



Démarche de mise en conformité RGS d'un téléservice

Retour d'expérience

Giles Carré

11/12/2013

- Retour sur une démarche de mise en conformité RGS (Référentiel Général de Sécurité)
 - Travaux en cours
 - Homologation à venir
- Présentation succincte des fondements du RGS
 - Accent sur les difficultés (compréhension et application des spécificités du RGS)

- Le 18/05/2010, publication au JO de l'arrêté « RGS »
 - officialisation du corps du RGS
 - top départ des délais de mise en œuvre
- À partir du 19/05/2013, tout téléservice existant ou à venir devrait être homologué

- Donner confiance à l'usager → Développer la dématérialisation

- Décret RGS, article 5

AA → EPA, EPST, etc.

- « L'Autorité Administrative

homologation

- atteste formellement

- auprès des utilisateurs de son système d'information

- que celui-ci est protégé conformément aux objectifs de sécurité fixés en application de l'article 3.

DIC

- Dans le cas d'un téléservice,

notion d'échange

- cette attestation est rendue accessible aux usagers [...] »

affichage

usagers :

- étudiants
- extérieurs
- personnels

gestion
des
risques

- Gestion des risques
 - mise en évidence des règles et recommandations spécifiques au RGS
 - pas de méthode imposée
- Homologation : autorisation de mise en exploitation
 - proposée par une commission d'homologation sur la base d'un dossier de sécurité
 - mesures mises en œuvre pour éliminer ou réduire les risques
 - risques résiduels
 - prononcée par l'AQSSI ou son délégué → acceptation des risques résiduels
 - homologation pour 3 à 5 ans
 - ou homologation provisoire sous conditions
 - (ou refus)
- Publication de la décision d'homologation

Organisme	Téléservice	Attestation d'homologation	Autorité de certification	
			Qualifiée	Non qualifiée
CNIL	www.plaintes.cnil.fr	oui	Certinomis (*)	
Minefi	impots.gouv.fr	oui		GeoTrust
L'Assurance Maladie	assure.ameli.fr	non trouvée homologué ?		Thawte
CAF	www.caf.fr	non trouvée homologué ?		Verisign (EV)
SGMAP	mon.service-public.fr	non trouvée homologué ?	IGC/A	

- D'après sondage en novembre 2013 auprès des RSSI
- Homologations
 - prononcées : aucune
 - travaux réellement en cours : 7 ou 8
- État des connaissances sur le RGS
 - lecture partielle ou exhaustive des documents : moins de 20
 - formation spécifique RGS suivie :
 - moins de 10
 - avis quasi-général de manque de concret
- Réponses et commentaires montrent :
 - nombreuses notions organisationnelles ou techniques peu ou mal intégrées
 - RGS souvent perçu comme contrainte, pas comme valeur ajoutée

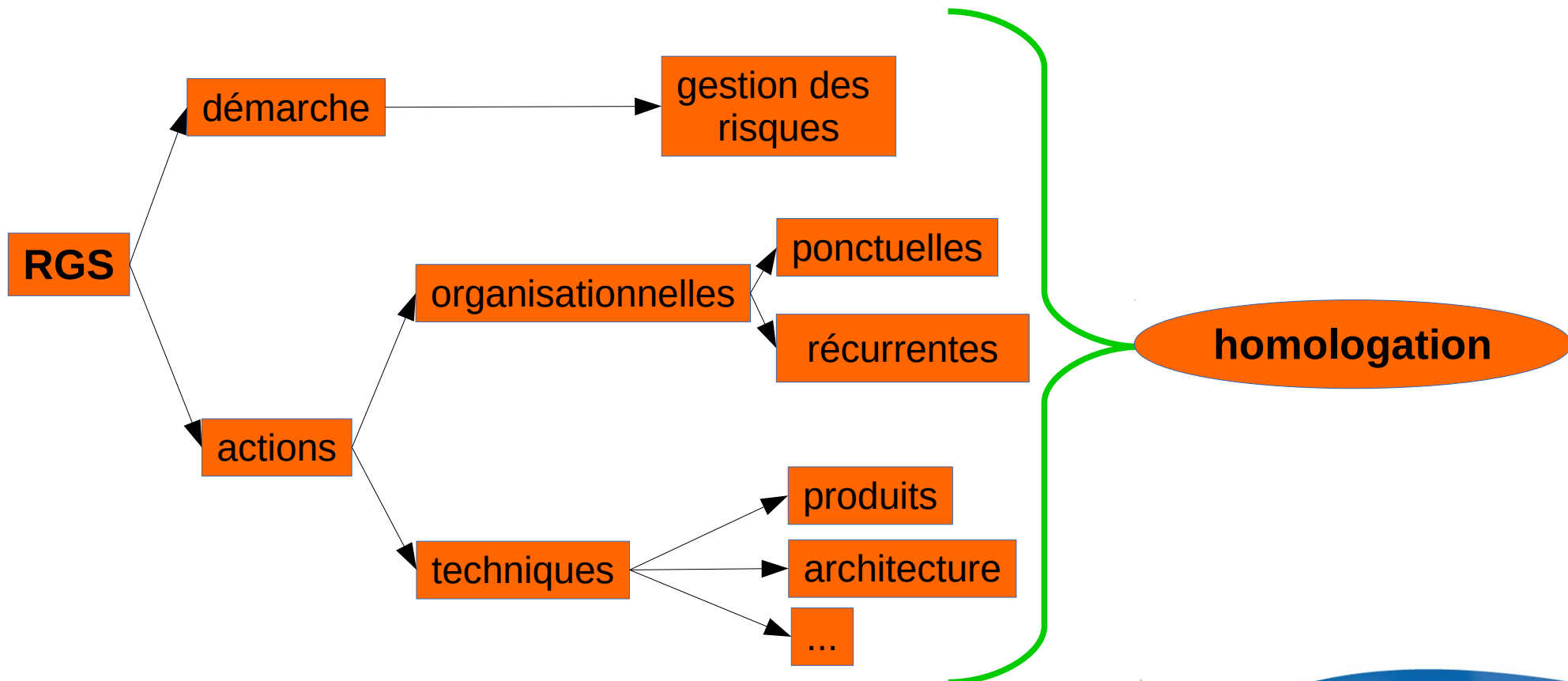
- Par formation ANSSI : parcours « RGS et labellisation » (02/2013)
 - prise de conscience des obligations, de la démarche et des délais
 - bonne découverte des principes de labellisation et d'homologation
 - volet RGS
 - porte surtout sur le cadre et la méthodologie → indispensable
 - mise en œuvre organisationnelle et technique
 - juste survolée
 - pourtant, c'est là que se posent les véritables problèmes (articulation des règles, niveaux de sécurité, processus, etc.) car :
 - systèmes souvent non homologables en l'état
 - difficulté pour la mise en œuvre à coût raisonnable

- Pas de PSSI
 - démarche descendante (approche RGS conseillée) impossible
 - démarche PSSI pas immédiate sans expérience méthodologique
 - élaboration préalable PSSI ? → report important de l'homologation
- Adoption d'une démarche ascendante : homologation RGS pilote
 - appropriation et ajustement des méthodes
 - sur un téléservice simple (périmètre et problèmes réduits)

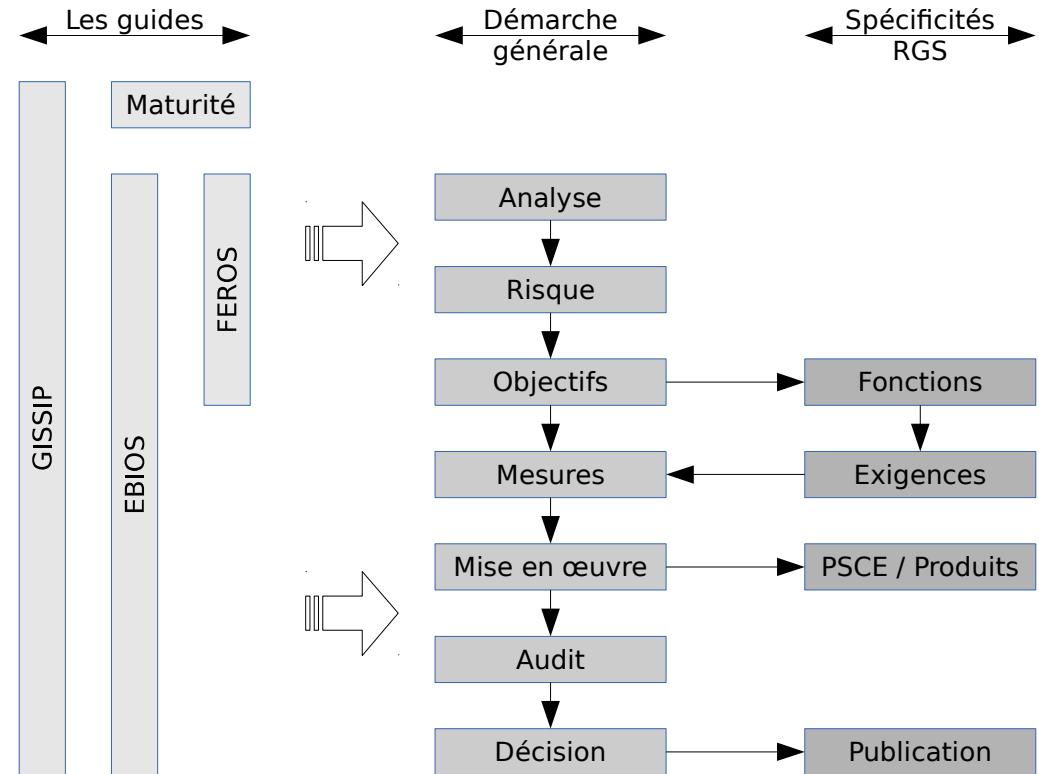
- Arguments poussant à homologuer dès que possible :
 - obligation légale (toutefois pas de sanction prévue)
 - affichage public de la prise en compte du sujet
 - évitement des plaintes des usagers (risques : fermeture du téléservice, invalidation (recrutement, concours, etc.), condamnation à des dommages)
 - obligation de protection des données des usagers (exigence déclaration CNIL)
 - élévation du niveau de sécurité (maturité 0/1 → 2)
- Coût :
 - essentiellement humain (surtout le RSSI)
 - mais à relativiser si remise en cause des mesures de sécurité habituelles
- Projet accepté fin 03/2013

- « Dons en ligne pour la Fondation universitaire »
 - pas d'inscription du donateur, pas de compte informatique => pas de problématique d'authentification d'usager
 - traitements manuels
 - pas de traitement automatisé en liaison avec le reste du SI
 - alerte par mail sur événement (dont AR / AE)
 - sous-traitance du paiement par carte bancaire Paybox : évaluation
- Choix validé par l'AQSSI (09/2013)

- Restreinte en taille afin de mettre en évidence les véritables besoins
- Composition
 - l'autorité d'homologation (AQSSI)
 - le responsable du service et l'agent effectuant les traitements
 - le responsable des systèmes et le chef de projet informatique
 - le RSSI
 - possibilité d'invités et d'observateurs (accompagnement OZSSI)
- Choix validé par l'AQSSI (09/2013)



- Guidé tout au long de la démarche par le GISSIP (Guide d'Introduction de la SSI dans les Projets)
- Guide à géométrie variable en fonction du niveau de maturité requis
- Méthode EBIOS appliquée sur l'ensemble du système
- Les mesures de sécurité et leur mise en œuvre sont générales ou propres au RGS



- Modules de la méthode EBIOS 2010 déroulés de bout en bout
- FEROS générique « paiement »
 - utilisée pour :
 - élaborer les métriques lors de l'étude de contexte (EBIOS module 1)
 - étudier les événements redoutés
 - basée sur EBIOS v2 → transposition
 - document de restitution

- Objectifs de sécurité

- authentification de serveur → HTTPS

- authentification de personnes :

- usager : pas d'authentification

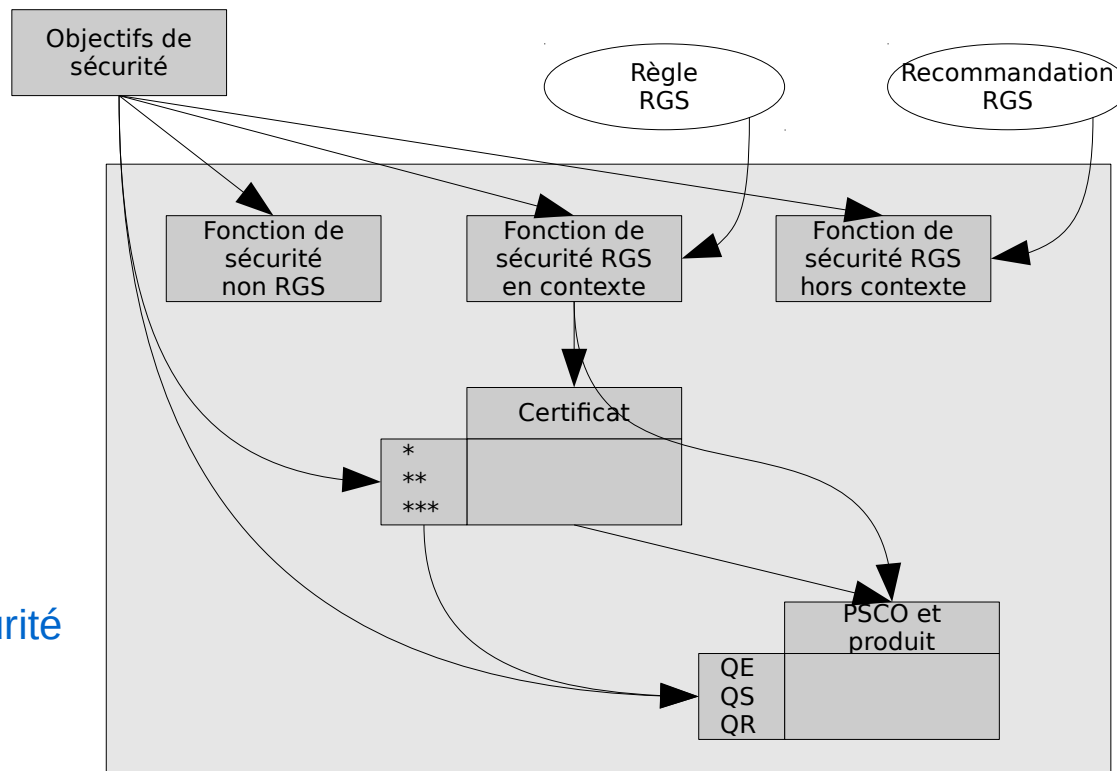
- agents : authentification par mot de passe

- accusé de réception :

- mail simple acceptable

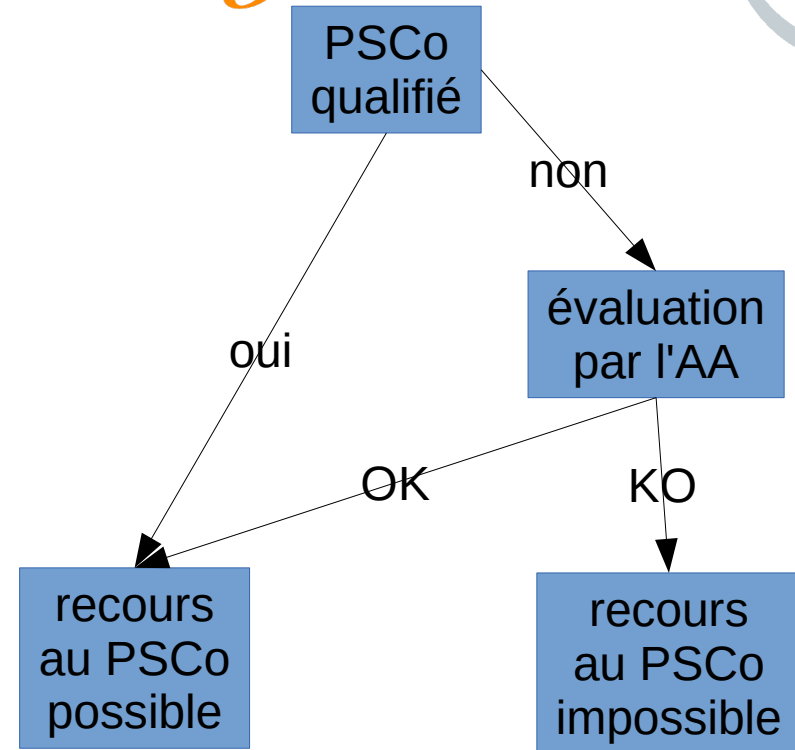
- car doublement par attestation papier → pas de dématérialisation (nécessaire pour déduction fiscale)

- Analyse de risques → objectifs de sécurité
- Définissent des mesures ou fonctions
 - générales
 - spécifiques au RGS
 - hors contexte RGS → recommandations
 - en contexte RGS → règles
 - recours à des produits de sécurité et des prestataires de sécurité
 - dont le niveau est lui aussi déterminé par les objectifs de sécurité



- RGS → fonctions de sécurité
 - 5 fonctions principales + l'horodatage :
 - confidentialité
 - authentification (personne et serveur)
 - signature (personne et cachet)
 - si l'une d'elle s'appuie sur la cryptographie asymétrique, alors les règles de mise en œuvre du RGS s'appliquent pour la fonction
 - et dans ce cas, il y a recours à :
 - des Prestataires de Service de Confiance ou PSCo
 - des produits de sécurité
 - qualifiés ou non
- Obligation d'envoi d'accusé de réception ou d'enregistrement

- PSCo (Prestataires de Service de Confiance)
 - PSCE (Certification Électronique)
 - PSHE (Horodatage Électronique)
 - PASSI (Audit SSI) → RGS v2
- PSCO qualifié
 - liste sur le site de l'ANSSI
 - déclaration d'utilisation à l'ANSSI



- 3 niveaux de sécurité (*, **, ***)
- principales différences :

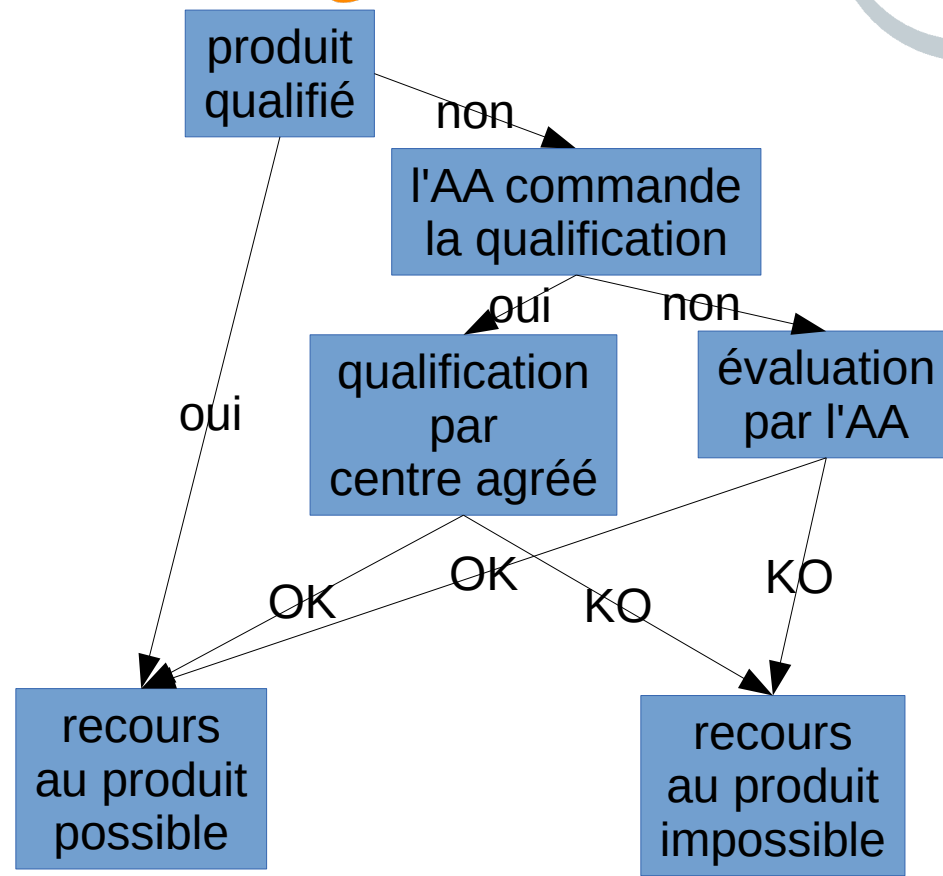
Portée / Niveau	*	**	***
Organisation de l'AA	risque moyen ; protection QE	risque fort ; protection QS	risque très fort ; protection QS/QR
Etablissement contrat AA /AC	courrier ou dématérialisation *	face à face ou dématérialisation **	face à face
Livraison de certificat	mail/téléchargement	face à face ou vérification ; acceptation	face à face ; contrôles ; accusé de réception
Organisation de l'IGC	analyse de risque ; séparation des rôles	analyse de risque ; accès restreint ; forte séparation des rôles	gestion de risque ; accès restreint et traçage ; très forte séparation des rôles
Gestion technique de l'IGC	crypto QE	dématérialisation ** ; crypto QS	face à face et pas de dématérialisation ; protection rayonnements ; crypto QR

- Les certificats utilisés doivent être validés par l'ANSSI (décret RGS) :
 - dépôt d'un dossier à l'ANSII par l'AA
 - validation de certificat ↔ validation de l'utilisation d'un PSCE spécifique par l'AA
 - pas de limite de validité de la validation
- Validation à effectuer même si le PSCE est qualifié

- TCS non qualifié, s'appuyant sur le contrat TERENA / Comodo
 - validation non possible avec les certificats DV (Domain Validated)
 - solution : recours aux certificats EV (Extended Validation) de Comodo → évaluation en cours
- Autre solution : recourir à un PSCE qualifié
- Comment éviter les surcoûts importants ?

AC	*	**	EV
Certinomis	300 € HT	350 € HT	
TCS			150 \$
GeoTrust			249 €
Verisign			1150 €

- 3 niveaux de qualification
 - élémentaire (QE) : basé sur la CSPN
 - standard (QS) : basé sur les CC EAL3+
 - renforcé (QR) : basé sur les CC EAL4+
- Rq : la CSPN est bien adaptée aux logiciels Open Source



- authentification de serveur : HTTPS
 - certificats *
 - validation TCS et certificats EV → validation par l'ANSSI
 - validation OpenSSL (Apache mod_ssl)
 - validation des recommandations cryptographiques
 - organisation de la gestion des certificats
- authentification de personnes :
 - agents uniquement
 - par identifiant/mot de passe
 - suivi des recommandations du RGS
- accusé de réception / enregistrement : sans dématérialisation

- N'entre pas dans le cadre des prestataires (au sens PSCO)
- Nécessité d'évaluer le sous-traitant :
 - relation contractuelle
 - éventuelles certifications du métier
- Dans le cas du paiement via Paybox :
 - évaluation du contrat
 - évaluation des critères de sécurité sur les informations transmises à Paybox
 - vérification de la validité de la certification métier PCI-DSS

- Pour l'homologation des nombreux téléservices existants, traitement par sphère métier ou par problématique similaire
- Recherche de solutions homogènes
 - toolbox RGS
 - choix de solutions utilisables pour tous les téléservices
 - s'inspirant des FEROS génériques
 - box RGS
 - constitution d'une plate-forme regroupant toutes les fonctions RGS
 - conception des téléservices en séparant sphère métier et fonctions de sécurité → déport des fonctions RGS vers la box (portail + fonctions)
 - à la « mon.service-public.fr » (ordonnance « téléservice » art. 7)
- Comment traiter les logiciels commerciaux monolithiques et fermés ?

- Réactivation en novembre 2013
- Regroupement de RSSI ayant des homologations en cours
- Objectifs
 - mieux comprendre
 - proposer des guides, des fiches techniques
 - explorer / valider des PSCE et des produits de sécurité
 - élaborer des solutions génériques
 - envisager des audits croisés
 - créer une synergie trans-ministérielle
 - aborder l'homologation entre AA
- Participation possible...

- Travail considérable en raison du défrichage et des surprises
- Forte valeur ajoutée
 - prise en main des méthodes et ré-utilisabilité
 - élévation du niveau de sécurité
 - ce qui est bon pour un téléservice peut l'être pour tout élément du SI
- Mais faut-il (fallait-il) s'y lancer tout de suite ?
 - oui, car plus facile d'intégrer la SSI dès le début des projets
 - si pas d'en-cours, peut-être attendre
 - l'aboutissement des premiers établissements afin de profiter des expériences
 - la publication du RGS 2



Des questions ?