SecNumCloud

Jean-Pierre Lacombe, Fidens
Étienne Aynès, Fidens
Rémi Grivel, SynAApS

Clusir Rhône-Alpes Club, le 10 mai 2017

Sommaire

- La genèse
- Objectifs de qualification des offres en nuage
- Une approche collégiale amendée
- Le référentiel
  - ✓ Niveaux
  - ✓ Qualification
  - ✓ Exigences
- Faisabilité et impact
- Les « beta certifiés »
- Le point de vue d'un fournisseur : SynAAps
- Questions ?

La genèse (2013)

Le contexte « Référentiel Général de Sécurité »

- Instaurer la confiance dans les échanges au sein de l'administration
  - ✓ Une méthodologie
  - ✓ Des règles et bonnes pratiques
  - ✓ La qualification de produits de sécurité et de prestataires
    - o PASSI (audit)
    - o PSCE (certification électronique), PSHE (horodatage), PSCO
    - o Formations
    - o Offre en nuage

Objectifs de qualification des offres en nuage

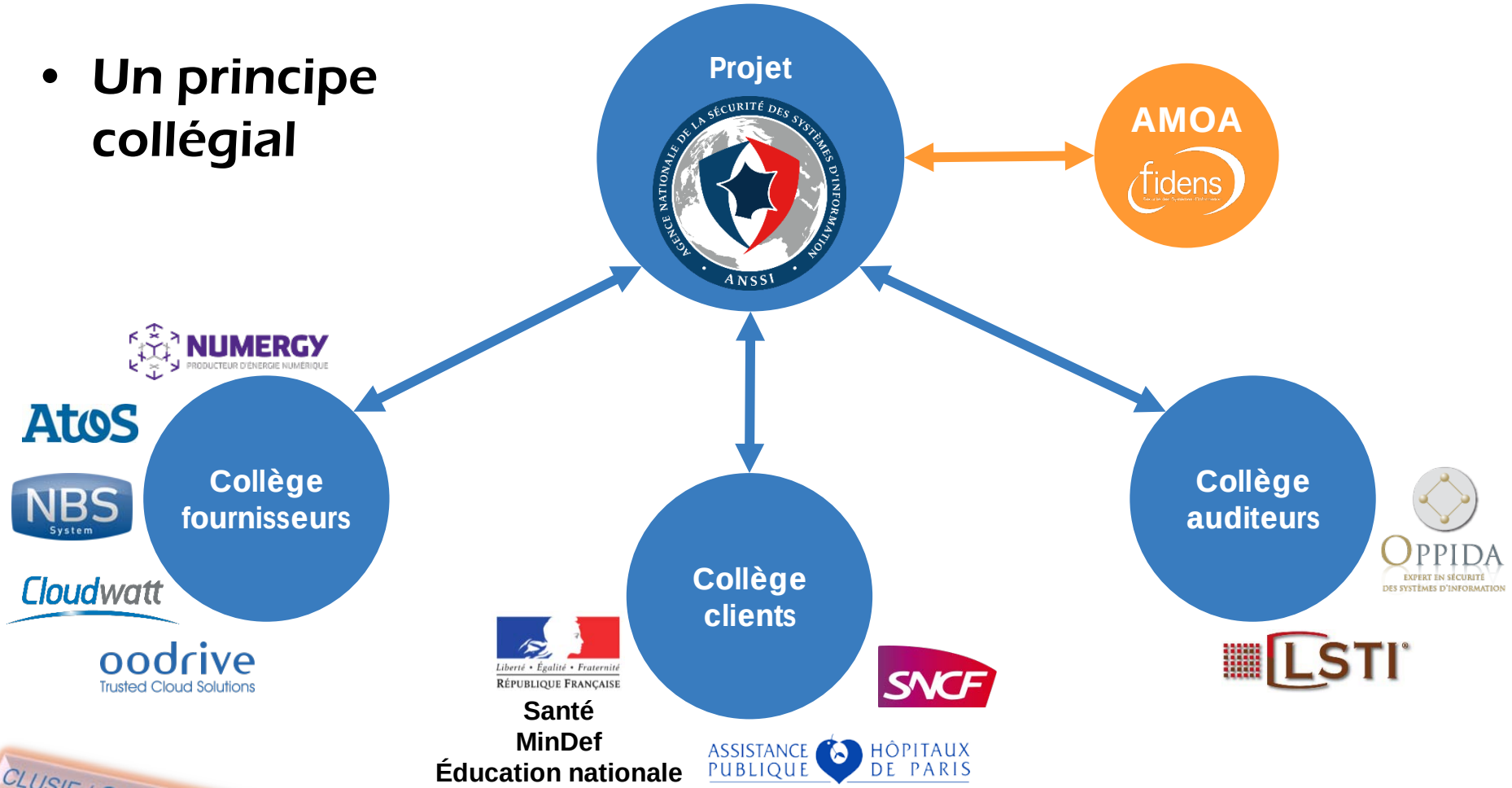
Des prestataires qualifiés : pourquoi ?

- Un constat : des relations parfois difficiles entre demandes et offres
  - ✓ Des offres packagées pas forcément négociables
  - ✓ Des expressions de besoins parfois mal exprimées
  - ✓ Des volontés de reporting, de contrôle et d'audit souvent peu réalistes sur le plan opérationnel
  - ✓ Des arguments commerciaux difficiles à apprécier

- Un souhait : faire émerger des offres génériques sécurisées conformes aux attentes des clients

Une approche collégiale amendée, ou les limites de la démocratie participative

- Un principe collégial



Une approche collégiale amendée, ou les limites de la démocratie participative

- Deux groupes de travail

- Un document largement revu par les instances, fond et forme

Une approche collégiale amendée

- Document soumis à commentaires
- Beta qualification avec des prestataires volontaires
- Sortie du référentiel avec les exigences pour le niveau « Essentiel »

Le référentiel et la qualification

- Une logique unique, avec deux niveaux de qualification

ESSENTIEL
Stockage et traitement de données pour lesquelles un incident de sécurité aurait une conséquence limitée pour le client

AVANCÉ
Stockage et traitement de données pour lesquelles un incident de sécurité aurait une conséquence importante pour le client

- Initialement basée sur les besoins en DICP, cette approche est de formulation plus simple, mais très ambiguë : la compta de mon plombier, c'est avancé ?! Se souvenir des représentants clients… Plus trop de place pour les petites gens

Le référentiel et la qualification

- Une logique de qualification type ISO 27K
  - ✓ Qui pourrait être basée sur une certification 27K préalable
  - ✓ Mais des exigences de sécurité obligatoires…
- Pour rappel :
  - ✓ ISO 27K :
    - o L'entité est propriétaire de ses risques, et libre de sa stratégie si elle est cohérente et conforme à la réglementation
    - o Notions de plan d'actions et d'amélioration
  - ✓ SecNumCloud : les exigences du référentiel sont en place nativement et contrôlables par l'organisme en charge de la qualification
- Un élargissement en cours des entités agréées pour la qualification

Le référentiel et la qualification

- Les limites : SecNumCloud n'affranchit pas des obligations réglementaires ou contextuelles :
  - ✓ Agrément santé : HDS
  - ✓ Conformité politique sécurité de l'État : PSSIE

- Mais on peut agréer en delta, si l'organisme veut bien avaliser le travail précédemment réalisé

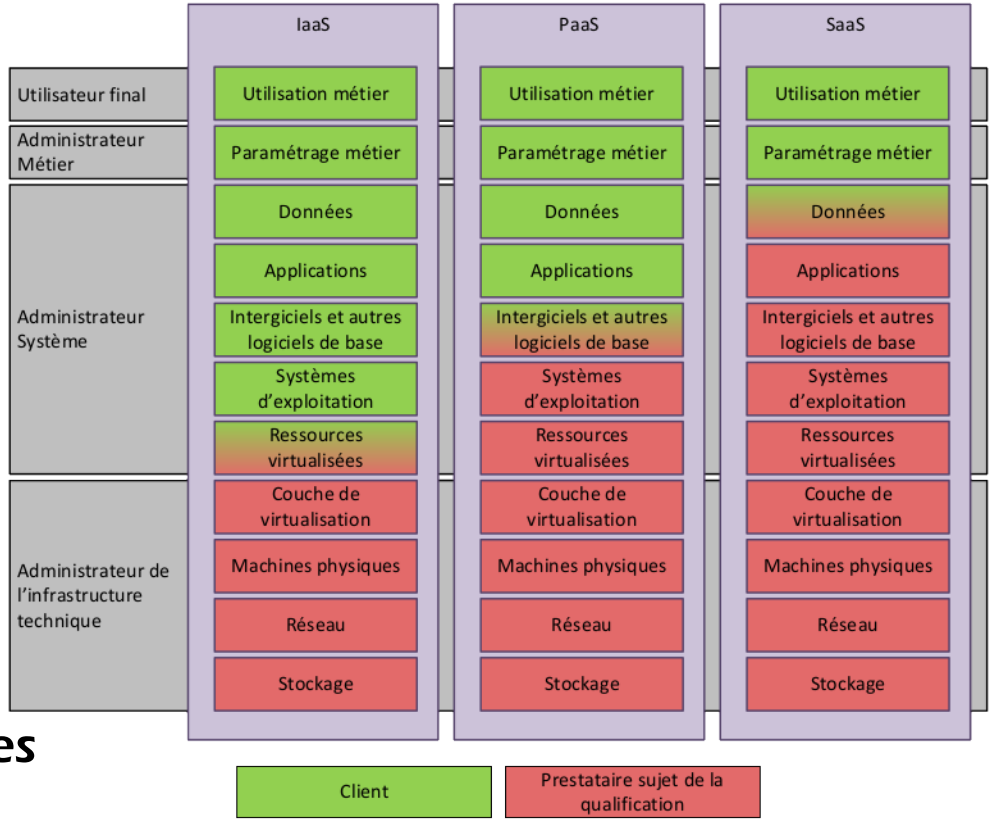
- L'idée est celle d'une qualification complémentaire, et non supplémentaire

Le référentiel

- Appuyé sur des travaux ayant fait l'objet d'un large consensus :
  - ✓ ISO 27002, 27017, 27018
  - ✓ Guide CSA (Cloud Security Alliance)
  - ✓ Travaux du NIST, de la Commission européenne…
- Présentation largement adossée sur 27002

Le référentiel, niveau essentiel

- Activités visées par le référentiel et limites de responsabilités
  - ✓ Qui fait quoi dans les différentes offres
  - ✓ Des exigences à nuancer selon les offres
    - o Sauvegardes
    - o Administration système
    - o Gestion des composantes sécurité et réseau
    - o ...



Répartition des responsabilités par type de service

Le référentiel, niveau essentiel

- Politique de sécurité (27K1 compliant)
- Gestion du risque (27K1 compliant)
  - ✓ Des orientations dans l'analyse
  - ✓ Approbation de la direction
  - ✓ Révision annuelle
- Organisation (27K1 compliant)
  - ✓ Communication vis-à-vis des clients sur les projets impactant
- Ressources humaines (27K1 compliant)

Le référentiel, niveau essentiel

- Gestion des actifs
  - ✓ Besoins de sécurité inhérents aux données clients
  - ✓ Recommandation seulement pour le marquage et la manipulation
- Contrôle d'accès et gestion des identités
  - ✓ Exigences renforcées (nominatif sauf exception, gestion des comptes clients le cas échéant, double authentification, interfaces distinctes, cloisonnement « approprié » entre clients…)
- Cryptologie
  - ✓ Exigences renforcées (chiffrement de données en cas de réallocation, supports de sauvegarde externalisés, méthode de chiffrement, signature, hachage, clés…)

Le référentiel, niveau essentiel

- Sécurité physique
  - ✓ Zones privées contrôlées (admin)
- Exploitation
  - ✓ Journalisation sur 6 mois minimum
  - ✓ À la demande tout événement concernant un client
  - ✓ Infrastructure de gestion et corrélation des logs
  - ✓ Machines d'administration durcies
- Communication
  - ✓ Cloisonnement (sensibilité, nature des flux, domaine…)
  - ✓ Sondes de détection

Le référentiel, niveau essentiel

- Acquisition, développement
  - ✓ Procédure de développement sécurisée, tests
- Relation avec les tiers
  - ✓ Contractualisation, contrôles
- Gestion des incidents
  - ✓ Classique
- Continuité
  - ✓ PCA, tests
- Conformité
  - ✓ Audits annuels PASSI, configuration, tests, code

Le référentiel, niveau essentiel

- Exigences supplémentaires par rapport à 27002
  - ✓ Convention de service avec le client (autorisant l'ANSSI à conduire des audits)
  - ✓ Stockage et traitement en Europe, support autorisé en dehors mais documenté ; support de premier niveau en français
  - ✓ Effacement sécurisé de toutes les données en fin de contrat
  - ✓ Suppression des données techniques en fin de contrat

Faisabilité et impact

- Et des mesures retenues en général dans 27002 non obligatoires dans SecNumCloud :
  - ✓ Relations appropriées avec autorités compétentes ou groupes de spécialistes (recommandation)
  - ✓ Procédures de marquage de l'information et procédures de traitement des actifs (recommandation)
  - ✓ Procédure de mise au rebut des supports
  - ✓ Protection des supports pendant le transport
  - ✓ Surveillance et ajustement au plus près de l'utilisation des ressources ; projections sur les dimensionnements futurs
  - ✓ Exigences en matière de sécurité et de continuité du management de la sécurité dans les situations défavorables

Les « beta certifiés »

Orange Cloud

Synchronisation et partage de documents, sauvegarde de données…

Niveau de qualification visé :
ESSENTIEL

Oodrive

Partage de fichiers et travail collaboratif

Niveau de qualification visé :
AVANCÉ

Vendôme Solutions

Hébergement et gestion de centre de données

Niveau de qualification visé :
AVANCÉ

Des questions ?