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.