

La France veut une certification pour la sécurité du Cloud

« L'approche consistant à contractualiser au cas par cas la sécurité dans chaque projet de mise en nuage montre ses limites », explique l'Anssi. D'où la volonté de l'Agence nationale de la sécurité des systèmes d'information de mettre au point un **référentiel permettant d'auditer et de certifier la sécurité** des prestataires de Cloud. Un référentiel qui a vocation à servir dans un premier temps les besoins de l'Etat, mais que pourront ré-exploiter les entreprises.

C'est ce document d'une quarantaine de pages que l'Anssi vient de publier [sur son site](#), en appelant les internautes à le commenter. Ces derniers ont **jusqu'au 3 novembre pour transmettre leurs remarques**, suite à quoi l'Anssi prévoit de procéder à une phase expérimentale « *permettant de tester en conditions réelles l'applicabilité de ce référentiel* ». L'agence invite les prestataires candidats à cette expérimentation à la contacter. Et précise que le futur référentiel a **vocation à converger avec le label « Secure Cloud »**, créé dans le cadre du [volet Cloud du plan de la Nouvelle France Industrielle](#), porté par Arnaud Montebourg.

Stockage et traitement en France

Au sein de 14 chapitres, le référentiel de l'Anssi répertorie les exigences et recommandations que les prestataires de Cloud (Saas, IaaS et PaaS) devront respecter pour être qualifiés. Et propose **deux niveaux de sécurité** : le premier, dit élémentaire, est conforme aux impératifs propres à la politique de sécurité des systèmes d'information de l'Etat (PSSIE), tandis que le second, dit standard, permet d'assurer le traitement des données de niveau diffusion restreinte (le niveau le plus faible en matière d'information classifiée). Le référentiel prévoit notamment que le stockage et le traitement des données doivent être effectués sur le territoire. Le prestataire doit également proposer un support de premier niveau francophone et installé dans l'Hexagone, revoir au moins une fois par an sa politique de gestion des identités et de contrôle des accès ou encore revalider, à la même fréquence, les droits d'accès des utilisateurs. Cette revalidation est même trimestrielle pour les comptes à privilèges élevés, selon la version du référentiel actuellement disponible. De même, l'Anssi prévoit **une généralisation du chiffrement** (flux et stockage des données), y compris au niveau élémentaire.

La sortie de ce référentiel en version définitive pourrait **ouvrir la porte à une utilisation du Cloud public par l'Etat**, utilisation pour l'heure proscrite mais qui pourrait avoir un rôle dans le plan d'économies que doit mettre en œuvre Jacques Marzin (économiser 25 à 40 % sur les dépenses externes, soit sur une enveloppe de 2 milliards par an). Fin mai dernier, [dans nos colonnes](#), le directeur de la Disic (Direction interministérielle des systèmes d'information et de communication) expliquait : « *Nous examinons avec nos collègues de l'ANSSI si cette certification est de nature à réviser notre politique consistant pour l'heure à proscrire tout recours au Cloud public, pour des raisons de sécurité. Avoir cette option pourrait s'avérer intéressant, pour du débordement, la montée en charge de projets ou comme solution transitoire, afin de libérer de l'espace dans les datacenters en déplaçant dans le Cloud des applications peu critiques* ».

A lire aussi :

[Pilotage des SI de l'Etat : Jacques Marzin et la Disic prennent la main](#)