CLUB DE LA SECURITE DE L'INFORMATION FRANCAIS

CLUSIF

Atouts et limites du RGS

Sébastien Herniote

Responsable du pôle conseil en cybersécurité

MOSSYS

I ♥ RGS

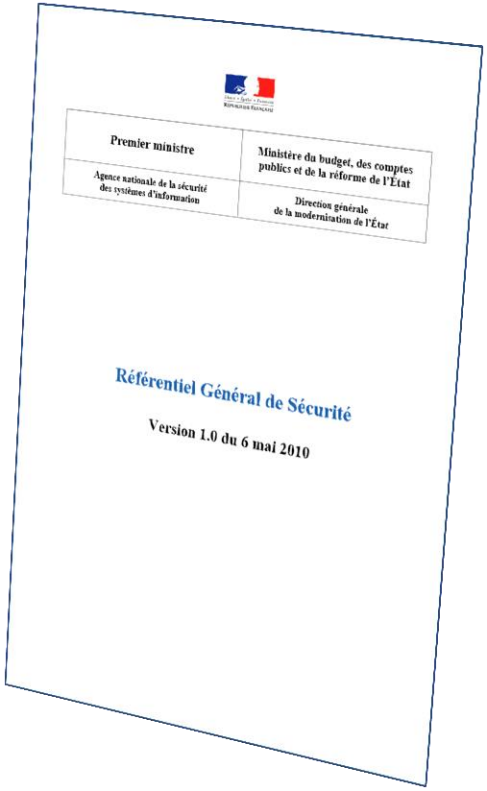
Place du RGS dans le paysage des *textes SSI*

- 4 objectifs stratégiques
- Sept axes d'effort

Février 2011

- Tout organisme (public et privé)
- 40 règles d'approche *holistique*

Janvier 2013



- Autorités administratives
- Centré *échanges électroniques*

Mai 2010

Tordons le cou à quelques idées reçues sur le RGS

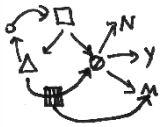
Appliquer le RGS me coûterait trop cher

Coût d'un SI mal ou non sécurisé ?

Règles alignées avec l'état de l'art

Rien d'orthogonal avec ISO 27K, guides CNIL, etc.

Etoiles, PRIS, SHA-x : c'est jargonneux et ne parle que de PKI

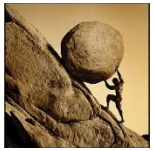


Le RGS, au final, en 2 notions :

Homologation de sécurité des SI

Confiance dans produits et prestataires

Le RGS, j'ai pas eu le courage de le lire : 1000 pages, non merci



30 pages pour les acteurs SSI des AA

800 pages pour les autorités de certification

100 pages pour les spécialistes crypto et les éditeurs

Le RGS est un texte de loi*

S'impose à ceux qui y sont soumis
Plus « puissant » qu'un simple recueil de bonnes pratiques

Vise large : les autorités administratives
Ministères, directions centrales, générales, collectivités locales, EPCA, organismes assurant un service public, CH, universités, etc.

Vise indirectement encore plus large
Editeurs et prestataires désireux d'adresser ce marché et proposer des produits et offres qualifiées

Centré sur les échanges électroniques
Protection des téléservices, pas des SI dans leur globalité
3 fonctions de sécurité déclinées « façon PRIS »
Petit sous-ensemble des thématiques ISO 27002

Pas de liste précise des autorités administratives
Tentation de ne pas être une « autorité administrative »
Des organismes qui ne savent aujourd'hui toujours pas

Le recours à des produits et prestataires qualifiés n'est pas imposé **

* *Ordonnance n° 2005-1516 du 8 décembre 2005*
Décret n° 2010-112 du 2 février 2010
Arrêté du 6 mai 2010 portant approbation du RGS v1

** *Les produits de sécurité et les prestataires de services de confiance peuvent obtenir une qualification […]*
L'autorité administrative recourt à des produits et à des prestataires ayant fait l'objet d'une qualification ou à tout autre produit ou prestataire […]

Le RGS prône l'homologation de sécurité

Approche par les risques pour la mise en place du juste niveau de sécurité

Analyse des risques > choix des mesures > audits > Homologation (risques résiduels) > Suivi dans le temps

Responsabilisation des Métiers / MOA

La sécurisation d'un SI n'est ni un sujet accessoire ni la seule affaire de spécialistes

Prise en compte de la sécurité dans les différentes phases projet

Démarche reconnue

En phase avec ISO 27001

Ancrée dans le monde du classifiée de défense (cf. IGI 1300)

Pas de guide thématique sur le sujet

Les acteurs sécurité peuvent parfois manquer de repères. Pièces du dossier de sécurité ? Profondeur d'analyse ? Comment sécuriser le parc d'applications existantes ?

Pas de précision sur la variabilité de la démarche

Homologation simplifiée / standard / complète ?

Cf. directive N° 27/DEF/DGSIC du 24 janvier 2013

Les projets ne se font pas tous « en V »

Méthodes agiles, « sprints », etc.

Besoin de mettre à jour le guide de l'ANSSI sur l'intégration de la sécurité dans les projets

La qualification des prestataires de services

Un schéma de qualification solide

Adossé à un texte réglementaire, Acteurs légitimes (ANSSI, COFRAC, organismes de qualification)
Référentiels de qualification partagés, discutés et reconnus

La faculté de rajouter des « familles » de prestataires qualifiables

PASSI en v2
Prestataires d'investigation numérique, de Cloud Computing, de cyberdéfense en v3

Une aide précieuse au choix par les autorités administratives

Inclusion dans les appels d'offre.
Effet boule de neige et capilarisation au secteur privé

Buzz parfois négatif autour de la famille des autorités de certification

Famille de prestataire qualifiable dans le RGS v1
Trop de monde croit que le RGS = certificats électroniques
Crispations sur SHA, double usage, …

L'audit de qualification des AC est de type conformité : pas d'audit technique (TI …)

*DigiNotar était conforme à la norme ETSI TS 101456 (équivalent au RGS ***) !*

Familles qu'il serait intéressant de qualifier

Prestataires intervenant en amont : accompagnement AR, homologation PSSI, SDSSI, etc.
Cf. initiative CESG

La qualification des produits de sécurité

Schéma solide

Adossé à un texte réglementaire, Acteurs légitimes (ANSSI, COFRAC, CESTI)
Critères d'éval. reconnus : CC, CSPN, annexes B du RGS

Surcouche à la certification

Tout produit qualifié répond à un besoin de l'administration
Cryptographie nécessairement étudiée

Gage de confiance pour les produits qualifiés

Cf. actualité : rapport Bockel, leak Snowden, etc.

Une facilité pour les AA

Réclamer des produits qualifiés dans les appels d'offre

Faible nombre de produits qualifiés

Limites du schéma

Qualification est valable pour une version donnée, à un instant donné, avec contraintes d'emploi précises
Pas assez de « mise sous maintenance »
Ne porte QUE sur la robustesse des fonctions de sécurité du produit : pas sur les autres critères intéressants les DSI (exploitabilité, performances, prix, etc.)

En synthèse

Positionnement stratégique du RGS lié à son caractère réglementaire

Faculté de le mettre à jour et de l'enrichir à loisir

Lien vers les guides thématiques / techniques de l'ANSSI nouvellement produits

L'homologation de sécurité est consacrée et la confiance est diffusée via la qualification

Assise réglementaire qui bride

Echanges électroniques

Pas assez régulièrement mis à jour

Entre l'ordonnance de déc. 2005 et aujourd'hui : 8 ans … pour une seule version du RGS publiée officiellement

Les concepts de cyberdéfense ne sont pas évoqués

surveillance > détection > réaction

Stratégie concernant l'emploi de produits qualifiés ?