

**Club 27001 – 11 juin 2009**

# **Présentation du RGS**

**Emeric Laroche**

[<Emeric.Laroche@hsc.fr>](mailto:Emeric.Laroche@hsc.fr)

- Présentation du RGS
- Intégrer le RGS dans une démarche ISO 27001

- Ordonnance 2005-1516
  - Pouvoir accéder à des services de l'administration par voie électronique
  - Échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives
  - Respecter des règles de sécurité → RGS
  - Respecter des règles d'interopérabilité → RGI

- Rédigé par la Direction Centrale de la Sécurité des Systèmes d'Information (DCSSI)
  - Contribuer à la définition interministérielle et à l'expression de la politique gouvernementale en matière de sécurité des systèmes d'information
  - Assurer la fonction d'autorité nationale de régulation pour la SSI en délivrant les agréments, cautions ou certificats pour les systèmes d'information de l'État, les procédés et les produits cryptologiques employés par l'administration et les services publics, et en contrôlant les centres d'évaluation de la sécurité des technologies de l'information (CESTI)
  - Évaluer les menaces pesant sur les systèmes d'information, donner l'alerte, développer les capacités à les contrer et à les prévenir (CERTA)
  - Assister les services publics en matière de SSI
  - Développer l'expertise scientifique et technique dans le domaine de la SSI, au bénéfice de l'administration et des services publics
  - Former et sensibiliser à la SSI

<http://www.ssi.gouv.fr>

- DCSSI
  - Sous l'autorité du Secrétaire Général de la Défense Nationale (SGDN)
  - Prochainement nommée : Agence Nationale pour la Sécurité des Systèmes d'Information (ANSSI)
  - Responsable du contrôle de son application

- « Fixe les règles que doivent respecter les fonctions des systèmes d'information contribuant à la sécurité des informations échangées par voie électronique »  
(ordonnance 2005-1516 Art 9)
- Présente les bonnes pratiques et la démarche pour sécuriser au mieux les SI

- 33 pages
  - Contexte : objectif / périmètre (p 5 à 9)
  - Sécurité organisationnelle (p 10 à 13)
  - Sécurité technique (p14 à 19 et 24 – 25)
  - Qualification et référencement (p 20 à 23 et 26)
  - Annexes (27 à 33)
- 
- Les chapitres intéressants pour chaque profils susceptible d'utiliser le RGS sont identifiés (ex: RSSI chapitres 2, 3 et 4)

- Autorités Administratives (AA)
  - « Les administrations de l'Etat, les collectivités territoriales, les établissements publics à caractère administratif, les organismes gérant des régimes de protection sociale relevant du code de la sécurité sociale et du code rural ou mentionnés aux articles L. 223-16 et L. 351-21 du code du travail et les autres organismes chargés de la gestion d'un service public administratif. Autrement dit, le périmètre de l'[Ordonnance] concerne tous les services publics administratifs de l'Etat. »
- Prestataires mettant en œuvre un système d'information pour une AA
- Editeurs de produits de sécurité pouvant être utilisés par les AA
- Prestataires de Service de Confiance (PSCo)

- Adopter une démarche globale (RGS 1.2.1)
  - Prendre en compte les aspects techniques et non-techniques
  - Considérer toutes les origines de risque (humaine, naturelle, accidentelle, délibérée)
  - Avoir une vision stratégique de la sécurité
  - Responsabiliser les acteurs
  - Intégrer la SSI tout au long du cycle de vie des SI

- Adapter la SSI selon les enjeux (RGS 2.2.2)
  - Consacrer les moyens financiers et humains juste nécessaires et suffisants
  - Utiliser le guide « Maturité SSI »
    - Définir la stratégie
    - Gérer les risques
    - Gérer les règles de sécurité
    - Superviser la sécurité
    - Concevoir les mesures
    - Réaliser les mesures
    - Exploiter les mesures
      - Amélioration continue que si besoin très important de sécurité ?

<http://www.ssi.gouv.fr/fr/confiance/documents/methodes/maturitessi-methode-2007-11-02.pdf>

# Partie organisationnelle : 6 principes

- Gérer les risques SSI <sup>(RGS 2.2.3)</sup>
  - Utiliser l'ISO 27005
  - Avec les outils EBIOS
- Elaborer une politique SSI <sup>(RGS 2.2.4)</sup>
  - Au plus haut niveau hiérarchique de l'AA
    - A décliner pour chaque entité
  - Utiliser le guide PSSI
    - <http://www.ssi.gouv.fr/confiance/pssi.html>
- Utiliser des produits et prestataires labellisés SSI <sup>(RGS 2.2.5)</sup>
  - Outil ou service qualifié par la DCSSI
  - Prise en compte d'autre certifications (ISO 27001 par exemple)

# Partie organisationnelle : 6 principes

- Viser une amélioration continue <sup>(RGS 2.2.6)</sup>
  - Mettre en œuvre un SMSI tel que défini dans l'ISO 27001

- Homologuer la sécurité des nouveaux systèmes
  - Moyen pour intégrer la sécurité dans les projets
  - Constitution du dossier d'homologation grâce au GISSIP
  - L'autorité d'homologation atteste que
    - les exigences de sécurité sont déterminées et satisfaites
    - les risques résiduels sont acceptés et maîtrisés
  - Sa composition n'est pas précisée
    - Le RSSI peut intervenir en tant que conseil pour cette autorité
    - Le RSSI y présente l'analyse des risques

- La décision d'homologation est :
  - émise par l'autorité d'homologation
  - publique pour les téléservices
  - fournie à la DCSSI sur demande
  - Réévaluée tout au long du cycle de vie du système d'information
- En cas de responsabilités partagées, l'homologation est collégiale ou déléguée à une des AA

- FEROS type
  - Fiche d'Expression Rationnelle des Objectifs de Sécurité
  - Exprimer les besoins en sécurité
- Guide d'exigences types
  - Catalogue de fonctions (mesures) de sécurité à mettre en œuvre pour atteindre les objectifs

[http://www.references.modernisation.gouv.fr/sites/default/files/Exigences\\_Types-%20ExigencesV1\\_0.pdf](http://www.references.modernisation.gouv.fr/sites/default/files/Exigences_Types-%20ExigencesV1_0.pdf)

- Ce qui est obligatoire
  - Faire une appréciation des risques
  - Fixer les objectifs de sécurité
  - Identifier les fonctions de sécurité à mettre en œuvre
  - Utiliser des produits qualifiés « à chaque fois que possible »
  - Homologuer les systèmes d'informations

- Exigences sur certaines fonctions/mesures de sécurité
- Authentification
  - Utilisation de la cryptographie ? → document RGS\_B\_1
  - Utilisation de clés cryptographiques ? → document RGS\_B\_2
  - RGS\_B\_1 : « Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques »
  - RGS\_B\_2 : « Règles et recommandations concernant la gestion des clés utilisées dans des mécanismes cryptographiques »
  - Documents antérieurs au RGS

- Authentication
  - Mot de passe → recommandé de n'être utilisé que pour déverrouiller un mécanisme cryptographique
    - Dans ce cas, voire les préconisations du CERTA
- Authentication, signature électronique, confidentialité
  - Certificats doivent respecter les politiques de certification types
    - 3 niveaux de sécurité de la PrisV2.1

Acronyme	Titre du document	Nom complet du document	Version du document
[RGS A 1]	Service de Confiance "Confidentialité"	RGS Service Confidentialite V2.2.pdf	2.2
[RGS A 2]	Service de Confiance "Authentication"	RGS Service Authentication V2.2.pdf	2.2
[RGS A 3]	Service de Confiance "Signature"	RGS Service Signature V2.2.pdf	2.2
[RGS_A_4]	Service de Confiance "Certificat Serveur"	RGS_Service_Authentification_Serveur_V2.2.pdf	2.2
[RGS A 5]	Service de Confiance "Cachet Serveur"	RGS Service Cachet Serveur V2.2.pdf	2.2
[RGS A 6]	Politique de Certification Type "Confidentialité"	RGS PC-Type Confidentialite V2.2.pdf	2.2
[RGS A 7]	Politique de Certification Type "Authentication"	RGS PC-Type Authentication V2.2.pdf	2.2
[RGS A 8]	Politique de Certification Type "Signature"	RGS PC-Type Signature V2.2.pdf	2.2
[RGS_A_9]	Politique de Certification Type "Certificat Serveur"	RGS_PC-Type Authentication Serveur V2.2.pdf	2.2
[RGS A 10]	Politique de Certification Type "Cachet Serveur"	RGS PC-Type Cachet Serveur V2.2.pdf	2.2
[RGS_A_11]	Politique de Certification Type "Authentication et Signature"	RGS_PC-Type Authentication Signature V2.2.pdf	2.2

- Pour les mécanismes cryptographiques
  - Documents RGS\_B\_1 et RGS\_B\_2
- Respecter la politique d'horodatage type

- « Toute demande, déclaration ou production de documents adressée par un usager à une autorité administrative par voie électronique ainsi que tout paiement opéré dans le cadre d'un téléservice fait l'objet d'un accusé de réception électronique » (Ordonnance Art 5.I)
- Si date limite de remise d'information ou demande par l'usager
  - horodatage et signature de l'accusé de réception

# Qualification d'un produit de sécurité

- « Acte par lequel la DCSSI atteste de la capacité d'un produit à assurer, avec un niveau de robustesse donné, les services de sécurité objet de la qualification. »
- « L'attestation de qualification indique le cas échéant l'aptitude du produit à participer à la réalisation, à un niveau de sécurité donné, d'une ou plusieurs fonctions traitées dans le RGS. »
- 3 niveaux de qualification:
  - Élémentaire (Certificat de Sécurité de Premier Niveau : CSPN)
    - Evaluation dans un temps et une charge contrainte
  - Standard : Critères Commun EAL 3 + divers paquets d'assurances
  - Renforcé : Critère Commun EAL 4 + divers paquets d'assurances

- Passage par un organisme accrédité et homologué
  - Accréditation : respect des exigences d'impartialité, de responsabilité et de confidentialité (évalué par le COFRAC ou équivalent européen)
  - Homologation : compétence technique à conduire l'évaluation de fonctions de sécurité (évaluée par la DCSSI)
  - Un représentant du SGDN et un représentant DCSSI au comité de qualification

- Infrastructure de Gestion des Clés
  - Rédiger une politique de certification
  - Respecter les règles précédentes pour les certificats serveurs et de personne
- Infrastructure de Gestion des Clés Administration
  - Certificats racine pour les certificats utilisés par les AA
  - Publiés au JO pour intégration par les éditeurs de logiciels...
    - ... et vérification par les utilisateurs

- Utiliser un produit ou service de sécurité par les utilisateurs
  - Conformité technique avec les installations du ministère
  - Respect des règles pour la mise en place du service
- Ex : Référencement pour l'émission de certificat de personne
  - Mise en œuvre des CRL
  - Reconnaissance par les applications visées

- Processus communs
  - Appréciation des risques
    - Faire accepter le risque résiduel par les responsables (homologation / acceptation par la direction du risque résiduel)
  - Revues régulières de la sécurité par les responsables
  - Prise en compte de la sécurité de manière globale (technique/organisation/physique/humain...)
  - Mise à disposition des ressources
  - Mise en place de mesures sélectionnées dans un référentiel

- Points divergents
  - Tous les points précédents sont **obligatoires** dans l'ISO 27001
  - Points supplémentaires de l'ISO 27001
    - Audits internes (ISO 27001 Chapitre 6)
    - Amélioration continue systématique (ISO 27001 Chapitre 8)
    - Gestion de la documentation (ISO 27001 Chapitre 4.3)

- Points divergents
  - Points supplémentaires du RGS
    - Fixer des objectifs de sécurité (DécretRGS art 3.b)
    - Utiliser du matériel qualifié (DécretRGS art 4)
    - Obtenir une homologation **par système d'information** avant mise en production (DécretRGS art 3)
    - Respecter les exigences des politiques de certification type (RGS Chapitres 3.2, 3.3 et 3.4)
    - Respecter les règles pour le dimensionnement des mécanismes cryptographiques (RGS Chapitres 3.2, 3.3 et 3.4)
    - Respecter les règles sur la gestion des clés utilisées dans les mécanismes cryptographique (RGS Chapitres 3.2, 3.3 et 3.4)

- Base intéressante
  - Impose une appréciation des risques
  - Impose l'utilisation de matériel qualifié
- Problèmes
  - Périmètre d'application flou
    - Téléservices ?
    - Tous les systèmes d'information ?
    - Echanges avec les partenaires ?
  - Non-obligation d'amélioration
  - Homologation déclarative
  - Composition de l'autorité d'homologation non précisée
    - Experts ?
    - Influencé par la politique ?

- Problèmes
  - Gestion des compétences (former et sensibiliser) (ISO 27001) vs Responsabiliser les utilisateurs (RGS)
  - Évocation de l'ISO 27005 & EBIOS
  - Utilisation d'outils lourds (EBIOS, GISSIP, guide PSSI)
  - Techniquement
    - Mot de passe uniquement utilisé pour déverrouiller un mécanisme cryptographique ?
  - Processus d'évolution du RGS lent
    - Retard sur la technique (exemple : impôts)

Merci

Questions ?