l'OFIT et portant en 2005 sur plusieurs LRA a révélé des lacunes. L'OFIT y a remédié et continue depuis de les éliminer, toutefois pas dans leur totalité. Jusqu'à présent, il n'existe aucun règlement stipulant qui à l'avenir devra contrôler les LRA.

Recommandation 5.2 (ordre de priorité: 1)
Etant donné que les LRA sont capitales pour tout le processus de sécurité lié à l'émission de certificats, il faut garantir via des audits menés à intervalles réguliers que ces autorités travaillent conformément aux dispositions prévues. En tant que fournisseur de produits, l'OFIT doit veiller à ce que de tels audits soient menés et à ce que le CI statue sur les dispositions adéquates.

*D'ici la fin de l'année, l'OFIT va mettre en place un concept d'audit pour les LRA puis soumettra au CI une proposition pour les dispositions correspondantes.*

### 5.3 Situation en matière de concurrence

Après la débâcle de Swisskey, il y eut longtemps aucun fournisseur de certificats en Suisse. L'entrée en vigueur de la loi sur la signature électronique (SCSE) a fourni une base définie juridiquement conforme au droit suisse, permettant de trouver une solution conforme aux normes reconnues. Actuellement, le marché en matière de conseils est très vaste en Suisse mais il n'existe que trois fournisseurs reconnus de certificats conformes à la SCSE. Beaucoup d'entreprises de conseil utilisent leurs propres certificats ou ceux de gros fournisseurs étrangers tels que Verisign, Cybertrust, Symantec ou d'autres. Pour les solutions de cyberadministration, les attentes concernant le degré de confiance et la fiabilité (continuité) d'un fabricant de certificats sont importantes. En effet, avec des entreprises étrangères ou non-certifiées SCSE, ces attentes ne sont que partiellement remplies.

Lorsque l'OFIT aura obtenu sa certification par KPMG, il verra s'ouvrir des perspectives très intéressantes. L'OFIT a pu conclure une convention avec La Poste et, via la reconnaissance mutuelle des certificats, tester la mise en œuvre technique afin d'obtenir le courrier électronique recommandé (IncaMail) également pour les collaborateurs de l'administration fédérale. Cet exemple montre qu'il est possible de servir l'administration publique à l'aide de certificats OFIT et les entreprises et les privés via des certificats de La Poste. C'est ainsi qu'il serait possible de réaliser des prestations de cyberadministration orientées vers un large public.

Swisscom et l'entreprise Quo Vadis ne représentent, dans un proche avenir, aucune concurrence dans le domaine de l'administration publique, étant actives sur des marchés plus petits et plus spécifiques. Nous n'avons pas connaissance non plus de produits impliquant de grandes quantités de certificats émis par Swisscom. De même, rien n'indique dans le domaine public une percée d'un produit nécessitant une utilisation étendue de certificats Swisscom sur le marché étroit que

représente la Suisse. Toutefois, une coopération avec l'OFIT, à l'image de celle qui existe avec La Poste, pourrait se révéler une option intéressante pour Swisscom.

Pour La Poste et Swisscom, la rentabilité de l'infrastructure PKI - comme pour l'OFIT – ne semble pas être quantifiable en fonction du prix des différents certificats. L'avantage découle plutôt du potentiel des nouvelles orientations permettant de sécuriser simplement les données et applications d'un grand nombre d'utilisateurs répartis dans différentes organisations. Cela profite avant tout au client, peu importe que les certificats proviennent de La Poste, de Swisscom ou de l'OFIT.

Pour les certificats de moindre qualité ou nécessitant des constellations de systèmes spéciales, les fournisseurs actifs sur le marché international sont et seront toujours en mesure de proposer et de vendre des certificats. Cependant jusqu'à présent, lorsque les exigences de qualité étaient élevées, il n'existait aucune alternative en Suisse. C'est pourquoi les perspectives d'avenir de l'OFIT sont très prometteuses.

### 5.4 Projets en cours

L'infrastructure Admin PKI est un produit de base qui permet d'émettre des certificats. Le projet visant à créer la première infrastructure a été officiellement terminé en 2002, soit intégré dans l'exploitation officielle. Dans les années qui ont suivi, les besoins des clients ont continuellement évolué et se poursuivront dans cette voie. A l'origine axées sur le secure-messaging, les prestations de l'OFIT ont été progressivement élargies et améliorées en fonction des nouvelles connaissances. Chaque extension de l'infrastructure de base initiale a donné ou donne lieu à des projets supplémentaires, décomptés et conduits séparément: mise en place de la PKI de classe 2 (actuelle classe B), introduction de la PKI dans les cantons en relation avec le portail SSO du DFJP, mise en place des classes C et D, élargissement de l'infrastructure à la classe 3 et diffusion de certificats pour le tachygraphe numérique (DFS). Actuellement, un projet spécifique est mené dans chacun des domaines suivants : secure-messaging, certification de la classe A et système de gestion des cartes à puce (Smartcard Management System [SCMS]). Cette liste est loin d'être exhaustive, servant avant tout à démontrer la diversité et la problématique propres au contexte de l'infrastructure Admin PKI.

L'équipe en charge de la révision a consulté tous les documents de projets existants jusqu'à au moment de l'audit, soit les offres, les contrats et les décomptes. Ces documents sont classés avec ordre et les flux financiers ont pu être retracés pour l'essentiel sur la base des contrats et, dès 2006, à partir des extraits comptables SAP. Toutefois, il n'y a pas eu de contrôle de leur intégralité et d'examen des acquisitions réalisées. Le résumé de toutes les factures examinées sert avant tout à évaluer les dépenses consenties jusqu'à présent conformément au chapitre 5.5.

### 5.5 Investissements, budget

Comme cela a été démontré précédemment, l'OFIT a su tirer profit d'une situation de crise pour construire sa propre CA. Ce faisant, il a décidé de conserver une position-clé importante en matière de sécurité au sein de l'administration fédérale et de ne pas la laisser à n'importe quel fournisseur externe. Lorsqu'il s'agit de choisir un fournisseur de certificat approprié, la confiance accordée au sérieux de ce dernier mais également sa présence sur le marché sont essentielles. En fonction des exigences posées au certificat, il faut que le niveau de sécurité soit élevé. Dans ce

cas, va-t-on confier le tout à un fournisseur de prestation interne à la Confédération ou simplement abandonner ce service de sécurité en mains externes? Peu importe maintenant que la décision d'alors de choisir des certificats basés sur le matériel ait été correcte ou pas. L'OFIT a depuis longtemps déjà reconnu que le marché nécessite davantage qu'un unique certificat fixe, basé uniquement sur le matériel.

La décision du DFJP de recourir à des cartes à puce pour le portail SSO a été déterminante. Deux solutions se présentaient : soit réactiver l'infrastructure Admin PKI alors en léthargie, afin de satisfaire aux exigences du DFJP et des cantons, soit rechercher sur le marché un autre fournisseur de certificats. La seconde solution aurait immanquablement conduit à un „grounding" de l'infrastructure Admin PKI, avec l'amortissement de tous les investissements consentis jusque là. Les décisions prises par le Conseil de l'informatique (CI) sont tombées au bon moment et ont joué un rôle prépondérant. Si l'on veut exploiter une infrastructure PKI fonctionnelle, il faut disposer préalablement de la structure de base et du savoir-faire. Il ne faut pas négliger les investissements consentis pour cela. Si l'on souhaitait un retour sur investissement via la vente de certificats, ceux-ci devraient être vendus à un prix n'étant pas à la portée des clients. En comparaison directe avec Swisscom ou La Poste, la politique des prix pratiquée par l'OFIT est dans tous les cas convenable et peut être qualifiée de concurrentielle, voire même d'avantageuse. L'émission et la gestion des certificats devraient cependant assumer en principe leurs coûts. Le seuil de rentabilité de l'exploitation actuelle peut être atteint uniquement en fonction de la quantité de certificats émis, l'OFIT avançant le chiffre de 100 000 à 130 000 certificats. Cette hypothèse est réaliste, dans la mesure où des certificats devront être utilisés comme éléments de sécurité pour d'autres applications de l'administration fédérale.

Sur la base des documents fournis, l'équipe en charge de la révision a établi une liste de toutes les factures. Les totaux qui en ont résulté ont été comparés aux listes du responsable de produit. Pour les années 2001 à 2003, il n'a pas été possible de reconstituer totalement les coûts en se référant au système SAP. En revanche, pour les années 2004 et 2005, il y a plutôt concordance compte tenu des délimitations exactes. Depuis l'exercice 2003, les comptabilisations sont devenues plus précises, c'est-à-dire que non seulement les coûts externes mais également les coûts internes proportionnels de l'OFIT ont été imputés à l'infrastructure Admin PKI. Dès 2005, les coûts comptabilisés et ventilés ont été examinés et évalués par le responsable de produit si bien qu'ils sont maintenant un peu plus précis.

La liste établie par le CDF montre pour les années 2001 à 2005 des coûts externes totaux (versements aux fournisseurs et prestataires de service) de 5 millions de francs. Ce montant inclut non seulement les coûts de l'exploitation courante, y compris la maintenance et les licences mais également tous les coûts des projets lancés dans le cadre de l'émission de certificats : p. ex. extension de l'infrastructure pour la classe 2 (classe B actuelle), classes C et D, mise en place de l'enregistrement pour les cantons, etc. En supposant (sur la base des évaluations faites par les anciens et actuels responsables de projet) qu'un poste de travail comptabilisé à coût complet pour chaque collaborateur de l'infrastructure PKI - deux en 2001 et 2002, quatre en 2003 et 2004, six en 2005 et 2006 - représente en moyenne 200 000 francs par collaborateur et par année, les coûts internes se montent jusqu'à présent à 4,8 millions de francs.

Les recettes dégagées de 2001 à 2005 sont si peu transparentes et explicites que l'équipe en charge de la révision n'a pas été en mesure de les analyser. Il ne sera possible d'établir véritablement une facturation globale qu'à partir de 2007. Les valeurs correspondantes planifiées conformément aux principes du NMC prévoient des dépenses liées à l'exploitation de l'infrastructure Admin PKI de l'ordre de 3,65 millions de francs, pour des recettes probables, incluant les moyens transversaux, de l'ordre de 2,8 millions (dont 700 000 francs de recettes ayant des incidences sur les finances). La perte budgétée est donc de 850 000 francs. Ce faisant, les projets en cours, de l'ordre de 1 million ne sont pas pris en compte. Les dépenses et recettes estimées pour les années 2008 à 2011 montrent des „gains" croissants dès 2009, pour autant que l'on puisse émettre davantage de certificats comme supposé et que les coûts évoluent dans la marge fixée. Pour l'instant, une analyse de ces chiffres est très difficile ; cependant l'équipe en charge de la révision estime qu'il y a de bonnes chances de les réaliser.

Pour les raisons énumérées, il n'est pas possible de calculer la rentabilité de manière correcte. Les avantages d'une infrastructure PKI découlent indirectement d'une sécurisation simplifiée des applications. Les économies potentielles profitent avant tout aux partenaires intervenant dans le processus de cyberadministration. Cependant, une collaboration active avec La Poste contribuera à renforcer les synergies potentielles qu'il s'agit de dégager. Compte tenu des expériences faites jusqu'à présent, il faut admettre que les investissements consentis de l'ordre de 12 millions de francs ne pourront pas dans l'immédiat être récupérés et devraient être considérés comme des coûts initiaux à amortir. Les directives en matière de comptabilité devraient également tenir compte de ces éléments ou plus exactement des délimitations entre les investissements nécessaires et l'exploitation propre, celle-ci devant répondre à des critères économiques. Conformément aux principes en vigueur pour calculer les prix imputés, les prestations fournies à l'interne dans l'administration ne peuvent se faire que sur la base des coûts complets planifiés, c'est-à-dire sans tenir compte des parts aux bénéfices et aux risques. Cette politique n'est concevable pour les investissements présentés et les moyens transversaux mis en œuvre chaque année que si l'on répercute les coûts en dehors de l'administration fédérale, p. ex. avec les cantons. Il n'est possible de couvrir intégralement les coûts que lorsque le produit peut être financé sans moyens transversaux supplémentaires. Dans ces calculs, les investissements consentis ne sons pas encore pris en compte, ni récupérés.

En fin de compte, l'équipe en charge de la révision constate que le développement de l'infrastructure Admin PKI et l'émission de certificats sont à la base d'une affaire qu'il n'est pas possible d'abandonner du jour au lendemain. Il faudrait au moins prendre des dispositions en matière de succession pour les certificats valables déjà utilisés, avec de possibles conséquences financières pour l'OFIT.

Recommandation 5.5 (ordre de priorité: 2)
En définissant les prix pour les différents certificats, il faut veiller à ce que la compensation des coûts complets n'intervienne que lorsqu'il n'y aura plus aucun flux de moyens transversaux. Il faudrait donc examiner dans quelle mesure des prix plus élevés pourraient être imputés aux clients extérieurs à l'administration afin d'arriver rapidement à une couverture totale des coûts.

*L'OFIT examinera la répartition des coûts et la structure des prix et discutera avec l'AFF de l'imputation de prix plus élevés pour les services fournis à l'extérieur de la Confédération.*

### 5.6 SCSE

En date du 27 juin 2005, le CI a autorisé l'OFIT à proposer des certificats de classe A au sein de l'administration fédérale. Simultanément, il a été décidé que cette prestation ne devait pas être financée par des moyens transversaux, contrairement aux classes B à D, mais que ces certificats devaient être refacturés de manière conséquente selon les coûts complets engendrés. Au vu de cette situation, l'OFIT a obtenu le feu vert pour introduire une certification selon les principes énoncés dans la SCSE. Lors d'un audit préliminaire qui a eu lieu à l'automne 2005, KPMG, seule société de certification accréditée en Suisse, a d'abord défini dans quelle mesure l'OFIT satisferait à une certification. Suite à ces résultats, mandat a été donné le 31 mai 2006 de procéder à l'audit de certification. Entre août 2006 et février 2007, KPMG a vérifié à l'OFIT les processus de mise en place et de déroulement ainsi que l'infrastructure logique du fournisseur de services de certification (CSP). Le rapport d'audit a été rendu au début du mois d'avril 2007.

L'audit a montré que les processus et l'infrastructure ne répondaient pas encore dans tous les domaines aux exigences de sécurité très élevées définies par le législateur. Toutefois, il n'a été relevé aucune lacune impossible à supprimer dans le délai imparti par la société KPMG. Il est donc probable que l'OFIT obtienne la certification souhaitée durant le deuxième trimestre de 2007. La certification n'a pas pour objectif initial la vente de certificats de classe A. En réalité, le marché est encore très restreint actuellement, les besoins au sein de l'administration fédérale ne sont pas encore concrets et le secteur privé réagit également avec circonspection.

La reconnaissance officielle de l'OFIT en tant que CSP doit dans un premier temps contribuer à établir la confiance, étant donné que l'évaluation se fait selon des bases légales et des normes sévères. Pour comprendre cet objectif, il faut savoir que les processus et infrastructures vérifiés par KPMG sont identiques à ceux qui servent à émettre tous les autres certificats. La plus-value qui en résulte de manière générale pour l'OFIT en tant que fournisseur et émetteur de certificats, devrait donc se répercuter sur la quantité des certificats vendus et améliorer de manière générale la situation financière. Le calcul des coûts et avantages effectué pour le projet de SCSE arrive à des conclusions similaires. A l'exception d'un faible montant résultant de la vente de certificats de classe A, les „recettes", sous forme d'avantage quantifiable, s'élèveront probablement à 450 000 francs par année. Par rapport à cette valeur théorique, les coûts d'exploitation et les intérêts se montent chaque année à quelque 230 000 francs. De la sorte, le retour sur investissement (ROI) devrait être atteint dans un délai de 5 ans. L'équipe en charge de la révision estime que les extrapolations de l'OFIT sont en principe réalistes mais ne s'inscrivent pas dans une optique de rentabilité. La certification a essentiellement une visée stratégique et politique dont il faut mieux tenir compte dans l'appréciation.

La décision du CI voulant que le financement des certificats de classe A se fasse sans moyens transversaux, un projet indépendant „Anerkennung Admin PKI Class A" a été mené jusqu'à la certification, affichant des coûts externes de 1,1 million de francs.

Dans les prochains budgets, il s'agira de continuer à présenter de manière séparée les coûts et recettes correspondant au scénario présenté; ils ne devront pas apparaître dans le budget global à la rubrique „PKI-Kosten_Ertrag" ni être compensés via les comptes de l'infrastructure Admin PKI. Afin de satisfaire à la décision du CI, il faudra être en mesure de présenter n'importe quand de manière transparente les coûts et recettes.

Recommandation 5.6 (ordre de priorité: 1)
Tous les coûts et recettes (coûts d'exploitation, investissements, audit de contrôle, recettes dégagées par la vente, etc.) liés aux certificats de classe A, doivent être budgétés et décomptés séparément. L'OFIT doit impérativement satisfaire aux principes énoncés dans la décision du CI du 27 juin 2005, en vertu desquels il ne doit y avoir aucune interférence avec les classes B à D (moyens transversaux).

*L'OFIT présentera chaque année les coûts et recettes liés aux certificats de classe A de manière séparée. Etant donné que dans la pratique, les classes A et B se partagent les mêmes infrastructures et processus d'exploitation (à l'instar de ce qui se passe également chez les autres CSP), la présentation se basera impérativement sur des modèles de calcul.*

## 6 Perspectives et appréciation

Ces dernières années, l'OFIT a réussi à développer aussi bien l'infrastructure que le savoir-faire permettant de répondre aux besoins des clients en certificats de différentes qualités couvrant des aspects de sécurité spécifiques aux applications. En déployant quelque 25 000 certificats pour les utilisateurs du portail SSO en 2006, l'OFIT a prouvé qu'il était en mesure de fabriquer dans les délais de grandes quantités de certificats fonctionnels. Via sa certification en tant que CSP par KPMG, l'OFIT atteste par ailleurs de la qualité et de la sécurité de l'infrastructure et des processus mis en œuvre pour émettre des certificats de classe A répondant aux dispositions de la SCSE. Vraisemblablement, l'OFIT sera le quatrième fournisseur sur le marché suisse à proposer ce type de certificats. Etant donné que pour toutes les classes de certificat l'OFIT utilise les mêmes infrastructures et processus que pour la classe A, les administrations publiques disposent dorénavant de moyens pour réaliser des solutions de cyberadministration à un niveau très élevé de sécurité.

Avec la reconnaissance fournie par KPMG, une condition essentielle a été remplie, à savoir que l'OFIT est un fournisseur de certificat digne de foi et de confiance sur le marché étroit que représente la Suisse. Cette prestation peut devenir une tâche fédérale importante. Les exigences élevées seront chaque année contrôlées par KPMG si bien que l'on peut augurer d'un label de qualité uniforme. La certification de l'OFIT doit être aussi jugée de qualité vu que plus de 40 000 certificats, dont 65% de classe B sont déjà fonctionnels. Certes, La Poste et Swisscom sont certifiées depuis plus longtemps mais n'ont proposé leurs produits qu'une fois leur certification obtenue. Ils ne disposent donc pas encore des expériences pratiques liées à des déploiements d'envergure. Par ailleurs, l'OFIT a conclu une convention de roaming avec La Poste dans le domaine IncaMail, distribution de plis électroniques recommandés, ce qui conduira également à un potentiel de synergies dans le secteur privé.

Il faut tabler sur des quantités importantes si l'on entend vendre des certificats en appliquant des critères de rentabilité. Les certificats des classes B à D sont un facteur de réussite décisif. Pour l'heure, il paraît plutôt improbable que la classe A, conforme à la SCSE, puisse être gérée de manière à assumer ses coûts. Le Code des obligations ne prévoit que dans de très rares cas une signature manuscrite qualifiée pour les affaires juridiques et celles-ci ne devraient à l'avenir aussi que rarement se dérouler électroniquement. La certification par KPMG doit donc être considérée avant tout comme un label de qualité non seulement pour l'émission de certificats mais également pour l'OFIT en tant que tel, l'essentiel étant alors la confiance des clients dans les processus et l'exploitation technique. L'OFIT peut tirer profit de cette chance afin de mieux sécuriser de manière simple un grand potentiel d'applications à travers les possibilités offertes par les certificats.