

Audit du projet informatique clé: Interception System Schweiz ISS 2

L'essentiel en bref

Conformément aux directives du Conseil fédéral concernant les projets informatiques clés, le Contrôle fédéral des finances (CDF) a effectué durant la période allant d'avril à juin 2014 l'audit du projet Interception System Schweiz (ISS 2) auprès du Centre de services informatiques du Département fédéral de justice et police (CSI-DFJP). Le CDF était chargé d'examiner l'état d'avancement du projet et les risques susceptibles de compromettre l'atteinte des objectifs.

Le système de surveillance des télécommunications utilisé actuellement ne permet plus au Service de surveillance de la correspondance par poste et télécommunication (service SCPT) d'exécuter son mandat légal. Sur ordre des ministères publics et après autorisation des tribunaux compétents, ce service accomplit des tâches de surveillance des télécommunications visant à élucider des infractions graves ou à retrouver des personnes disparues. Pour ce faire, le CSI-DFJP exploite le système LIS (*Lawful Interception System*), qui lui permet de récupérer des données auprès des fournisseurs de services de télécommunication et de mettre ces informations à la disposition des autorités de poursuite pénale. Le système LIS étant arrivé au terme de son cycle de vie, son remplacement est inévitable. Le projet Interception System Schweiz (ISS 1) avait été lancé à cet effet en 2008.

Dans le cadre de l'art. 3 de la loi fédérale sur les marchés publics (LMP), une procédure invitant à soumissionner avait permis de sélectionner un fournisseur pour ISS 1. En 2013, le projet avait été interrompu pour des raisons diverses. Rebaptisé ISS 2, le projet a pris un nouveau départ avec une société sœur d'un autre fabricant issu de la même procédure. Le présent rapport concerne le projet actuel ISS 2.

Malgré la nécessité de certaines mesures, le projet ISS 2 est sur la bonne voie. Les risques liés aux délais et aux coûts sont correctement examinés en vue du lancement prévu pour mars 2015. Le concept de sûreté de l'information et de protection des données (concept SIPD) n'a pas encore été validé. Le déroulement du projet pâtirait de l'ajout de nouvelles exigences et des adaptations qui s'avéreraient nécessaires.

L'organisation du projet répond aux attentes. L'étendue du projet est clairement définie et l'organisation adéquate. Les principales parties prenantes ont été associées aux travaux par l'intermédiaire du comité de projet, dirigé par le secrétaire général du DFJP en tant que mandant.

L'architecture de solution exige des mesures d'accompagnement en vue de la mise en œuvre et de l'exploitation. Comme le prévoyait le mandat de projet, le système de base défini n'a pas été conçu de manière redondante. Il satisfait aux exigences minimales qui permettent de remplir l'actuel mandat légal. La quantité de données que le système et les réseaux traitant les informations entrantes et sortantes devront gérer est difficile à déterminer. En effet, la téléphonie traditionnelle laisse peu à peu place à celle passant par Internet (*Voice over IP*) ainsi qu'à d'autres services fournis sur le Web, créant ainsi de plus en plus de contenus multimédias. L'évolution du nombre de surveillances est elle aussi difficile à prévoir. Il ne serait pas rentable de donner dès à présent une ampleur trop importante à l'ISS 2. C'est pourquoi le projet suit une approche différente. Pour compenser les éventuels pics au niveau de l'entrée des données et réduire les conséquences négatives de l'absence de redondance, un système tampon, qui doit encore être élaboré, devra

compléter le système de base. Cependant, le concept correspondant n'est pas encore achevé. Il n'a en outre pas encore été décidé si le système sera développé au sein de l'administration fédérale ou mis au concours. Selon le CDF, le projet ne tient pas suffisamment compte de la priorité du système tampon.

Les incertitudes mentionnées quant à l'ampleur du système de base regardent également le système tampon, qui est seulement à même de les lever partiellement. Le développement des capacités concerne toujours la totalité des composants d'une chaîne de transformation. C'est pourquoi le CDF recommande au DFJP de contrôler régulièrement le calcul des capacités dès le lancement, et ce, au moyen des quantités effectives de données entrantes, et de préparer d'ores et déjà un éventuel développement du système.

En raison de l'absence de redondance dans le système de base, la gestion de la continuité joue un rôle central. Le service SCPT élabore actuellement les projets nécessaires dans le domaine de la gestion de la continuité des affaires (Business Continuity Management, BCM). La gestion de la continuité des services informatiques prévoit aujourd'hui une transformation du système d'intégration en système productif en cas de catastrophe, mais cela n'a pas encore été concrétisé. Selon le CDF, des plans d'urgence détaillés ainsi que divers scénarios devront être disponibles avant le lancement.

Certaines exigences en matière de sécurité restent à concevoir. Les besoins de protection sont établis et les exigences en matière de sécurité définies. Cependant, le concept SIPD a pris du retard. Par conséquent, son élaboration doit bénéficier d'une priorité majeure. En outre, le concept d'autorisations doit être mis en œuvre avant le lancement de l'ISS 2.

Texte original en allemand