



Le référentiel général de sécurité (RGS)

Pierre RAYNAL délégué de l'Observatoire Zonal SSI au Ministère de l'Intérieur

ANSSI

Agence nationale de la
sécurité des systèmes
d'information

OZSSI zone de défense Sud-Est



Citoyens



Quelle confiance ?

- Est-ce que je m'adresse effectivement à un service de l'administration française ?
- Nos échanges et les données que je transmets restent-ils bien confidentiels ?
- Comment attester de la signature d'un document électronique ? A quelle date ?
- Quel accusé de réception et attestation vais-je obtenir et pouvoir conserver ?

Autorité administrative

Téléservices

État-civil,
Allocations familiales,
etc.

Besoin

**attestation formelle
de la prise en compte de
la sécurité du téléservice**

Préfecture :

- Site web
- Formulaires en ligne
- Informations :
 - Concours et examens
 - Marchés publics
 - Enquêtes publiques
 - Élections
 - Etc.
- Espace réservé sur authentification

Région:

- Site web
- Marchés publics
- Offres d'emploi
- Espace entreprises
- Portail des territoires

L'utilisateur utilisant ces services est-il protégé ?

Peut-il faire confiance sur :

- l'absence de logiciel malveillant ;
- la confidentialité des données à caractère personnel qu'il fournit ;
- la bonne prise en compte d'une demande ;
- la fiabilité des informations lues ;
- etc.

30 septembre 2010 Inscriptions scolaires auprès des communes :
la CNIL contrôle un mauvais élève

Les écoles maternelles et primaires sont sous la responsabilité des communes. [...] La commune contrôlée ne demandait pas moins de 10 documents ou renseignements différents pour la définition du quotient familial, dont **certains semblent excessifs**.

On peut notamment citer :

- * la copie de l'attestation de sécurité sociale,
- * la copie complète de jugements de divorce susceptibles de faire apparaître les motifs de séparation,
- * la copie des tableaux d'amortissements de prêts immobiliers,
- * la copie des derniers bilans d'activités ou d'attestations comptables pour les professions libérales ou artisanales faisant apparaître les détails des actifs et des passifs (charges salariales, loyer de locaux, prêts etc.),
- * la collecte de données d'infraction relatives à la situation irrégulière de parents étrangers ou à du travail non déclaré. [...]

Pour noircir le tableau, **la sécurité des systèmes d'information est apparue insuffisante**, tant par l'absence de renouvellement des mots de passe d'accès aux postes informatiques, que par des **transmissions de données non sécurisées**.

La CNIL se prononcera prochainement sur les suites à apporter à ces **manquements à la loi** « informatique et libertés ».

- Le contexte du RGS
 - L'ordonnance de 2005
 - Les télé-services
 - Les autorités administratives
- Le contenu du RGS
 - Ce qu'il prescrit
 - Son organisation
 - Fonctions de sécurité et cryptographie
- La mise en application du RGS
 - Échéances
 - La démarche
 - Les aides

Décembre 2005

- **Ordonnance « téléservices »** relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives

Art. 9 : Un RGS fixe **les règles que doivent respecter les fonctions** des systèmes d'information

Art 10 : Les **certificats électroniques** délivrés aux autorités administratives et à leurs agents font l'objet d'une **validation par l'Etat**

Art 12 : Les produits de sécurité et les prestataires de services de confiance peuvent faire l'objet d'un **référencement par l'Etat**

n°2005-1516 du 8 décembre 2005

Février 2010

- **Décret RGS** pris pour l'application des articles 9, 10 et 12 de l'ordonnance.

• n°2010-112 du 2 février 2010

Mai 2010

- **Arrêté** du Premier ministre
- Rend le **contenu du RGS** officiel

Contexte : à qui s'adresse le RGS ?

Directement, le RGS s'adresse aux **autorités administratives**

- les administrations de l'État
- les collectivités territoriales
- les établissements publics à caractère administratif
- les organismes gérant des régimes de protection sociale
- les autres organismes chargés de la gestion d'un service public administratif

Celles-ci sont d'une **grande variété** selon leur taille, leur fonction, leurs exposition aux risques, leur maturité en sécurité des systèmes d'information, etc.

Pour **les autres organismes**, le RGS est un recueil de bonnes pratiques pour évaluer et améliorer le niveau de sécurité de leurs systèmes

Indirectement, le RGS s'adresse

- aux **prestataires** qui assistent les autorités administratives dans la sécurisation des échanges dématérialisés
- aux **industriels** réalisant des **produits de sécurité**

Chaque organisme adapte l'usage qu'il fait du RGS à ses besoins et ses moyens

Téléservice : tout système d'information permettant aux usagers de procéder par voie électronique à des démarches ou formalités administratives.

Par exemple :

Candidature : enseignement supérieur, permis de conduire

Consultation : remboursements SS, résultats d'examens ou concours

Déclaration : TéléIR, comptes fiscaux professionnels, changement d'adresse

Demande : extraits d'état-civil, permis de construire, licence IV, stages étudiants

Inscription : Concours fonction publique

Paiement : Amendes, TVA, impôt sur le revenu

Simulation : Pensions

- Le contexte du RGS
 - L'ordonnance de 2005
 - Les télé-services
 - Les autorités administratives
- **Le contenu du RGS**
 - Ce qu'il prescrit
 - Son organisation
 - Fonctions de sécurité et cryptographie
- La mise en application du RGS
 - Échéances
 - La démarche
 - Les aides

Mieux connaître son patrimoine informationnel

Obtenir et conserver la **confiance** des usagers

Engager les investissements **au juste niveau**
(humains et financiers)

Maîtriser les risques techniques et juridiques

Améliorer la capacité de résistance des SI à une
attaque

1. Identifier les biens à protéger et les menaces à prendre en considération

2. Déterminer les **objectifs de sécurité**

selon les critères de disponibilité, intégrité, confidentialité, traçabilité, identification, pour se protéger de manière **proportionnée** face aux risques

3. En déduire les **fonctions de sécurité** nécessaires

Dans sa première version, le RGS traite des fonctions de sécurité **authentification, signature électronique, chiffrement, horodatage**, et fournit les règles à respecter en fonction du niveau de sécurité recherché

4. Recourir de préférence à des **produits et services labellisés**

5. Attester formellement de la prise en compte de la sécurité : Homologuer C'est la prise de responsabilité de l'autorité administrative

6. Viser le **maintien** du niveau de sécurité et une **amélioration** continue

Analyse
de
risque

- Corps (33 pages)

Fonctions de sécurité

- A1 Confidentialité
- A2 Authentification
- A3 Signature électronique
- A4 Authentification serveur
- A5 Cachet serveur

A12 Politique d'horodatage type

A13 Variables de temps

A14 Profils de certificats

Politiques de certification type

- A6 Confidentialité
- A7 Authentification
- A8 Signature électronique
- A9 Authentification serveur
- A10 Cachet serveur
- A11 Authentification et signature

Mécanismes cryptographiques

- B1 Choix et dimensionnement
- B2 Gestion des clés
- B3 Authentification : règles et recommandations

- Si l'autorité administrative décide de mettre en œuvre une fonction de sécurité décrite, elle doit respecter les règles.

Trois **niveaux de confiance** de l'IGC :

1*, 2**, 3***

selon le processus d'enregistrement et de remise des clés et certificats

Cryptographie asymétrique :
RSA 2048 SHA 256 minimum

Cryptographie symétrique
100 bits minimum
128 bits recommandé

Le RGS impose de distinguer les **usages** qui sont faits des clés et des certificats.

L'usage mixte authentification et signature à vocation à disparaître.

Les algorithmes SHA 1 et MD5 sont **obsolètes** et ne doivent plus être utilisés.

- Le contexte du RGS
 - L'ordonnance de 2005
 - Les télé-services
 - Les autorités administratives
- Le contenu du RGS
 - Ce qu'il prescrit
 - Son organisation
 - Fonctions de sécurité et cryptographie
- **La mise en application du RGS**
 - Échéances
 - La démarche
 - Les aides

Qualification des produits :

- Cible de sécurité
- Élémentaire, standard, renforcée
- Catalogue publié par l'ANSSI

Qualification des prestataires de services de confiance

- Autorités de certification et d'horodatage
- par l'intermédiaire d'un LSTI

Validation des certificats électroniques :

- des autorités administratives et des agents

évolution des techniques et des menaces ;
nouvelles **fonctions de sécurité** ;
avis et propositions reçus après la publication ;

définir des référentiels techniques destinés à la qualification
de nouvelles familles de **prestataires de services de
confiance** :

- **audits** de systèmes d'information ;
- **hébergement** de systèmes d'information ;
- personnalisation des dispositifs sécurisés ;
- archivage sécurisé de données.

Délais de mise en conformité

- 3 ans pour les téléservices et systèmes en service
- 1 an pour les téléservices et systèmes en cours de réalisation jusqu'à octobre 2010
- d'emblée pour les téléservices et systèmes déployés après novembre 2010

1. Recenser les télé-services mis à disposition par l'autorité administrative ;
2. Constituer une commission d'homologation ;
3. Évaluer leurs besoins de sécurité :
 - sous l'angle de la **disponibilité** du service,
 - de **intégrité** des données,
 - de la **confidentialité** des données.
 -
4. Analyser les risques auxquels ils sont exposés ;
5. Prendre (compléter) des mesures de sécurité ;
6. Évaluer les risques résiduels que l'autorité administrative accepte en commission d'homologation et attester formellement de la prise en compte de la sécurité du téléservice.

**Non
technique**

**Technique et
organisationnel**

**Non
technique**