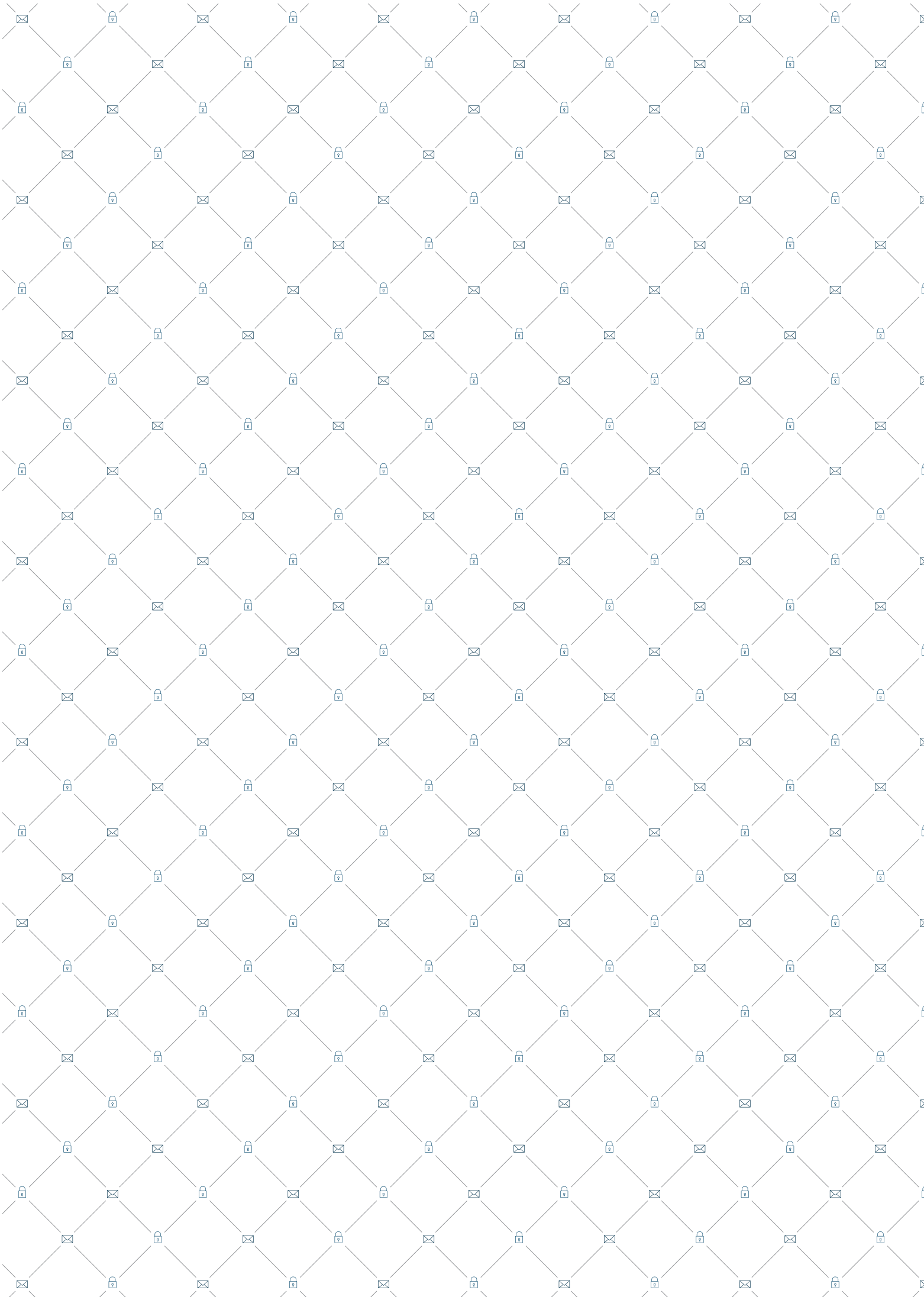
CHARTE POUR LA SÉCURITÉ DES SERVICES DE COURRIERS ÉLECTRONIQUES

élaborée dans le cadre d'une coopération entre
l'agence nationale de la sécurité des systèmes d'information
et des fournisseurs de services de courriers électroniques



PRÉAMBULE

La dématérialisation sans cesse croissante des échanges d'information expose quotidiennement les données personnelles et les correspondances privées à la cybermenace. Dans ce contexte, la sécurité des réseaux publics de communications électroniques est devenue l'une des clés de la protection de la vie privée et des correspondances électroniques.

Face à ce constat, l'Agence nationale de la sécurité des systèmes d'information (ANSSI) et des opérateurs et fournisseurs de Services de courriers électroniques volontaires ont défini ensemble des mesures de sécurité destinées à renforcer la sécurité des canaux de transmission des courriers électroniques. Reposant sur des principes de chiffrement des flux de données, ces mesures ont pour objectif de lutter contre les interceptions massives de courriers électroniques, notamment par écoute passive ou par détournement des communications.

Les opérateurs et fournisseurs de Services de courriers électroniques destinés au grand public qui souhaitent mettre en œuvre ces mesures de sécurité peuvent signer la présente Charte afin de marquer leur engagement à protéger les courriers électroniques de leurs Utilisateurs conformément à ces mesures de sécurité.

Article 1er

DÉFINITIONS

Au sens de la présente Charte, on entend par :

- **« Charte » :** la présente Charte y compris son annexe.
- **« Service de courriers électroniques » :** un service destiné au grand public permettant d'échanger entre Utilisateurs tout message sous forme de texte, de son ou d'image et des documents numériques, en utilisant le protocole de transport *SMTP (Simple Mail Transfer Protocol)* via Internet. Les services de messagerie instantanée (ou de dialogue en ligne) et les forums de discussion ne sont pas considérés comme des Services de courriers électroniques.
- **« Utilisateur » :** une personne utilisant un Service de courriers électroniques.
- **« Signataire » :** un opérateur ou fournisseur de Service de courriers électroniques ayant signé la présente Charte.

Article 2

OBJET

La présente Charte a pour objet de définir des mesures de sécurité destinées à renforcer la protection des courriers électroniques ainsi que les engagements des opérateurs ou fournisseurs de Services de courriers électroniques relatifs à la mise en œuvre de ces mesures.

Article 3

RÔLE DE L'ANSSI

L'ANSSI a élaboré la présente Charte avec le concours des opérateurs ou fournisseurs de Services de courriers électroniques volontaires et en est le dépositaire.

L'ANSSI anime les travaux menés avec les opérateurs ou fournisseurs de Services de courriers électroniques volontaires en vue de l'élaboration des mesures de sécurité qui figurent en annexe et de leur mise à jour compte tenu de l'évolution des technologies et des menaces. L'ANSSI s'assure notamment que les mesures de sécurité ainsi élaborées sont pertinentes au regard des menaces.

Article 4

ENGAGEMENTS DES SIGNATAIRES

Cette Charte se base sur l'engagement volontaire des Signataires à respecter de bonne foi les mesures techniques et organisationnelles décrites en annexe.

Dans ce cadre, les Signataires s'engagent à :

1. appliquer l'intégralité des mesures décrites en annexe au sein de leurs infrastructures techniques et de leur organisation, de manière permanente ;

2. coopérer entre eux, et avec l'ANSSI, chaque fois que nécessaire, afin d'assurer la bonne application des dispositions de la Charte et d'adapter les mesures décrites en annexe en fonction des évolutions technologiques et des nouvelles menaces ;

3. s'échanger les informations techniques nécessaires pour la détection, le diagnostic et la résolution des incidents intervenant sur les liens de transmission entre Signataires, dans le respect de la confidentialité de ces informations ;

4. prendre en compte, notamment dans la configuration de leurs infrastructures de courriers électroniques, les noms de domaine de chaque nouveau Signataire dans un délai de trois mois à compter de son adhésion à la Charte ;

5. communiquer régulièrement à l'ANSSI et à l'ensemble des Signataires des indicateurs techniques sur la mise en œuvre dans leurs infrastructures et leurs organisations des mesures décrites en annexe, après avoir conjointement défini avec l'ANSSI le type d'indicateurs à mesurer ;

6. informer sans délai l'ANSSI et les autres Signataires de toute difficulté dans l'application ou l'interprétation de la Charte.

Article 5

UTILISATION DU SERVICE DE COURRIERS ÉLECTRONIQUES

Afin de bénéficier des mesures de sécurité mentionnées en annexe, l'Utilisateur d'un Service de courriers électroniques doit :

- utiliser le Service de courriers électroniques d'un Signataire et s'assurer que le destinataire utilise également le Service de courriers électroniques du même ou d'un autre Signataire ;
- accéder au Service de courriers électroniques par l'utilisation soit :
  - de l'interface web permettant de lire, gérer et envoyer des courriers électroniques *(Webmail)* mise à disposition par le Signataire ;
  - d'une application de courriers électroniques configurée de telle sorte que le chiffrement soit activé en émission et en réception ; selon les cas, cette configuration est gérée par le Signataire fournissant le Service de courriers électroniques et activée par défaut, ou bien elle doit être

effectuée par l'Utilisateur.
Les mesures mentionnées en annexe n'offrent pas une protection contre l'ensemble des risques liés à l'utilisation d'un Service de courriers électroniques. Les Utilisateurs des Services de courriers électroniques sont en conséquence encouragés à adopter de bonnes pratiques de sécurité informatique, notamment en choisissant convenablement les mots de passe de courriers électroniques et en se protégeant des courriers malveillants.

Article 6

RESPONSABILITÉ À L'ÉGARD DES UTILISATEURS

En publiant la présente Charte sur leur site Internet, les Signataires informent leurs Utilisateurs de leur démarche visant à renforcer la sécurité des canaux de transmission des courriers électroniques en mettant en œuvre les mesures de protection prévues par la Charte. Il est rappelé que ces mesures ne sauraient offrir en tout état de cause une protection contre toutes les menaces.
Les dispositions de la présente Charte n'engagent pas les Signataires à l'égard des Utilisateurs de leurs Services de courriers électroniques.

Article 7

ADHÉSION À LA CHARTE

Tout opérateur ou fournisseur d'un Service de courriers électroniques peut adhérer à la Charte, dès lors qu'il s'engage à en respecter l'ensemble des dispositions. À cet effet, il signe la Charte et en communique à l'ANSSI un exemplaire signé. L'ANSSI publie sur son site Internet (www.ssi.gouv.fr) les exemplaires signés de la Charte et tient à jour la liste des Signataires. Chaque Signataire informe ses Utilisateurs de son adhésion à la Charte en publiant sur son site Internet la Charte signée et en précisant les noms de domaine concernés. Chaque Signataire est libre à tout moment de mettre fin à son adhésion à la Charte, en en informant par écrit au moins 3 mois en avance les autres Signataires et l'ANSSI. Dans ce cas, le Signataire ne fait plus état de son adhésion à la Charte sur son site Internet.

Article 8

MODIFICATION ET ABROGATION DE LA CHARTE

L'ANSSI et les Signataires peuvent, d'un commun accord, modifier à tout moment la Charte par un avenant qui est signé par ces derniers.
Toutefois, l'ANSSI et les Signataires peuvent modifier l'annexe de la Charte d'un commun accord sans que cela ne nécessite la signature d'un avenant. Dans ce cas, l'ANSSI communique au préalable l'annexe modifiée à chaque Signataire pour recueillir son accord.
La Charte modifiée est publiée dans les conditions prévues à l'article 7.
L'ANSSI et les Signataires peuvent, d'un commun accord, abroger la Charte. L'ANSSI peut aussi abroger unilatéralement la Charte en cas de désaccord avec ou entre les Signataires. En cas d'abrogation, les Signataires en informent leurs Utilisateurs au moyen de leurs sites Internet.

Signataire de la Charte : LA POSTE

Représenté par *(nom, prénom)* **:** COLLIN NATHALIE

Date : 16/10/2010

Signature :

ANNEXE

MESURES DE SÉCURITÉ DES SERVICES DE COURRIERS ÉLECTRONIQUES

Cette annexe comprend les mesures de sécurité applicables d'une part aux liens d'accès des Utilisateurs au Service de courriers électroniques et d'autre part aux liens entre les serveurs de transfert de messages des Signataires.

1.
Sécurité des liens d'accès des Utilisateurs au Service de courriers électroniques

1.1 Exigences générales

Quelles que soient les modalités d'accès (interface web, protocoles *IMAP* ou *POP* et *SMTP*, etc.), le Signataire permet à l'Utilisateur de recourir au protocole *TLS (Transport Layer Security)*. Les paramètres *TLS* doivent permettre un bon niveau de sécurité sans empêcher l'accès de certains logiciels clients particuliers (logiciels anciens, systèmes mobiles, etc.). À cet effet, les politiques de choix des mécanismes cryptographiques appliqués par les Signataires sont régulièrement réévaluées pour suivre les évolutions techniques. Il est tenu compte de l'état du parc matériel et logiciel des Utilisateurs, des vulnérabilités rendues publiques et des recommandations émises par les organismes spécialisés, notamment l'ANSSI.

Les Services de courriers électroniques sont authentifiés par des certificats délivrés par des autorités de certification reconnues par les principaux navigateurs et clients de messagerie.

Les Signataires prennent en charge au moins une suite cryptographique offrant une confidentialité persistante *(Perfect Forward Secrecy)*, par exemple en recourant à l'algorithme d'échange de clé *Diffie-Hellman (DHE)* ou sa variante basée sur les courbes elliptiques *(ECDHE)*.

1.2 Accès *Webmail*

Lorsque l'accès au Service de courriers électroniques se fait au moyen d'une interface web, le protocole *HTTPS* est utilisé pour le formulaire d'authentification et pour l'ensemble des pages du *Webmail* parcourues pendant la session authentifiée.

Ce service web fait par ailleurs l'objet d'un processus d'amélioration continue de la sécurité, portant notamment sur la protection contre le vol de session ou de données d'authentification. Les Signataires se tiennent informés des recommandations émises par les organismes spécialisés, tels que l'*OWASP (Open Web Application Security Project)*, ou par l'ANSSI et s'en inspirent pour maintenir à un bon niveau leurs mesures de protection.

1.3 Accès par les protocoles de messagerie

Lorsque l'accès aux courriers électroniques se fait au moyen de protocoles de messagerie tels que *POP, IMAP* et *SMTP*, le *TLS* « implicite » est pris en charge sur les ports prévus à cet effet : 995 ou 993 pour *POP* ou *IMAP* et 465 pour *SMTP*. Dans la mesure du possible, le *TLS* « explicite » *(« STARTTLS »)* est pris en charge sur les ports standards : 110 ou 143 pour *POP* ou *IMAP* et 587 (et éventuellement 25) pour *SMTP*.

Les terminaux ou les applications fournis par les Signataires et qui intègrent des Services de courriers électroniques dont ils maîtrisent le paramétrage initial utilisent le protocole *TLS* dans ces conditions.

2.
Sécurité des liens entre les serveurs de transfert de messages

2.1 Exigences générales

Les communications entre les serveurs *Mail Transfer Agents (MTA)* de deux Signataires sont protégées par *TLS*.

Les serveurs *MTA* sur lesquels les courriers électroniques transitent ou sont stockés sont situés sur le territoire national pour les domaines concernés. Les conditions d'exploitation de ces serveurs permettent d'assurer la sécurité des courriers électroniques.

Lorsqu'une interruption du chiffrement par *TLS* vers ou depuis un *MTA* réputé conforme à la Charte est détectée, le Signataire s'efforce de rétablir l'utilisation de *TLS* dans les meilleurs délais.

2.2 Configuration des *MTA*

La configuration des *MTA* associés aux Services de courriers électroniques des Signataires respectent les dispositions suivantes :

- *TLS* est utilisé, en version 1.0, 1.1 ou, idéalement, en version 1.2.
- La méthode *STARTTLS* du protocole *SMTP* (port 25) est acceptée en réception ; elle est employée en émission lorsque le destinataire indique la supporter. Le support de *STARTTLS* est annoncé en réponse à la commande *EHLO*.

Ces dispositions sont appliquées au moins vis-à-vis de l'ensemble des autres Signataires, l'objectif étant de les appliquer à terme vis-à-vis de tous les autres Services de courriers électroniques supportant *STARTTLS*. Les Signataires favorisent l'emploi d'algorithmes cryptographiques de bonne qualité. À cette fin, ils privilégient lorsque les équipements concernés les prennent en charge :

- l'algorithme de chiffrement symétrique *AES* plutôt que les algorithmes obsolescents *3DES* ou *RC4* qui peuvent présenter des faiblesses dans certains cas ;
- les algorithmes d'échange de clé *ECDHE* et *DHE*, qui présentent la propriété de « confidentialité persistante » ;
- les algorithmes de hachage *SHA-256* et *SHA-384* plutôt que les algorithmes obsolescents *MD5* et *SHA-1* qui peuvent présenter des faiblesses dans certains cas.

- L'authentification des serveurs en réception est assurée par l'usage de certificats délivrés par une autorité de certification.