

Le référentiel général de sécurité (RGS)

L'ADMINISTRATION ÉLECTRONIQUE EN TOUTE CONFIANCE



Le développement de l'administration électronique est l'un des principaux leviers de l'amélioration de la qualité des services publics. Pour permettre cet essor, la confiance des usagers est primordiale. Dans le monde des échanges numériques, la confiance se construit pour une large part en garantissant la sécurité des systèmes d'information.

C'est pour répondre à cet enjeu et aider les autorités administratives à y faire face qu'a été élaboré le référentiel général de sécurité (RGS).

1. Qu'est-ce que le RGS ?

Le RGS est un recueil de règles et de bonnes pratiques en matière de sécurité des systèmes d'information destiné principalement aux autorités administratives qui proposent des services en ligne aux usagers.

Des bonnes pratiques de gestion de la sécurité des systèmes d'information

Le RGS encourage les administrations à adopter une approche globale pour la protection de leurs systèmes d'information afin de mettre en œuvre des mesures de sécurité cohérentes, adaptées aux enjeux et répondant aux besoins de sécurité. Ceci passe par une **analyse systématique des risques** qui pèsent sur les systèmes d'information. Cette analyse, qu'il est

souhaitable de faire dès la phase amont des projets, est régulièrement mise à jour pour permettre une **amélioration continue** de la sécurité des systèmes d'information.

Des règles techniques concrètes

Selon les fonctions de sécurité (cf. encadré ci-contre) retenues et le niveau de sécurité souhaité par l'autorité administrative, le RGS définit les exigences techniques et les moyens de protection pertinents en termes de produits de sécurité et d'offres de services de confiance. **Le RGS constitue ainsi un cadre adaptable aux enjeux et aux besoins spécifiques de chaque autorité administrative.**

Quatre fonctions de sécurité

- **L'authentification :**
l'authentification est l'action par laquelle le système d'information vérifie l'identité de l'utilisateur. Les procédés utilisés par l'utilisateur pour prouver son identité vont de l'emploi d'un couple identifiant/mot de passe à l'utilisation d'un certificat électronique personnel stocké sur une carte à puce.
- **La signature électronique :**
la signature d'un document électronique garantit l'identité du signataire et l'intégrité du document signé.
- **La confidentialité :**
cette fonction permet de s'assurer qu'une information ne peut être consultée par un tiers non autorisé au cours de son transfert ou de son stockage.
- **L'horodatage :**
ce procédé permet de garantir qu'un document ou un message existait à un instant donné. Il fait foi dans le domaine des échanges électroniques.

2. Les objectifs du RGS

Le RGS a pour principal objectif de développer la confiance des usagers et des administrations dans leurs échanges numériques.

Dans ce cadre, le RGS permet notamment :

- de favoriser l'adoption par les administrations de bonnes pratiques en matière de sécurité des systèmes d'information ;
- d'adapter les solutions techniques aux

justes besoins de sécurité identifiés pour chaque système d'information ;

- d'offrir aux autorités administratives les labels de sécurité permettant de s'assurer de la qualité des produits et des services de sécurité proposés par le marché ;
- de favoriser le respect des dispositions de la loi « informatique et libertés » relative à la protection des données personnelles.

Quel est le cadre juridique du RGS ?

- Le RGS est prévu par l'ordonnance 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives. Cette ordonnance définit le périmètre et le rôle du référentiel général de sécurité : « fixer les règles que doivent respecter les fonctions des systèmes d'information contribuant à la sécurité des informations échangées par voie électronique ».
- Le décret n° 2010-112 du 2 février 2010 porte création du référentiel général de sécurité.

3. À qui s'adresse le RGS ?

Le RGS s'adresse avant tout aux autorités administratives. Il s'adresse également aux prestataires qui les assistent dans la sécurisation des échanges dématérialisés.

Les directeurs de services informatiques, les responsables de la sécurité des systèmes d'information de même que les chefs de projets au sein de

maîtrises d'œuvre sont les principaux acteurs pour lesquels le RGS est utile.

Le RGS est également destiné aux :

- prestataires de services de confiance (par exemple, les fournisseurs de certificats électroniques) ;
- industriels développant des produits de sécurité.

De qui émane le RGS ?

Le RGS est le résultat d'un travail conjoint entre l'agence nationale de la sécurité des systèmes d'information (ANSSI) et la direction générale de la modernisation de l'État (DGME).

Qu'est-ce que l'ANSSI ?

L'agence nationale de la sécurité des systèmes d'information, service du Premier ministre, est rattachée au secrétaire général de la défense et de la sécurité nationale. Créée le 7 juillet 2009, elle est l'autorité nationale en matière de cybersécurité.

Plus d'informations sur le RGS :

www.references.modernisation.gouv.fr

Rendez-vous sur le site pour :

- obtenir les documents constitutifs du référentiel ;
- télécharger les supports méthodologiques pour sa mise en œuvre ;
- connaître l'actualité du RGS.

Retrouvez également sur ce site les documents de référence de l'administration électronique sur l'accessibilité, l'interopérabilité et l'ergonomie des sites Internet publics.

Contact :

- DGME - Service Projets : rgs.dgme@finances.gouv.fr
- ANSSI (pour les questions techniques) : rgs@ssi.gouv.fr

Accueil - RGS - Sécurité

RGS - Sécurité

Présentation du Référentiel Général de Sécurité

Le Référentiel général de sécurité (RGS) définit un ensemble de règles de sécurité qui s'imposent aux autorités administratives dans la sécurisation de leurs systèmes d'information. Il propose également des bonnes pratiques en matière de sécurité des systèmes d'information que les autorités administratives sont liées d'appliquer.

Le RGS a été élaboré conformément à l'article 9 de l'ordonnance n°2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives ainsi qu'entre les autorités administratives. Il fixe les règles que doivent respecter les fonctions des systèmes d'information contribuant à la sécurité des informations échangées par voie électronique.

Le RGS apporte les éclairages nécessaires aux autorités administratives pour prendre en compte pleinement les dispositions de l'ordonnance.

Statut du document

La version en cours de ce document est une version de travail rédigée conjointement par l'Agence nationale de sécurité des systèmes d'information (ANSSI) et la Direction générale de la modernisation de l'État (DGME). Elle tient compte des contributions reçues suite à :

- la consultation des hauts fonctionnaires de défense et de sécurité des systèmes d'information des ministères (HFDSS) en juin 2007 ;
- la présentation du document aux représentants des collectivités territoriales en mai 2008 ;
- l'appel à commentaires publics qui a eu lieu durant les mois de mai et juin 2008 ;
- la consultation des ministères en novembre 2008.

Les grandes dates

Décret RGS

TÉLÉCHARGER LA VERSION PDF

- RGSV0-99.pdf 1.425 Mo
- RGS-AnnexesA.zip 6.982 Mo
- RGS-AnnexesB.zip 8.933 Mo

AUTOUR DU RGS

LA DIRECTION GÉNÉRALE DE LA MODERNISATION DE L'ÉTAT

Au sein du ministère du Budget, des Comptes publics et de la Réforme de l'État, la direction générale de la modernisation de l'État (DGME) pilote le suivi de la mise en œuvre de la révision générale des politiques publiques et accompagne les ministères dans leurs chantiers de transformation. À l'écoute des usagers et de leurs attentes, la DGME conduit également des chantiers interministériels structurants dans les domaines de l'administration électronique, de la simplification administrative, de l'amélioration de l'accueil des usagers et de la qualité des services publics.