

Démarche de mise en conformité RGS d'un téléservice : retour d'expérience

Giles Carré

RSSI / Centre des Services Numériques / INSA de Toulouse
135 avenue de Rangueil
31077 Toulouse Cedex 4

Résumé

Depuis le 19 mai 2013, tout téléservice offert par une autorité administrative à ses usagers doit être en conformité avec le Référentiel Général de Sécurité (RGS) et homologué ([1] article 14 et [3]).

Le document central, ou corps, décrit très clairement le contexte d'application du RGS et son intégration dans le cadre de la Sécurité du Système d'Information (SSI) d'un établissement ; le cheminement proposé est descendant et se décline à partir de la politique SSI. Le corps du RGS en lui-même est concis mais il fait référence en permanence à de nombreuses annexes ainsi qu'à des méthodes et nomenclatures (PSSI, EBIOS, GISSIP, FEROS) dont l'ensemble de la documentation couvre quelques milliers de pages. En première approche, une démarche d'homologation RGS peut donc paraître abrupte et son déroulement dépendra certainement de l'état initial de l'organisation de la SSI de l'établissement.

Dans ce contexte, l'INSA de Toulouse décide, au printemps 2013, d'initier une démarche d'homologation d'un premier téléservice simple dans le but de constituer un socle de compétences et de pouvoir envisager par la suite l'homologation de l'ensemble de ses téléservices.

Mots-clefs

RGS, GISSIP, maturité SSI, EBIOS, FEROS, homologation

1 Introduction

Au printemps 2013, l'INSA de Toulouse décide de prendre en mains l'obligation d'homologuer ses téléservices selon les principes du Référentiel Général de Sécurité (RGS). Celui-ci recommande une démarche globale dont le sommet de la pyramide est la politique SSI de l'établissement ([4] section 2.2).

Notre premier problème devient dès lors celui de la démarche à utiliser car nous ne possédons ni politique SSI formalisée, ni documents d'application pouvant en découler, tels que des Procédures d'Exploitation de Sécurité (PES) issues d'une analyse structurée. Cela ne signifie pas, bien évidemment, que nous ne disposons pas de pratiques de sécurité cohérentes et éprouvées, mais simplement qu'elles ne participent pas d'une vision globale et systématique. Nous nous rendons compte alors qu'une approche ascendante, à partir de briques de base issues d'une première homologation RGS expérimentale, pourrait constituer un levier pour mettre en œuvre une organisation structurée de notre SSI. Cet article est un exposé de nos travaux dans ce sens.

Très vite, nous percevons que la première étape sera celle de la compréhension des méthodes et des normes de sécurité à utiliser.

2 Appropriation des méthodes et des normes

Le premier élément à cerner est le corps du RGS, puisque l'objectif premier est bien d'homologuer un téléservice selon ses principes. Il pourrait donc constituer le point de départ de la démarche. Toutefois, bien qu'un bon sens général transparaisse dès la première lecture du corps, le RGS n'est ni une méthode, ni un guide de solutions. Tout au contraire, il fait en permanence référence à d'autres méthodes et normes qu'il va falloir s'approprier et synthétiser. Cette section

n'est pas un exposé sur les méthodes — pour cela, le lecteur pourra se référer à la bibliographie — mais elle apporte quelques réponses aux nombreuses questions que nous nous sommes posées tout au long de l'étude et pour lesquelles on ne trouve pas de réponse directe dans les formations ou les documents publiés à ce jour. Cette section fait partie intégrante de notre démarche car les réponses qui y apparaissent ne sont survenues qu'au fur et à mesure de notre progression, de nos tâtonnements et de nos erreurs, et nous avons trouvé qu'il serait plus clair d'en faire une synthèse plutôt que de signaler comment elle nous sont apparues.

2.1 Le RGS 1.0

L'esprit du RGS est de donner confiance à l'utilisateur d'un téléservice ; pour cela, le fournisseur du service (l'Autorité Administrative ou AA) atteste, via une homologation, que son système est protégé de manière adaptée ([2] article 5).

Le corps du RGS détaille essentiellement la démarche de mise en œuvre d'un point de vue autorité administrative ; il précise les notions de fonctions, de prestataire et de produits de sécurité.

2.1.1 La démarche de mise en œuvre du RGS d'un point de vue AA

Les seules étapes qu'impose le RGS sont :

- une démarche de gestion des risques, quelle qu'elle soit, ce qui signifie qu'elle peut-être élémentaire — pourvu qu'elle réponde aux enjeux — et qu'aucune méthode n'est imposée, seule la connaissance des risques étant requise ([2] article 3) ;
- un engagement de l'AA auprès des usagers, formalisé par une homologation ([2] article 5) pour une durée de 3 à 5 ans ([4] section 2.3.2). Aboutissement de l'analyse de risques, l'homologation est une acceptation des risques résiduels et une autorisation de mise en exploitation¹.

En complément aux règles, le RGS formule des recommandations telles que l'adoption d'une démarche descendante et la pratique de méthodes éprouvées ([4] section 2.2) :

- démarche globale, élaboration d'une PSSI, mise en place des conditions pour une amélioration continue (Système de Management de la Sécurité de l'Information ou SMSI, défini par une norme telle que ISO 27001 ou un standard tel que ITIL Security Management) ;
- efforts proportionnés aux enjeux : intégration de la SSI dans les projets (voir le Guide d'Intégration de la SSI dans les Projets, ou GISSIP [8]) et analyse de maturité SSI (voir la section 2.3 et [9]) ;
- emploi d'outils adaptés, en particulier par le biais des Fiches d'Expression Rationnelle des Objectifs de Sécurité (FEROS) génériques (voir la section 2.2 et [7]) ;
- gestion systématique des risques par une méthode telle qu'EBIOS, complétée par les FEROS ;
- utilisation de produits de sécurité et de Prestataire de Services de CONfiance (PSCO) qualifiés.

2.1.2 Les fonctions et les produits de sécurité du RGS

L'analyse de sécurité aboutit à la définition de mesures de sécurité dont la mise en œuvre s'appuie sur des fonctions matérielles ou logicielles ([2] article 4). Lorsque les fonctions de sécurité retenues sont, d'une part, répertoriées dans le RGS (c'est-à-dire les cinq fonctions *confidentialité*, *authentification des personnes*, *signature*, *authentification des serveurs* et *cachet*) et qu'elles font appel, d'autre part, à des mécanismes de cryptographie asymétrique, alors les règles de mise en œuvre du RGS s'imposent ([5] section I des annexes A1 à A5). À contrario, toute fonction de sécurité autre que ces cinq fonctions, et que l'on aura retenue à l'issue de la même analyse de risques, ne relève pas des règles du RGS. De plus, si l'une des cinq fonctions RGS n'utilise pas, dans le contexte du service concerné, de mécanisme de cryptographie asymétrique, alors sa mise en œuvre ne relève pas des obligations du RGS mais, tout au plus, de simples recommandations. C'est le cas, par exemple, d'une authentification des personnes basée sur un couple (identifiant, mot de passe) pour laquelle on aurait opté dans la gestion du risque ([4] section 3.2.2).

Après avoir déterminé si les fonctions à mettre en œuvre dans le contexte relèvent des règles du RGS, il faut fixer leur

1. Dans le cadre de PSSIE (Politique de Sécurité des Systèmes d'Information de l'État), dont la parution est imminente, tout système d'information devra être homologué, au sens de l'acceptation des risques résiduels.

niveau d'application. Comme indiqué précédemment, ces règles s'appuyant sur les mécanismes de cryptographie asymétrique, le niveau d'application est en quelque sorte le niveau du certificat. Le RGS définit trois niveaux de sécurité pour les certificats (une, deux ou trois étoiles, notés aussi « * », « ** » ou « *** »). La sémantique de ces niveaux est définie dans les annexes A1 à A5 du RGS d'un point de vue utilisateur de certificat, et dans les annexes A6 à A11 d'un point de vue fournisseur du certificat (autorité de certification ou Prestataire de Service de Certification Électronique (PSCE)). Les annexes A6 à A11, ou Politiques de Certification, listent les obligations que doivent suivre les PSCE selon le niveau de sécurité du certificat fourni. Ces politiques de certifications ont donc deux objectifs :

1. indiquer aux PSCE les critères qui seront retenus par les organismes habilités pour les qualifier ;
2. donner aux utilisateurs de certificat, c'est-à-dire les autorités administratives (AA), les éléments qui leur permettront de définir le niveau du certificat (une, deux ou trois étoiles) dont ils ont besoin.

A partir de l'analyse de sécurité et, plus particulièrement, des besoins de sécurité, l'AA choisit le niveau du certificat à utiliser dans le contexte étudié (Figure 1). Le RGS ne donne aucune indication ou règle pour mettre en relation un objectif de sécurité donné avec un niveau de sécurité d'une fonction mais c'est le bon sens qui doit prévaloir ici : choix d'un niveau qui couvre tous ses besoins (afin de répondre complètement aux objectifs), mais rien que ses besoins (afin de maîtriser coûts et complexité).

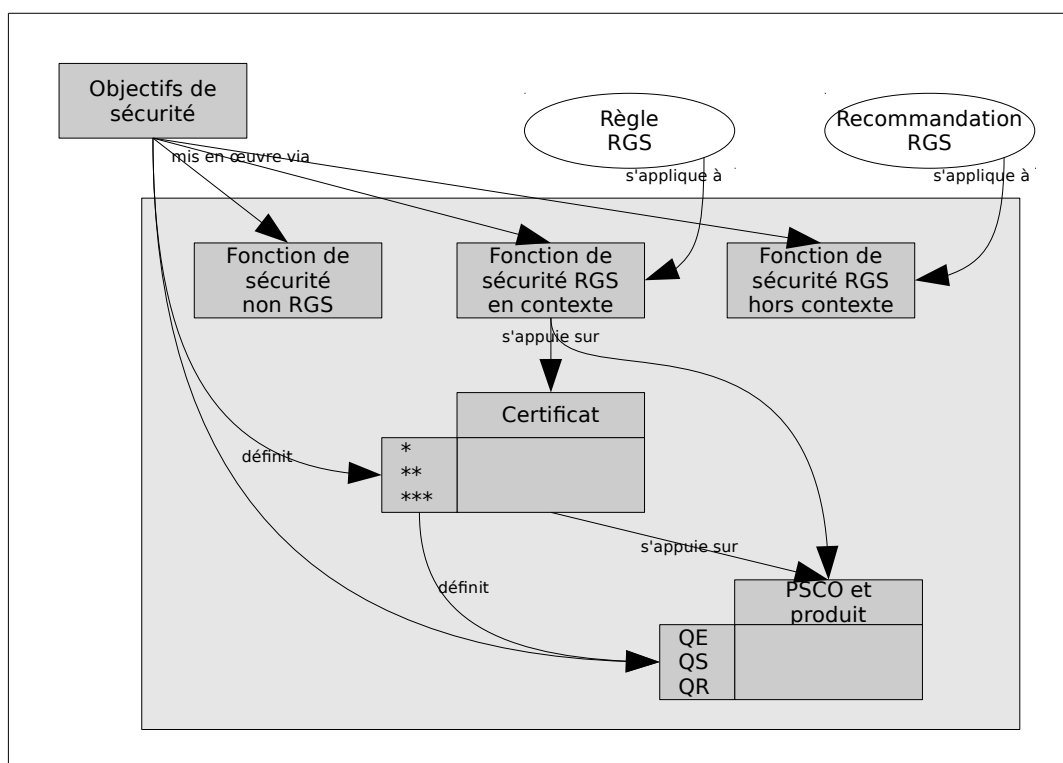


Figure 1 - Niveaux relatifs des fonctions et des produits de sécurité

Les fonctions de sécurité sont implémentées par des produits de sécurité matériels ou logiciels. Selon le niveau du certificat retenu, chaque produit de sécurité utilisé doit répondre à des critères spécifiés dans le RGS, voire être qualifié RGS et porter un label indiquant le niveau de qualification. Le RGS définit trois niveaux de qualification des produits : Qualification Élémentaire, Qualification Standard et Qualification Renforcée (QE, QS et QR). À nouveau, ce sont les annexes qui indiquent, pour une fonction spécifique, la relation entre le niveau de sécurité du certificat et la qualification requise pour un produit. Les notions de Prestataire de Service de CONfiance (PSCO) et de produit de sécurité définies dans le RGS ne concernent que la mise en œuvre des fonctions de sécurité du RGS ([2] article 4).

Le tableau de la Figure 2 synthétise, à partir des annexes A4 et A9 du RGS, les différences entre les niveaux de sécurité *, ** et *** et explicite ainsi la portée des niveaux des certificats et des produits dans le cas de l'authentification de serveur. La plupart des éléments répertoriés sont valables pour les autres fonctions de sécurité.

| Catégorie d'opération | * | ** | *** | Référence |
|--|---|---|--|------------------------|
| utilisation par l'AA | risque moyen d'usurpation d'identité ; si dispositif de clé privée fournie par l'AC, protection QE | risque fort d'usurpation d'identité ; si dispositif de clé privée fournie par l'AC, protection QS ; application et module auth. QS recommandés | Risque très fort d'usurpation d'identité ; si dispositif de clé privée fournie par l'AC, protection QR ; application et module auth. QS recommandés | A9 § I.4.1 A4 § III |
| authentification initiale destinataire du certificat | dossier papier, échange secret partagé ou dématérialisation * | en face à face ou dématérialisation ** | en face à face | A9 § III |
| remise de certificat | mail ou téléchargement ; acceptation tacite par le destinataire | face à face, ou vérification du destinataire ; acceptation explicite par le destinataire | face à face, ou vérification du destinataire ; contrôle possession clé privée associée ; acceptation signée par le destinataire | A9 § IV |
| gestion de l'IGC | analyse de risque recommandée ; séparation des rôles | analyse de risque recommandée ; accès physique limité ; sauvegarde hors site ; séparation renforcée des rôles | analyse et gestion de risque exigés ; accès physique limité et traçage ; sauvegarde hors site ; séparation encore plus renforcée des rôles | A9 § I.3.1 A9 § V |
| gestion technique de l'IGC | certaines opérations par au moins 1 personne de confiance et devant témoins ; module crypto au moins QE, et QS recommandé | renforcement nombre de personnes de confiance et de témoins ; fractionnement du secret ; opérations en face à face ou dématérialisation ** ; système info QS recommandé ; module crypto au moins QS, et QR recommandé | renforcement nombre de personnes de confiance et de témoins ; protection contre les rayonnements ; fractionnement du secret ; opérations en face à face sans dématérialisation ; système info QS recommandé ; module crypto QR exigé | A9 § VI |

Figure 2 - Synthèse des différences entre les niveaux de sécurité pour la fonction d'authentification de serveur (annexes A4 et A9).

2.1.3 Évolution du RGS 1.0

L'ANSSI prépare actuellement la version 2 du RGS. Les évolutions annoncées portent essentiellement sur :

- la définition des critères retenus pour la qualification d'un nouveau type de prestataire (PSCO), les Prestataires d'Audit en SSI (PASSI) ;
- une restructuration de la documentation, dont l'utilité peut se percevoir à la lecture de la section précédente, la complexité de la documentation actuelle s'expliquant par son volume et par les nombreuses références croisées ;
- dans le futur, l'extension de la portée des fonctions de sécurité et le glissement de certaines recommandations en exigence.

Lorsque l'on aborde le RGS 1.0, on constate que la démarche est relativement simple mais que le volume d'informations à synthétiser est très important. Chacun doit donc se positionner entre l'attente de la simplification de la documentation et l'obligation de devoir déjà disposer de téléservices homologués. Dans tous les cas, plus tôt on prendra en mains le sujet et plus il sera facile d'homologuer, en particulier en introduisant les concepts du RGS dès les prémices des nouveaux projets. De plus, aucun investissement effectué dans le cadre de la version 1.0 du RGS ne devrait être remis en cause par la version 2.

2.2 La gestion des risques par EBIOS et les FEROS

Le RGS recommande donc une démarche globale et exige une connaissance des risques ([2] article 3). La méthode EBIOS propose une démarche structurée et guidée pour établir la liste des risques, puis les mesures à appliquer pour réduire ces risques et, enfin, la liste des risques résiduels ([6]). La méthode peut être utilisée sur des systèmes élémentaires comme sur l'intégralité d'un système d'information. Sur un système simple et en fonction des objectifs visés, elle peut être bouclée en quelques jours.

Elle comporte plusieurs étapes, dont la plus importante est sans doute la première : l'identification de tous les éléments qui serviront au cours des étapes suivantes. Tout particulièrement pour cette première étape, le responsable de l'analyse devra s'entourer des personnes compétentes pour répondre aux questions sur le système à étudier : identification des biens à protéger, identification des menaces potentielles, mais aussi quantification des impacts suite à des événements de sécurité, besoins en sécurité...

Selon les objectifs de l'analyse, la liste des livrables est variable mais l'un d'eux peut être intéressant dans le cadre du RGS : l'analyse de risques et l'identification des fonctions de sécurité peut être représenté par une Fiche d'Expression Rationnelle des Objectifs de Sécurité (FEROS), dont il existe des versions génériques dans le cadre du RGS ([7]).

2.3 Le GISSIP et la maturité SSI

Mais ni le RGS, ni la méthode EBIOS, ni les FEROS ne peuvent constituer le point de départ des travaux d'homologation, car l'ensemble de ces guides et nomenclatures se réfèrent les uns les autres en permanence.

Pour cela, l'ANSSI propose le Guide d'Introduction de la SSI dans les Projets ou GISSIP ([8]), une méthode modulaire basée sur le cycle de vie d'un système. Sa particularité est d'être adaptable dans sa granularité au contexte étudié. En particulier, il indique, pour chaque étape, les actions à conduire selon le niveau de sécurité requis, ou maturité SSI.

Il faut donc commencer par évaluer sa maturité SSI, une approche méthodologique de l'ANSSI ([9]), qui permet de mettre en parallèle le niveau de maturité adéquat d'un système et son niveau de maturité effectif, puis d'en déduire une démarche d'évolution. Le déroulement de la méthode peut être simple et se situer uniquement au niveau de la perception de l'état de sécurité de son système.

Grâce au niveau de maturité adéquat, le GISSIP indiquera les actions à mener pour chaque étape. Ainsi, par exemple, on constate qu'aux étapes 2 et 3 (respectivement conception générale puis conception détaillée), la FEROS n'est requise qu'à partir du niveau 3 de maturité adéquat, sur 5 niveaux.

Le schéma simplifié de la Figure 3, dérivé d'un document de l'ANSSI, représente notre utilisation des guides dans la démarche d'homologation.

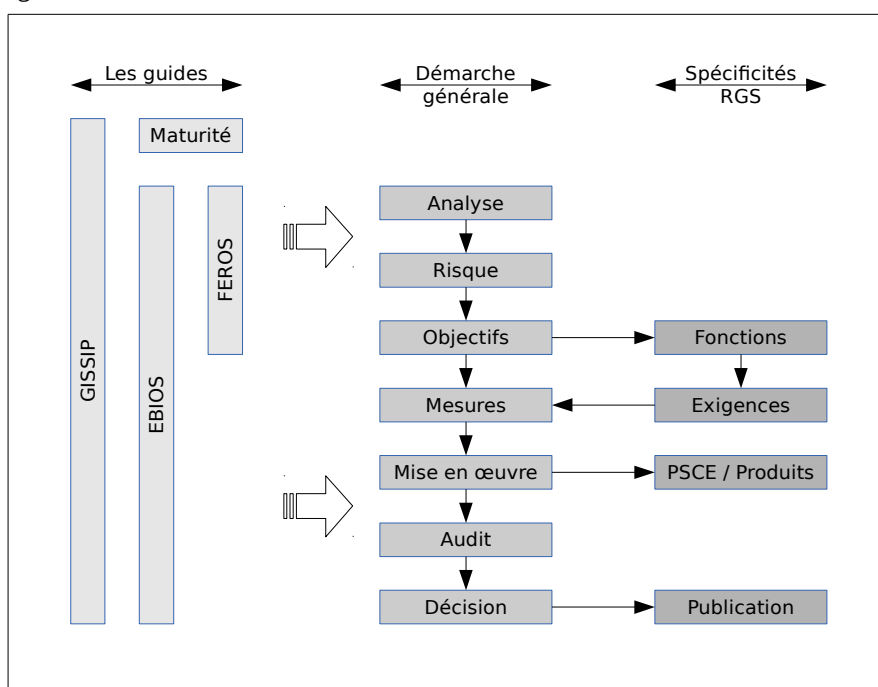


Figure 3 - Positionnement des guides dans la démarche d'homologation.

3 Le déroulement du projet

Cette section décrit le déroulement de notre travail d'homologation et commente les étapes.

3.1 Le point de départ

L'INSA de Toulouse change de RSSI en 2012 et envoie son nouveau responsable à la formation « RSSI » d'une semaine à l'ANSSI ; une journée complète y est consacrée à la méthode EBIOS et à l'homologation RGS. C'est là que nous découvrons nos obligations d'homologation et que nous percevons l'intérêt des méthodes formelles. Mais cette initiation est insuffisante et il est nécessaire de poursuivre les formations à l'ANSSI avant de passer à l'action :

- janvier 2013, « la méthode EBIOS » (3 jours) : sa durée est suffisante pour s'imprégner de la méthode et l'étude de cas (1 journée complète) permet de commencer à se l'approprier ;
- février 2013, le parcours « RGS et labellisation » (3 jours) permet de découvrir les concepts de labellisation et d'homologation ainsi que le vocabulaire associé ; en ce qui concerne le RGS (1 journée), la formation insiste essentiellement sur le cadre et la méthodologie mais passe quasiment sous silence le positionnement des fonctions de sécurité et leur contenu ; il faudra combler nous-même, et avec difficulté, l'absence d'éléments concrets ;
- mai 2013, après avoir commencé à travailler sur le sujet, nouvelle journée « RGS » dans le cadre de l'OZSSI, assez proche d'un des modules de la formation de février, néanmoins très bénéfique pour approfondir le sujet et répondre plus précisément aux questions que nous nous sommes posées entre temps.

Durant toute cette période de formation, plusieurs lectures croisées des documentations (RGS, EBIOS, FEROS et GISSIP) sont nécessaires et il nous faut plusieurs mois de gestation avant d'attaquer l'analyse de sécurité orientée RGS.

3.2 Le lancement du projet

Pour initier le projet d'homologation des téléservices, le RSSI propose une démarche d'homologation à sa DSI puis se place dans son rôle de conseiller auprès de sa direction afin de l'alerter sur la nécessité d'une action en présentant le cadre, les principes et les raisons justifiant une démarche d'homologation :

- assise juridique : présentation de l'enchaînement des loi, ordonnance et décret ;
- portée du RGS : téléservices aux usagers ou entre autorités administratives (AA) ;
- raisons poussant à aborder l'homologation :
 - être en conformité avec la législation, dans l'esprit et dans la lettre ;
 - éviter des poursuites par un usager ou groupe d'usagers (bien qu'aucune sanction ne soit envisagée au niveau de l'état) ;
 - éviter de devoir suspendre un service, d'annuler ou invalider une opération (recrutement, etc.) ou de devoir verser des dommages ;
 - protéger les données personnelles et le prouver ;
- obligations du RGS : homologation s'appuyant sur une gestion des risques, acceptation des risques résiduels et publication de la décision ;
- démarche ascendante car une démarche globale et descendante n'aboutirait pas dans notre contexte ;
- importance d'homologuer rapidement (échéances légales), mais aussi pour introduire dès que possible la SSI et le RGS en particulier dans les nouveaux projets ; inutilité d'attendre la publication de la version 2 du RGS.

Les moyens et les objectifs de l'homologation expérimentale sont formulés et approuvés par le Directeur Général des Services :

- choix d'une démarche ascendante pour expérimenter et s'approprier les méthodes, ainsi que pour comprendre suffisamment les concepts généraux et être en mesure de produire des appels d'offre ;
- travail sur un téléservice existant simple, à choisir de manière à ce que la gestion de la sécurité n'impose pas de remise en cause majeure, l'objectif principal étant de rôder la démarche ;
- constitution officielle d'une commission d'homologation et implication des instances concernées ;
- objectif direct : homologation d'un téléservice et mise au point de la méthode ;
- objectifs indirects : commencer à structurer l'aspect organisationnel de notre SSI, afficher que les obligations liées au RGS sont prises en compte et évaluer dans quelle mesure on améliore la sécurité, dans le but d'envisager une PSSI.

3.3 Choix du téléservice

Le téléservice « Dons en ligne pour la Fondation universitaire de l'INSA de Toulouse » ([10]) choisi pour la première homologation existe depuis deux ans. Les arguments du choix sont liés à la simplicité de ses processus :

- pas d'inscription du donateur, pas de compte informatique, ce qui évite la problématique de l'authentification des personnes ;
- paiement par mécanisme externe via Paybox, service pouvant être considéré lui-même comme un téléservice, et qui pourrait être à évaluer ;
- pas de traitement automatisé en liaison avec le reste du système d'information, ce qui limite le périmètre ;
- traitements exclusivement manuels (extraction de données et édition de documents) et alerte par mail sur événement.

La FEROS Type « paiement » ([7]) pourra servir de guide d'analyse et d'ébauche de solution.

Le fait de choisir un service simple et maîtrisé n'est pas un détournement mais il permet de réduire la quantité de problèmes à traiter. A priori, il y aura au minimum à utiliser la fonction d'authentification de serveur, associée à une cryptographie asymétrique (utilisation de SSL), ainsi qu'une évaluation des certificats issus du service TCS de Renater. Le choix semble donc pertinent dans le cadre de l'expérimentation et est validé par le Directeur général des Services.

3.4 Communication et constitution de la commission d'homologation

Un article est publié dans l'hebdomadaire interne de l'INSA afin de présenter le principe du RGS et de prévenir les personnels qu'ils seront susceptibles d'être consultés par la commission d'homologation.

La commission formée est minimaliste afin de pouvoir détecter facilement les manques (il s'agit d'une expérimentation), ce qui ne transparaîtrait pas s'il y avait trop de redondances de compétence. En raisonnant à partir des questions auxquelles il va falloir répondre durant l'analyse de sécurité, la liste des membres est établie : autorité d'homologation et président (le Directeur de l'INSA ou son représentant, le DGS), animateur de la commission (le RSSI), autorité d'emploi (directrice de la fondation universitaire), utilisateur gestionnaire (secrétaire de la fondation), responsable des biens support (responsable système et réseau) et chef de projet informatique. Il est officiellement précisé que la commission peut, à sa discrétion, associer tous les experts dont elle aura besoin ainsi qu'inviter des observateurs extérieurs, le but étant d'éventuellement amorcer des collaborations régionales en invitant d'autres organismes.

La commission est officiellement nommée par le Directeur de l'INSA. Pour simplifier son fonctionnement, des consignes et directives sont fixées par le DGS, ce qui lui permettra de ne pas participer directement aux réunions. Le mandat de la commission est fixé : conduite des travaux, émission d'un avis sur l'homologation et proposition d'homologation en vue du maintien en service.

3.5 L'étude de sécurité

Nous suivons les étapes du GISSIP.

3.5.1 Première étape : opportunité

Elle consiste à déterminer le niveau de maturité adéquat. Ce travail a déjà été réalisé en début d'année 2013 à la demande du FSSI² ; notre niveau de maturité adéquat visé est le niveau 2. Une note d'orientation élémentaire est rédigée ; le plus grand soin doit être apporté à ce document, car il constituera une source d'informations essentielle pour ceux qui devront maintenir le système en conditions de sécurité et renouveler son homologation dans le futur.

3.5.2 Seconde étape : faisabilité

Aucune action n'est requise à cette étape pour une maturité de niveau 2.

3.5.3 Troisième étape : conception générale

Au niveau de maturité 2, cette étape produit une liste des meilleures pratiques SSI applicables dans le cadre du système. Cette liste est élaborée à partir du déroulement de la méthode EBIOS ; elle permet d'identifier les objectifs de sécurité :

- étude du contexte (module 1) :
 - là aussi, le plus grand soin et la plus grande simplicité sont apportés lors de la rédaction des documents définissant le cadre, à nouveau à destination des équipes qui assureront la continuité dans le futur ;
 - la définition des métriques s'avère difficile pour nous qui n'avons jamais pratiqué cet exercice, mais nous y parvenons en nous demandant si les niveaux retenus nous permettront de tout qualifier de manière intelligente et en nous rendant compte que les échelles ne sont pas nécessairement linéaires ;
 - l'identification des biens essentiels est relativement aisée, celle des biens support n'est pas complexe (car guidée par la nomenclature) mais elle est laborieuse car vaste, même sur un projet simple ; nous savons toutefois qu'elle sera réutilisable pour d'autres téléservices, tout comme l'inventaire des mesures existantes ; cette phase est menée au cours d'entretiens individuels.
- l'étude des événements redoutés (module 2), des scénarios de menace (module 3) et des risques (module 4) est assez mécanique et ne présente pas de difficulté majeure. Elle se conclut par la définition des objectifs de sécurité. Dans notre contexte, le niveau de sécurité retenu est le niveau « une étoile » ou « * ».
- à partir des objectifs de sécurité, nous identifions d'une part les fonctions de sécurité à mettre en œuvre, que nous validons avec la FEROS type « paiement », et, d'autre part, les mesures de sécurité générales et spécifiques RGS.

3.5.4 Quatrième étape : conception détaillée

Les mesures de sécurité identifiées à l'étape précédente sont validées avec le chef de projet informatique et le responsable des biens support ; les moyens sont identifiés. C'est à cette étape que les certificats TCS de Renater sont évalués par rapport aux exigences du niveau « * ».

Le dossier de sécurité est assemblé : note d'orientation, étude de sécurité et FEROS type complétée.

3.5.5 Cinquième étape : réalisation

Les mesures de sécurité sont mises en place sous la direction du chef de projet informatique et du responsable des biens support, puis leur bonne application est vérifiée sous le contrôle du RSSI.

La démarche et le système sont évalués par notre OZSSI qui intervient donc comme auditeur externe. Il intervient aussi sous la forme de transfert de compétences sur les méthodes et l'audit, l'un des objectifs étant de pouvoir participer ultérieurement à des audits croisés avec d'autres organismes.

Le dossier de sécurité est enrichi des résultats de l'audit et la commission propose l'homologation du système.

2. Le Fonctionnaire de la Sécurité des Systèmes d'Information est chargé d'animer la SSI au sein d'un ministère, en autres en direction des AQSSI (Autorité Qualifiée pour la SSI), autorités responsables de la SSI dans les services ministériels et les établissements publics.

3.5.6 Sixième étape : exploitation

Sur présentation de la FEROS, l'autorité d'homologation accepte les risques résiduels et prononce l'homologation. La durée d'homologation choisie est volontairement courte (un an), bien que le RGS recommande une durée allant de trois à cinq ans ; en effet, il s'agit d'une expérimentation et des affinages seront sans doute nécessaires.

La forme de la décision d'homologation à publier sur le téléservice avait été soumise en amont au service juridique afin d'être certain de répondre aux obligations en la matière. Une forme synthétique et très lisible pour le public est retenue de manière à respecter l'esprit du RGS.

4 Conclusion

Les objectifs de l'expérimentation ont été remplis. La démarche utilisée nous a permis d'homologuer un premier téléservice avec un minimum d'effort, si on ne comptabilise toutefois pas le temps de formation et d'appropriation initial. Avant de passer à un programme global d'homologation, il s'avère toutefois nécessaire d'ajuster notre démarche et de la vérifier sur un téléservice quelconque de notre système d'information.

L'utilisation d'une méthode formelle d'analyse nous a permis de repérer quelques mesures de sécurité, non spécifiques au RGS, à ajuster sur ce téléservice ; l'étude a donc contribué à l'amélioration de la sécurité. Ce constat nous donne des arguments en faveur d'une approche globale de la SSI et de l'élaboration d'une politique de sécurité.

Bibliographie

- [1] Ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives, surnommée « ordonnance téléservices ». Journal Officiel du 9 décembre 2005.
<http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000636232&dateTexte=vig>
- [2] Décret n° 2010-112 du 2 février 2010 pris pour l'application des articles 9, 10 et 12 de l'Ordonnance 2005-1516, surnommé « décret RGS ». Journal Officiel du 4 février 2010. <http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000021779444&dateTexte=vig>
- [3] Arrêté du 6 mai 2010 portant approbation du référentiel général de sécurité et précisant les modalités de mise en œuvre de la procédure de validation des certificats électroniques. Journal officiel du 18 mai 2010.
<http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000022220429>
- [4] ANSSI. Référentiel Général de Sécurité version 1.0. Corps du RGS. 6 mai 2010.
<http://www.ssi.gouv.fr/fr/reglementation-ssi/referentiel-general-de-securite/liste-des-documents-constitutifs-du-rgs-v1-0.html>
- [5] ANSSI. Référentiel Général de Sécurité version 1.0. Annexes du RGS. 6 mai 2010.
<http://www.ssi.gouv.fr/fr/reglementation-ssi/referentiel-general-de-securite/liste-des-documents-constitutifs-du-rgs-v1-0.html>
- [6] ANSSI. EBIOS 2010 - Expression des Besoins et Identification des Objectifs de Sécurité.
<http://www.ssi.gouv.fr/fr/bonnes-pratiques/outils-methodologiques/ebios-2010-expression-des-besoins-et-identification-des-objectifs-de-securite.html>
- [7] DGME. FEROS types. <http://references.modernisation.gouv.fr/outils-pour-la-mise-en-oeuvre-du-rgs>
- [8] ANSSI. Guide d'Intégration de la Sécurité des Systèmes d'Information dans les Projets. 11/12/2006.
<http://www.ssi.gouv.fr/fr/bonnes-pratiques/outils-methodologiques/gissip-guide-d-integration-de-la-securite-des-sytemes-d-information-dans-les.html>
- [9] ANSSI. Maturité SSI. 02/11/2007.
<http://www.ssi.gouv.fr/fr/bonnes-pratiques/outils-methodologiques/guide-relatif-a-la-maturite-ssi.html>
- [10] INSA de Toulouse. Site de don en ligne de la fondation universitaire.
<http://www.insa-toulouse.fr/fr/institution/fondation/don.html>