Le RGS pour une prise en compte de la sécurité par tous

Ministère de l'intérieur

Service du HFD / Fonctionnaire SSI

R. Marichez

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE DE L'INTÉRIEUR
SECRÉTARIAT GÉNÉRAL

1. Transposition interne du RGS
   - Homologation ?
   - Les briques de confiance
   - L'ouverture aux partenaires
2. Complexité vs. compréhensibilité
   - « Autorité administrative » ?
   - Stratégie en faveur de produits ou services « qualifiés »
   - Temporalité et gouvernance
3. RGS facteur de cybersécurité nationale ?
   - RGS vs. vulnérabilités : risque d'une conformité « cache-misère »
   - Accompagnement des usagers de l'administration
   - Le « niveau de sécurité » guidé par la contrainte de moyens
   - L'implication des décideurs…. Contraints et forcés ?
   - Foisonnement des téléservices

Préambule

Référentiel général de sécurité v1.0

- Ordonnance (8 décembre 2005) ratifiée (12 mai 2009)
- Décret (2 février 2010)
- Arrêté (6 mai 2010, publié JORF 18 mai 2010)
- Document visé par arrêté, avec ses annexes

- Objectifs :
  - Faire appliquer la réglementation, rien que la réglementation, toute la réglementation
  - Faire augmenter, dans la durée, le niveau de sécurité global du ministère

Transposition interne du RGS

1. Homologation

- FSSI :

  - Transposition interne de la réglementation interministérielle

  - Evaluation hyper-macro du risque, et recommandations

  - PSSI-MI pour organiser et faire porter le risque par des AQSSI

  - Contrôle de son application :
    Les exigences réglementaires doivent être respectées
    L'analyse du risque ne doit pas être manifestement erronée

Transposition interne du RGS

1. Homologation

- Téléservices? :
  - « Démarche ou formalité administrative »
  - Par voie électronique
- Article 5 du décret de 2010 « atteste formellement »
- Démarche :
  - Demande auprès des directions
  - Très peu de retours
- Autre approche :
  S'intégrer dans les projets

Transposition interne du RGS

1. Homologation

- « Démarche d'Intégration de la SSI dans les Projets » (« DISSIP »)

- Conçue pour respecter *a minima* le principe de l'homologation RGS et annoncée comme telle
- Méthode simple et présentée comme très simple
  - ➔ Trois niveaux de « besoins SSI du projet »
  - ➔ Démarrage systématique par une note d'orientation
    - Note « conséquences » (enjeux, impacts métier…)
    - Note « sensibilité » (besoin DICT)
    - Note « exposition » (source de menace)
    - Note « vulnérabilité » (hétérogénéité du SI, ouverture, variabilité…)
    - Somme des 4 notes

Transposition interne du RGS

1. Homologation

- « Démarche d'Intégration de la SSI dans les Projets » (« DISSIP »)

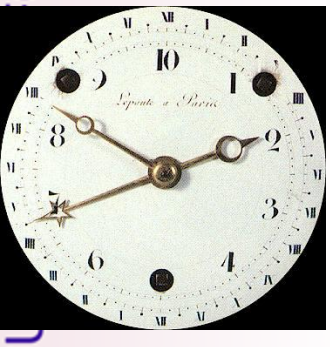
Niveau de maturité « pertinent »	Livrables principaux
[0]	aucun
[1]	Liste des meilleures pratiques SSI négociées (établie par le directeur de projet et négociée avec l'autorité d'homologation)
[2]	Dossier d'exigences de sécurité (DES) comprenant un inventaire des risques et des mesures de sécurité applicables, et une estimation de l'impact de ces solutions techniques.
[3]	FEROS et TDBSSI

- Point de passage obligé de la démarche projet
  - ➔ Convaincre la gouvernance des SI (DSI)
  - ➔ Former les chefs de projets DSI
  - ➔ Accompagner la mise en œuvre de la démarche
  - ➔ Contrôler que les projets les plus « sensibles » (« méta-analyse du risque ») sont couverts

Transposition interne du RGS

1. Homologation

- Influer sur le projet. Ne pas s'opposer :
  L'absence d'homologation ne pourra jamais empêcher la mise en service du SI



- Faire désigner une autorité d'homologation (AH)
  ➔ J - 6 à 9 mois

- Réunir les membres de la commission d'homologation (associer les représentants métiers)
  ➔ Suivi mensuel ou bimestriel : audits, risques…

- Anticiper le rapport de forces AH / chefferie de projet
  ➔ Influer sur le projet avant le point de non-retour

Transposition interne du RGS

1. Homologation

- Pièges difficiles à éviter :
  - Cahiers des charges fixant le niveau de sécurité trop tôt (absence d'étude de risque amont…)
  - Désignation d'une AH trop liée au maître d'œuvre, ou trop tardive

- Facteurs de succès :
  - Trouver un allié au sein de la maîtrise d'ouvrage ou des propriétaires de l'information
  - « Utiliser » le rapport de forces naturel MOA/MOE
  - Systèmes utilisés par plusieurs entités (interministériels)
  - Savoir piloter une sous-traitance de projet (pénalités…)

- Après l'homologation, suivi dans le temps de la SSI :
  - soit par une succession d' « homologations provisoires » (dévoiement du concept de l'attestation de sécurité)
  - soit par un comité de suivi SSI (de type SMSI)

  généralement tous les 6 mois environ

Transposition interne du RGS

2. Les briques de confiance

- Article 4 du décret de 2010
  « … fonctions ainsi déterminées … »
  « … recourt à des *produits de sécurité* et à des *prestataires de services de confiance* [PSCo] ayant fait l'objet d'une *qualification* (…) ou *à tout autre produit ou prestataire pour lesquels elle s'est assurée de la conformité de leurs fonctions de sécurité au [RGS]* »

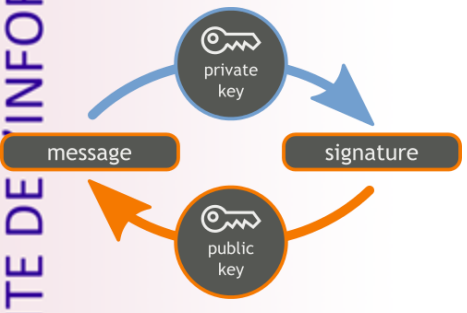
- Principe :
  Risques
  ➔ Fonction(s) de sécurité d'un niveau dépendant des risques
  ➔ Conformité des fonctions à l'annexe du RGS correspondante

- Danger de sur-investissement dans la sécurité d'une fonction et d'omission de l'environnement autour de la fonction de sécurité

Transposition interne du RGS

2. Les briques de confiance

- Mise en place d'une Infrastructure de gestion de clé (IGC)
  Conforme au RGS niveau 2 étoiles
  Fonctions :



Authentification (« identification »)
Chiffrement (« confidentialité »)
Signature électronique (au sens du code civil français)
Horodatage

Prestataire (même interne) de services de confiance (« offre d'IGC »)

➔ IGC personnes (avec carte à puce / carte professionnelle)

➔ IGC serveurs

Transposition interne du RGS

2. Les briques de confiance

- Produits de confiance éligibles au RGS (« qualification ») :
  Infrastructures tranverses de sécurité :
  - tous les outils de protection des clés privées utilisées dans les IGC
  - pare-feux
  - portails d'authentification SSO
  - outils de chiffrement (fichiers, mails, flux, volumes…)
  - outils de signature (création, validation…)
  - *etc*

- Infrastructure DNS ? (« minint.fr »…)

- Recours non systématique à des produits qualifiés :
  Qualifiés, si demandé par le RGS
  Qualifiés, lorsque cela est possible et pertinent
  Quelconque, sinon

Transposition interne du RGS

3. L'ouverture aux partenaires

- Inter-opérabilité des briques de confiance
  Gabarits des certificats…
  ➔ référencement ?
  ➔ compatibilité à l'international ?
  Gestion des cartes à puce (standard IAS-ECC)
  ➔ implémentation du standard ?

- Convergence des SI d'infrastructure reposant sur les IGC
  ➔ Authentification SSO
  ➔ Outils de chiffrement / de signature

- Délimitations des responsabilités
  Cas « machine-machine » fréquent au sein de l'administration
  Cas d'un tiers intermédiaire
  ➔ Deux homologations : engagement réciproque de sécurité

Transposition interne du RGS

Conclusion

- L'homologation RGS, démarche subjective fondée sur la sensibilité de certains au risque, permet de :
  - influer positivement sur la sécurité d'un projet
  - sensibiliser les directions et les partenaires aux enjeux de sécurité

- Le recours à un socle de confiance :
  - mutualisation des efforts
  - une certaine garantie de sécurité évaluée objectivement, apportée par les briques de confiance

- Dans un système utilisé par plusieurs acteurs :
  - Une autorité s'engage « moralement » auprès des « clients »

- Mais l'homologation ne permet pas de :
  - « rattraper » un projet dont le niveau de sécurité est « bloqué »
  ➔ difficulté à anticiper dans un contrat de sous-traitance les charges des mesures de sécurité non encore identifiées

1. Transposition interne du RGS
   - Homologation ?
   - Les briques de confiance
   - L'ouverture aux partenaires
2. Complexité vs. compréhensibilité
   - « Autorité administrative » ?
   - Stratégie en faveur de produits ou services « qualifiés »
   - Temporalité et gouvernance
3. RGS facteur de cybersécurité nationale ?
   - RGS vs. vulnérabilités : risque d'une conformité « cache-misère »
   - Accompagnement des usagers de l'administration
   - Le « niveau de sécurité » guidé par la contrainte de moyens
   - L'implication des décideurs…. Contraints et forcés ?
   - Foisonnement des téléservices

Complexité *vs.* compréhensibilité

1. « Autorité administrative » ?

- Le contour de l'autorité administrative au sein de l'Etat : pas de réponse tranchée

  Pistes de réponses :

➔ l'Etat, une personne morale
➔ quel en est son représentant ?
➔ le ministre, membre du Gouvernement, ayant autorité sur un département ministériel
➔ le Préfet de département, représentant de l'Etat, dans son ensemble, au sein du département

- Eligibilité d'un système d'information au RGS ?

- Identifier le porteur du risque juridique ?

Complexité *vs.* compréhensibilité

2. Stratégie en faveur de produits ou services « qualifiés »

- Vocabulaire :

  Qualification de produit de sécurité, de PSCo
  ➔ décret du 2 février 2010 (RGS) : **attestation** qu'un produit ou qu'un service offert par un PSCo est conforme à un **niveau de sécurité** du RGS
  « Signal » du niveau de sécurité d'un produit commercialisé
  Apporter de la confiance par une démarche objective et transparente => rendre efficace le marché

  Homologation de système d'information (attestation unilatérale)
  ➔ document RGS v1.0, §3.2
  Certification de la sécurité offerte par les produits ou services
  ➔ décret du 18 avril 2002
  Habilitation, accréditation…

Complexité *vs.* compréhensibilité

2. Stratégie en faveur de produits ou services « qualifiés »

- Objectif : éviter les prestataires peu scrupuleux
- Sécurité des IGC : contrôler les conditions d'exploitation (penser à Diginotar…) et le paramétrage (penser à la PKI Microsoft...)

- ➔ **besoin d'un schéma de qualification des offreurs de service**

- Qualification de fonctions de sécurité offertes par un PSCo
  Abus de langage :
  - « certificat qualifié »
  - « IGC qualifiée » (RGS §6.2)

- Contre-sens :
  Qualification de PSC**E** pour l'émission de **certificats électroniques qualifiés** : décret du 30 mars 2001 sur la signature électronique
  - procédure différente de la qualification de PSC**o**
  - (presque) aucun lien avec la qualification RGS des offres d'IGC

  Cf RGS v1.0, §3.3.2 (fin)

Complexité *vs.* compréhensibilité

2. Stratégie en faveur de produits ou services « qualifiés »

- La qualification d'une offre de PSCo ne traite pas que du certificat :
  - conditions sur la protection et les emplois de la clé privée
  - conditions sur la disponibilité (LRC), les PCA/PRA, l'auditabilité…

- Conditions générales de vente des certificats :
  Le client devrait aussi respecter le RGS en ce qui le concerne

Complexité *vs.* compréhensibilité

2. Stratégie en faveur de produits ou services « qualifiés »

- Qualification de produit ou de service :
  « Signal » à destination du marché

  obligation ou recommandation ?

  Article 4 du décret de 2010
  « … recourt à des *produits de sécurité* et à des *prestataires de services de confiance* [PSCo] ayant fait l'objet d'une *qualification* (…) ou *à tout autre produit ou prestataire pour lesquels* ***elle s'est assurée*** *de la conformité de leurs fonctions de sécurité au [RGS]* »

Complexité *vs.* compréhensibilité

2. Stratégie en faveur de produits ou services « qualifiés »

- Limites actuelles de la qualification de sécurité d'un produit :

  - Intégration, exploitabilité et qualité au sein d'un SI
    ➔ référencement *vs.* qualification

  - Assurance sur le produit effectivement commercialisé, dans les conditions où il sera effectivement utilisé (-> hypothèses)

  - Faiblesse de l'offre concurrentielle et concentration :
    Pare-feux : 2 fournisseurs
    Chiffreurs IP : 5 fournisseurs
    Outils de chiffrement sur le poste de travail : 3 fournisseurs
    Boîtiers HSM : 1 fournisseur

  - Avantage concurrentiel des « insiders »

  - Garanties quant à un suivi de la qualification dans la durée

Complexité *vs.* compréhensibilité

3. Temporalité et gouvernance

- Facteur temps IGC / cycle de vie
  Projet IGC avec déploiement : classiquement sur 3 ans
  Recours à la sous-traitance (annuaire, enrôlement…)
  Recours à des produits qualifiés à l'instant *t*

- Paysage réglementaire évolutif et riche
  - Supra-national (Europe, marché intérieur, Trusted-lists)
  - Commercial/Privé (CA/Browser Forum…)
  - Réglementations nationales voisines (informatique et libertés…)

- Transition PRIS inachevée

- Evolution de la cryptanalyse

Complexité *vs.* compréhensibilité

3. Temporalité et gouvernance

- Une transition PRIS encore inachevée
  Milliers de certificats « usagers » en circulation
  Continuité du téléservice…
  Projet de communication / lobbying et pas uniquement technique

- Découvertes de la cryptanalyse
  Les découvertes sont impossibles à anticiper
  … et si SHA256/SHA512 étaient demain « cassés » ?
  Exemple de SHA1 : toutes les IGC n'ont pas encore évolué

Complexité *vs.* compréhensibilité

Conclusion

- **Le RGS est une opération de communication**
  Mais un référentiel maîtrisé par des spécialistes…

- Difficultés d'intégrations dans l'environnement :
  - Réglementation sur la signature électronique (code civil)
  - Réglementation communautaire (Union européenne)
  - Intérêts privés des éditeurs d'OS / de navigateurs web

- Adhérence à des SI particulièrement complexes
  - Faire évolutivité des IGC
  - Dilemme de l' « attestation de conformité à un niveau de sécurité » d'un produit nécessairement évolutif au sein d'un SI

1. Transposition interne du RGS
   - Homologation ?
   - Les briques de confiance
   - L'ouverture aux partenaires
2. Complexité vs. compréhensibilité
   - « Autorité administrative » ?
   - Stratégie en faveur de produits ou services « qualifiés »
   - Temporalité et gouvernance
3. RGS facteur de cybersécurité nationale ?
   - RGS vs. vulnérabilités : risque d'une conformité « cache-misère »
   - Accompagnement des usagers de l'administration
   - Le « niveau de sécurité » guidé par la contrainte de moyens
   - L'implication des décideurs…. Contraints et forcés ?
   - Foisonnement des téléservices

RGS : facteur de cybersécurité nationale

1. Le RGS face aux vulnérabilités des SI

- Surenchérissement d'une (certaine) sécurité par des maîtrises d'œuvre

  ➔ exagération du recours à la cryptographie (signature/chiffrement applicatif (XML) sur un flux HTTPS (RGS) entre deux datacenters reliés par un VPN/IPSec…)

  ➔ exagération du temps passé à l'analyse du risque

- Oubli des règles d'hygiène (mises à jour du socle applicatif web, sécurité sur les terminaux…)

- ➔ risque d'une impression de sécurité par la conformité

RGS : facteur de cybersécurité nationale

2. L'accompagnement des usagers de l'administration

- Le RGS, pour apporter de la confiance aux utilisateurs des SI
  ➔ Besoin d'une meilleure lisibilité des téléservices :
  - Quelles hypothèses (recommandations) sur les postes de travail ?
  - Quel type de certificat ? Où les trouver, à quel prix ?
  ➔ Informations sur certains sites de téléservices
  ➔ Informations sur chaque site de PSCo…

- Exemple du certificat authentification serveur 2 étoiles :
  - PSCo « A » : 80 / 160 / 220 (euros HT 1 an / 2 ans / 3 ans)
  - PSCo « B » : 120 / 240 / 252
  - PSCo « C » : x / 180 / 255

  Certificat authentification serveur 1 étoile : 50 / 80 / 105 …
  Tarifs selon volume / clients / devis / corps de métiers…
  A rapprocher du **TCO annuel du poste de travail**

- Accompagnement des transitions de la réglementation…

RGS : facteur de cybersécurité nationale

3. Le « Niveau de sécurité » guidé par la contrainte des moyens

- Cinématique projet
  Cas 1 : certificats internes
  ➔ en fonction des infrastructures existantes
  Cas 2 : certificats des usagers
  ➔ tenir compte du coût d'acquisition par usager, des moyens existants (support physique)

- Logique d'analyse du risque ???

- Evaluation réelle et objective du « juste » niveau de sécurité ?

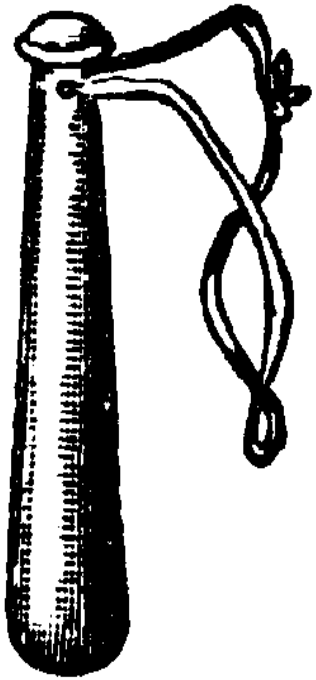
RGS : facteur de cybersécurité nationale

4. L'implication des décideurs… contraints et forcés ?

- Les directeurs de projet :
  - Volonté politique de mener un projet à bien
  - Ne peut refuser à l'usager l'accès au téléservice parce que son navigateur / son OS / sa JRE n'est pas à jour
  - L'agitation de la menace « RGS », sans sanctions

  Dans quel but ?

  ➔ « Raccrocher » la SSI au projet
  Avec un pouvoir faible, dans un rôle d'accompagnement



- Tiers à l'autorité d'homologation (utilisateurs, partenaires administratifs, syndicats professionnels…) :
  ➔ Souvent difficiles à convaincre
  ➔ CGU : pis-aller inefficace, en l'absence d'audit

RGS : facteur de cybersécurité nationale

5. Foisonnement des téléservices

- Simplification des démarches administratives
- Utilisation des moyens de communication modernes (nomadisme, internet haut débit…)
- Mutualisation interministérielle des fonctions support (compatibilité, paie, infrastructures de télécommunication…)

- Enjeu primordial : obtenir l'adhésion des usagers
  - ➔ Accessibilité des téléservices
  - ➔ Inter-opérabilité
  - ➔ Stabilité pour apporter de la confiance

RGS : facteur de cybersécurité nationale

Conclusion : **« Oui » à condition d'être bien utilisé :**

- Acculturation des administrations à la sécurité
- Faire participer les RSSI, les faire connaître
  ➔ besoin de RSSI adhérant aux projets, pas s'y opposant
- Lisibilité et stabilité pour l'efficience du marché et la confiance
- Consolidation, urbanisation des services, pour l'efficience de moyens
- Eviter le zèle (analyses du risque, cryptographie…) : certains projets peuvent en mourir
- Système *de fait* incomplet :
  ➔ ne remplace pas le « bon vieux test d'intrusion »
  ➔ pas de garantie totale du niveau de sécurité (complexité et évolutivité des SI) --> démarche d'homologation subjective
  ➔ bien gérer les partenaires et faire monter ensemble le niveau de sécurité, à force de patience et de persuasion

Merci de votre attention

Origine des images utilisées :
- ministère de l'intérieur
- projet wikimedia commons