Centre de la sécurité des télécommunications
Communications Security Establishment

CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

Directives de mise en œuvre :

Protection du domaine de courrier

SÉRIE PRATICIEN

Canada

AVANT-PROPOS

L'ITSP.40.065, intitulé *Directives de mise en œuvre : Protection du domaine de courrier,* est un document NON CLASSIFIÉ publié avec l'autorisation du dirigeant principal du Centre canadien pour la cybersécurité (Centre pour la cybersécurité). Pour obtenir de plus amples renseignements, envoyez un courriel ou téléphonez à notre centre d'appel :

Centre d'appel
contact@cyber.gc.ca
(613) 949-7048 ou 1-833-CYBER-88

DATE D'ENTRÉE EN VIGUEUR

Le présent document entre en vigueur le 12 août 2021.

HISTORIQUE DES RÉVISIONS

Révision	Modifications	Date
1	Première version	7 avril 2020
1.1	Les changements ci-dessous ont été apportés : - ajout de l'annexe C : Analyser l'information liée aux courriels; - simplification de l'étape de la mise en application dans le plan de mise en œuvre; - suppression des mentions du service de rapports DMARC du Centre pour la cybersécurité; - ajout d'éclaircissements sur la manière dont le protocole DMARC gère la mise en correspondance des domaines et la balise sp; - élargissement des orientations sur les sous-domaines et les domaines autres que les domaines de courrier; - restructuration des sections sur les normes pertinentes - diverses corrections et précisions.	12 août 2021

ISBN 978-0-660-40019-8
CAT D97-3/40-065-2021F-PDF

TABLE DES MATIÈRES

1 Vue d'ensemble 7

2 Mécanismes de protection des domaines de courrier 8

2.1 SPF 8

2.2 DKIM 8

2.3 Limites des protocoles SPF et DKIM 9

2.4 DMARC 10

2.4.1 Validation DMARC 10

2.4.2 Rapports DMARC 12

3 Autres considérations 13

3.1 Prise en charge par le fournisseur 13

3.2 Expéditeurs tiers 13

3.2.1 Expéditeurs tiers et protocole SPF 13

3.2.2 Expéditeurs tiers et protocole DKIM 13

3.2.3 Expéditeurs tiers et protocole DMARC 13

3.2.4 Séparation de sous-domaines 14

3.3 Transfert de messages 14

3.3.1 Protocole ARC (Authenticated Received Chain) 14

3.4 Courrier entrant 15

3.5 Chiffrement de courriels dans la couche transport 15

3.5.1 STARTTLS 15

3.5.2 Protocole DANE (DNS-Based Authentication of Named Entities) 15

3.5.3 Protocole MTA-STS (*MTA Strict Transport Security*) 16

3.6 Domaines autres que les domaines de courrier 16

3.7 Brand Indicators for Message Identification (BIMI) 16

4 Résumé 17

4.1 Coordonnées 17

5 Contenu complémentaire 18

5.1 Abréviations, acronymes et sigles 18

5.2 Références 19

LISTE DES FIGURES

Figure 1 : Validation DMARC.....11

LISTE DES ANNEXES

Annexe 1 Plan de mise en œuvre 20

1.1 Vue d'ensemble 20

1.2 Évaluer 21

1.2.1 Déterminer les domaines de courrier 21

1.2.2 Évaluer l'état actuel 21

1.2.3 Déployer l'enregistrement DMARC initial 21

1.2.4 Recueillir et analyser les rapports DMARC 22

1.3 Déployer 24

1.3.1 Déterminer les expéditeurs autorisés 24

1.3.2 Configurer la durée de vie (TTL) des enregistrements DNS 24

1.3.3 Déployer le protocole SPF pour tous les domaines 24

1.3.4 Déployer le protocole DKIM pour tous les domaines et expéditeurs 24

1.3.5 Surveiller les rapports DMARC et corriger les erreurs de configuration 25

1.4 Mettre en application 26

1.4.1 Renforcer progressivement la mise en application 26

1.4.2 Exceptions liées aux sous-domaines 27

1.4.3 Domaines autres que les domaines de courrier 27

1.5 Assurer la maintenance 28

1.5.1 Surveiller les rapports DMARC 28

1.5.2 Corriger les erreurs de configuration et mettre les enregistrements à jour 28

1.5.3 Assurer la rotation des clés DKIM 28

Annexe 2 Référence sur les protocoles 29

2.1 SPF 29

2.1.1 Enregistrements SPF 29

2.1.2 Expéditeurs tiers 30

2.1.3 Limite de recherches DNS 30

2.2 DKIM 31

2.2.1 Enregistrements DKIM 31

2.2.2 Considérations cryptographiques 31

2.2.3 Expéditeurs tiers 32
2.3 DMARC 33
2.3.1 Enregistrements DMARC 33
2.3.2 Sélection de la stratégie DMARC 34
2.3.3 Mise en correspondance des domaines dans le protocole DMARC 35
2.4 Domaines autres que les domaines de courrier 36
2.4.1 Enregistrement MX indiquant l'absence de service 36
2.4.2 SPF 36
2.4.3 DMARC 36
Annexe 3 Analyser l'information liée aux courriels 37
3.1 En-têtes de message 37
3.1.1 Authentication-Results 38
3.1.2 DKIM-Signature 40
3.1.3 Received-SPF 41
3.2 Rapports DMARC globaux 42
3.2.1 Métadonnées du rapport 42
3.2.2 Stratégie publiée 42
3.2.3 Enregistrements 43
3.3 Interpréter les résultats DMARC 47
3.3.1 Résultats SPF 47
3.3.2 Résultats DKIM 48
3.3.3 Échecs DMARC 48
3.3.4 Caractéristiques d'une campagne d'usurpation 49

1 VUE D'ENSEMBLE

Le présent document fournit des conseils aux propriétaires de systèmes sur la mise en œuvre de mesures de sécurité techniques visant à protéger leurs domaines contre l'usurpation d'adresse électronique. Dans le présent document, nous décrivons les mesures techniques que les propriétaires de systèmes peuvent mettre en œuvre afin de prévenir la livraison de certains messages malveillants qui minent la réputation de leurs domaines et de détecter l'infrastructure utilisée par les auteurs malveillants.

La mise en œuvre de ces directives vous aidera à empêcher les auteurs de menace de se faire passer pour votre organisation en utilisant vos domaines de courrier. Elle vous permettra également de bloquer les courriels d'hameçonnage envoyés à votre organisation.

L'hameçonnage est une méthode d'attaque qu'utilisent couramment les auteurs de menace et qui consiste à envoyer des messages par courriel (ou par l'entremise d'autres modes de communication comme les messages textes ou les appels téléphoniques), de manière à ce qu'ils semblent provenir d'une source de confiance et passent pour des messages légitimes. Les auteurs de menace lancent des attaques par hameçonnage pour inciter les destinataires à divulguer des données personnelles et d'autres renseignements de nature délicate, ou encore pour installer des logiciels malveillants (c'est-à-dire des maliciels) sur des appareils.

Vous pouvez réduire les risques qu'un auteur de menace mène avec succès des campagnes de courriels malveillants en mettant en œuvre les mesures de sécurité techniques décrites dans le présent document. Ces mesures protégeront votre organisation de la façon suivante :

- Empêcher la livraison de messages malveillants qui usurpent vos domaines;
- Dissuader les auteurs de menace de tenter d'usurper les domaines protégés;
- Améliorer la sécurité des destinataires des courriels;
- Protéger la réputation des organisations dont les domaines sont la cible d'usurpation.

2 MÉCANISMES DE PROTECTION DES DOMAINES DE COURRIER

Trois protocoles de sécurité servent conjointement à protéger les domaines de courrier contre l'usurpation :

- Sender Policy Framework (SPF);
- DomainKeys Identified Mail (DKIM);
- Domain-based Message Authentication, Reporting, and Conformance (DMARC).

Pour une protection complète, vous devez mettre en œuvre les trois protocoles et les configurer de manière à indiquer aux destinataires de rejeter les messages non authentiques. Les sections suivantes décrivent ces protocoles. Pour obtenir des conseils sur la mise en œuvre, voir l'annexe A.

2.1 SPF

Le protocole SPF permet de préciser les adresses de protocole Internet (IP pour *Internet Protocol*) à partir desquelles les courriels peuvent être envoyés au nom d'un domaine. La norme SPF est officiellement définie dans la publication *Request for Comments (RFC) 7208: Sender Policy Framework (SPF) for Authorizing Use of Domains in Email* de l'Internet Engineering Task Force (IETF)[1][1].

Vous pouvez mettre en œuvre le protocole SPF en publiant, pour chacun de vos domaines et sous-domaines, un enregistrement dans le système de noms de domaine (DNS pour *Domain Name System*) qui énumère les adresses IP autorisées directement ou en faisant référence à d'autres enregistrements.

Lorsqu'un message est reçu, un système de courrier qui prend en charge le protocole SPF effectue les actions suivantes :

1. Récupérer l'enregistrement SPF associé au domaine d'envoi;
2. Vérifier que l'adresse IP utilisée pour envoyer le message a été autorisée à le faire.

Les messages provenant d'adresses IP non autorisées peuvent être acceptés, marqués comme suspects ou rejetés, selon la stratégie définie dans l'enregistrement SPF.

2.2 DKIM

Le protocole DKIM offre un mécanisme d'authentification des courriels au moyen d'une signature cryptographique. La norme DKIM est officiellement définie dans la publication *RFC 6376: DomainKeys Identified Mail (DKIM) Signatures* de l'IETF [2].

Vous pouvez mettre en œuvre le protocole DKIM comme suit :

1. Pour chaque domaine de courrier, publier au moins un enregistrement DNS constitué d'une clé cryptographique publique et de renseignements supplémentaires;

[1] Les chiffres entre crochets renvoient aux références citées dans la section Contenu complémentaire du présent document.

2. Déployer les clés privées correspondantes aux agents de transfert de courrier (MTA pour *Mail Transfer Agent*) du domaine;
3. Configurer les MTA pour qu'ils signent les messages sortants.

Vous devez configurer chaque MTA au moyen d'une clé privée qui correspond à un enregistrement DKIM publié. Lorsque le MTA envoie un message, il utilise la clé privée pour ajouter une signature cryptographique en insérant un en-tête de message. Si du contenu réutilisable doit être ajouté aux messages sortants, comme un avis de non-responsabilité, il faut le faire avant d'appliquer la signature DKIM. Sinon, la signature sera invalidée.

Lorsqu'un système de courrier qui prend en charge le protocole DKIM reçoit un message comportant une signature DKIM, il récupère l'enregistrement associé à l'en-tête DKIM du message et vérifie la signature à l'aide de la clé publique publiée. Cette vérification confirme sur le plan cryptographique que le message a été envoyé par un expéditeur autorisé et qu'il n'a pas été modifié pendant sa transmission. Si la signature n'est pas valide ou si aucun enregistrement DKIM n'est trouvé, le message échouera à la vérification DKIM et pourrait être rejeté.

2.3 LIMITES DES PROTOCOLES SPF ET DKIM

En raison d'une limite commune, les protocoles SPF et DKIM sont inefficaces devant des auteurs de menace dotés de moyens modérément sophistiqués. En effet, les deux protocoles reposent sur des noms de domaine que ne voit pas l'utilisateur et qui peuvent être différents du domaine qui s'affiche dans le champ d'en-tête `From` (De) d'un courriel (également appelé *header from*). Le protocole SPF utilise le domaine de la commande SMTP HELO ou l'adresse courriel de l'enveloppe (également appelé *envelope from* ou `Return-Path`), qu'utilisent les serveurs de courrier en arrière-plan. Le protocole DKIM utilise le domaine indiqué dans l'en-tête DKIM.

Les domaines utilisés dans les champs d'en-tête *envelope from*, *header from* ou DKIM n'ont pas forcément besoin de se correspondre. Par conséquent, un auteur de menace peut accroître la probabilité que ses courriels malveillants soient livrés en mettant en œuvre les protocoles SPF et DKIM pour un domaine qui est sous son contrôle tout en affichant un domaine différent d'une source de confiance dans le champ `From` (De) du message, dans le but de tromper le destinataire.

Il est à noter que des messages de source légitime peuvent être rejetés par des systèmes de réception si les enregistrements SPF ou DKIM sont manquants ou mal configurés. Comme ces protocoles ne comportent pas de mécanisme de notification, vous ne serez peut-être pas au courant des livraisons qui ont échoué. De même, il n'existe aucun mécanisme permettant aux systèmes de réception d'informer les propriétaires de domaine des messages qui ont été détectés comme étant de source non légitime et rejetés à la suite de l'échec d'une vérification SPF ou DKIM.

2.4 DMARC

Le protocole DMARC a été créé en réponse aux limites des protocoles SPF et DKIM et dans le but d'améliorer la vérification et les rapports. La norme DMARC est définie officiellement dans la publication *RFC 7489: Domain-based Message Authentication, Reporting, and Conformance (DMARC)* de l'IETF [3].

Le protocole DMARC comporte plusieurs améliorations :

- Vérifier que les domaines indiqués dans les champs *envelope from et header from* du protocole SPF correspondent;
- Vérifier que les domaines d'en-tête DKIM et *header from* pour le protocole DKIM correspondent;
- Permettre aux propriétaires de systèmes de préciser les actions qu'un système de réception devrait prendre advenant l'échec des vérifications SPF et DKIM;
- Fournir un mécanisme permettant aux systèmes de réception de communiquer des renseignements sur les résultats des vérifications DMARC aux propriétaires de domaines.

Vous pouvez mettre en œuvre le protocole DMARC en publiant, pour chacun de vos domaines, un enregistrement DNS qui fournira aux systèmes de réception l'information sur la stratégie utilisée.

2.4.1 VALIDATION DMARC

Pour qu'un courriel réussisse la validation DMARC, il doit avoir réussi la vérification SPF ou DKIM, et le domaine utilisé lors de cette vérification doit correspondre à celui qui se trouve dans le champ `From` (De) du courriel. Si un courriel échoue aux vérifications SPF et DKIM, y compris la mise en correspondance des domaines, la validation DMARC échouera à son tour. Le mécanisme qui permet au système de réception de déterminer la stratégie DMARC à appliquer à un message donné est expliqué à la section B.3 de l'annexe B.

Si un courriel réussit la validation DMARC, il est livré. Si la validation DMARC échoue, le système de réception appliquera alors la stratégie précisée dans l'enregistrement DMARC du domaine d'envoi. La stratégie doit correspondre à l'une des options suivantes :

- **Aucune (None)** : Le courriel est livré (c.-à-d. mode surveillance seulement);
- **Mettre en quarantaine (Quarantine)** : Le courriel est livré, mais il est désigné comme étant suspect;
- **Rejeter (Reject)** : Le courriel est rejeté.

Un enregistrement DMARC peut également préciser que la stratégie publiée ne s'appliquera qu'à un pourcentage des messages qui échouent à la validation, pour alors appliquer la stratégie du prochain niveau aux autres. Par exemple, une stratégie de **rejet** de 50 % rejettera 50 % des messages qui échouent, et les 50 % qui restent seront mis en quarantaine.

Bien que les stratégies définies sur **Aucune** et **Mettre en quarantaine** puissent vous aider à recueillir de l'information et à configurer vos systèmes, seule l'application de la stratégie **Rejeter** à 100 % empêchera la livraison de tous les messages de source non légitime.

La figure 1 illustre le processus de validation DMARC.

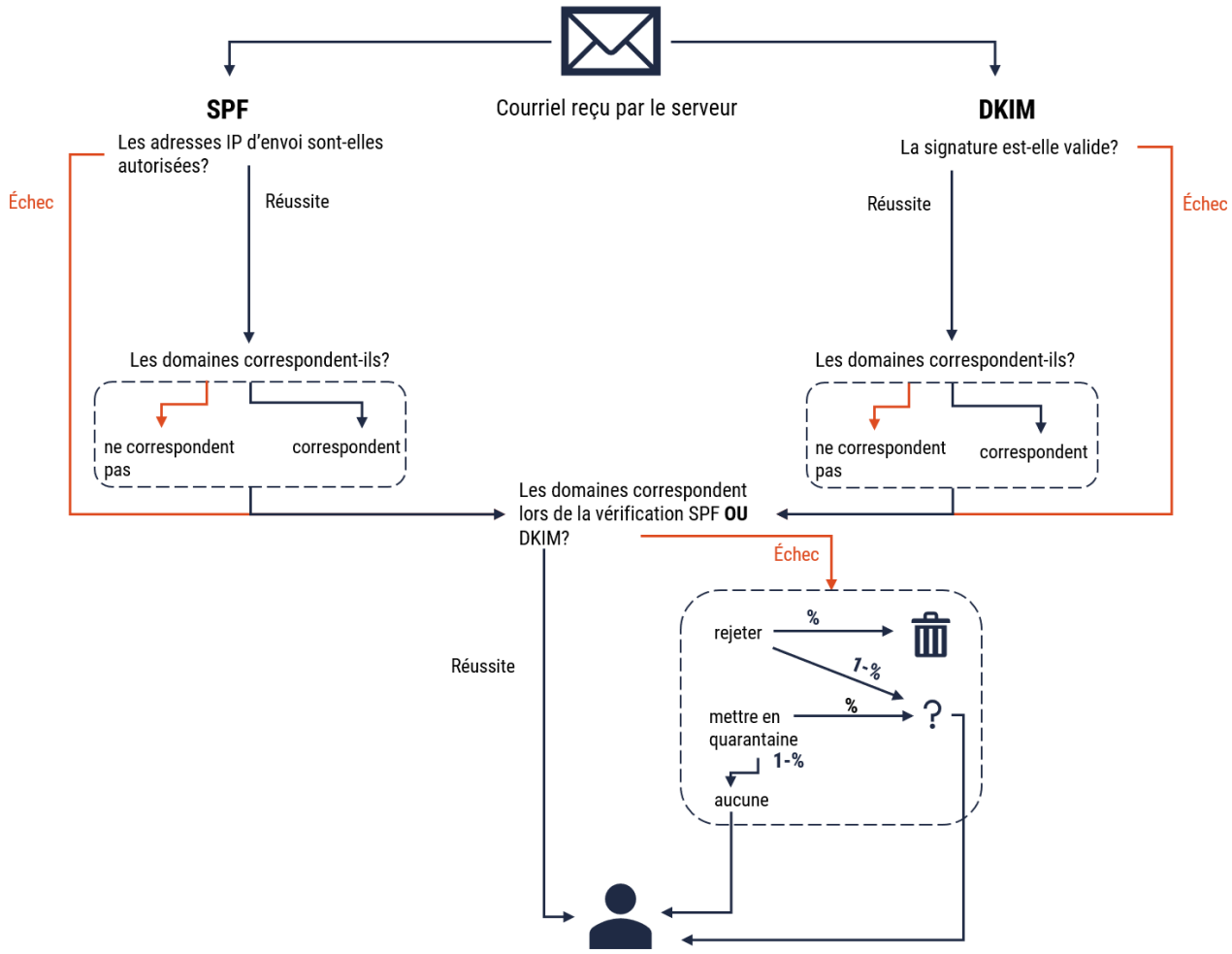

Figure 1 : Validation DMARC

2.4.2 RAPPORTS DMARC

L'un des mécanismes du protocole DMARC permet aux propriétaires de systèmes de recevoir de l'information sur les courriels envoyés qui comportent le nom de l'un de leurs domaines dans le champ `From` (De). Vous pouvez utiliser cette information aux fins suivantes :

- Déterminer les composantes de l'infrastructure de courriel de votre organisation, y compris les expéditeurs tiers;
- Confirmer que les protocoles SPF et DKIM ont été déployés et qu'ils fonctionnent correctement pour vos domaines;
- Confirmer que les courriels envoyés par des utilisateurs légitimes à partir de vos domaines arrivent à destination et que tous les autres sont rejetés;
- Découvrir l'infrastructure utilisée par les auteurs malveillants pour usurper vos noms de domaine.

Les rapports globaux du protocole DMARC sont produits par les systèmes de réception et sont habituellement envoyés une fois par jour aux propriétaires de domaines. Ces rapports sont envoyés sous forme de pièces jointes à l'adresse indiquée dans l'enregistrement DMARC du domaine. Les systèmes de réception de courriel n'envoient pas tous des rapports globaux, mais de nombreux grands fournisseurs de services de messagerie le font.

Les rapports globaux sont produits au format XML (Extensible Markup Language) normalisé et devraient être traités par un système automatisé dans la mesure du possible. Vous pouvez utiliser l'un des nombreux produits de source ouverte, gratuits ou commerciaux pour traiter les rapports DMARC. Des conseils sur l'interprétation de l'information figurant dans les rapports globaux DMARC sont présentés à la section C.2 de l'annexe C.

Certains systèmes de réception peuvent également fournir des rapports d'échec ou de criminalistique constitués de copies des messages qui ont échoué à une ou plusieurs vérifications DMARC. Les propriétaires de systèmes peuvent demander des rapports de criminalistique en réglant certains paramètres dans l'enregistrement DMARC d'un domaine. Toutefois, nous ne recommandons pas aux propriétaires de systèmes de demander des rapports de criminalistique, car ils pourraient contenir de l'information nominative (PII pour *Personally Identifiable Information*).

3 AUTRES CONSIDÉRATIONS

3.1 PRISE EN CHARGE PAR LE FOURNISSEUR

Les fournisseurs de matériel, de logiciels ou de services ne prennent pas tous en charge l'ensemble des fonctionnalités associées aux protocoles SPF, DKIM et DMARC. Il convient de consulter la documentation sur les composantes et les services associés à votre infrastructure afin de déterminer les fonctionnalités prises en charge et les limites potentielles.

Il se peut que les systèmes de réception ne mettent pas pleinement en œuvre les vérifications SPF, DKIM ou DMARC, ou encore qu'ils ne tiennent pas compte de la stratégie publiée par l'organisation. Par exemple, la plupart des systèmes de réception qui envoient des rapports globaux DMARC le font toutes les 24 heures, peu importe la période établie dans la stratégie du domaine d'envoi.

3.2 EXPÉDITEURS TIERS

Lors de la mise en œuvre des protocoles SPF, DKIM et DMARC, il convient de tenir compte des expéditeurs tiers qui ont été autorisés à envoyer des courriels au nom d'un domaine donné.

3.2.1 EXPÉDITEURS TIERS ET PROTOCOLE SPF

Pour que les courriels envoyés par des tiers réussissent la vérification SPF, les adresses IP d'envoi doivent être intégrées dans l'enregistrement SPF du domaine. Pour ce faire, l'enregistrement SPF du domaine doit énumérer les adresses IP ou faire référence à un enregistrement SPF détenu par le tiers.

Il est à noter que le protocole SPF impose une limite de dix recherches DNS par enregistrement. Selon la structure des enregistrements des tiers auxquels on fait référence, cette limite risque d'être dépassée par inadvertance.

3.2.2 EXPÉDITEURS TIERS ET PROTOCOLE DKIM

Pour que les courriels envoyés par des tiers réussissent la vérification DKIM, ils doivent être signés à l'aide d'une clé privée et un enregistrement DKIM correspondant doit avoir été publié pour le domaine. Pour ce faire, les expéditeurs tiers demandent habituellement aux propriétaires de systèmes de publier un enregistrement DKIM qu'ils leur fournissent ou un enregistrement CNAME qui renvoie à un enregistrement DKIM qu'ils détiennent. Dans ce dernier cas, l'expéditeur tiers est généralement responsable de la gestion et de la rotation des clés cryptographiques utilisées, mais en tant que propriétaire du système, vous pouvez aussi demander que la rotation des clés soit effectuée sur demande.

3.2.3 EXPÉDITEURS TIERS ET PROTOCOLE DMARC

Comme il a été mentionné ci-dessus, le protocole DMARC doit confirmer que les domaines des champs *envelope from* et *header from* correspondent pour que les vérifications SPF et DKIM soient considérées comme étant réussies. Des complications risquent de se présenter dans certains cas si des expéditeurs tiers sont utilisés et que les deux domaines ne correspondent pas.

En ce qui concerne la mise en correspondance des domaines pour le protocole DKIM, il suffit de suivre les étapes ci-dessus en utilisant un enregistrement CNAME qui renvoie à un enregistrement DKIM. Pour remédier à un problème de correspondance SPF, vous pouvez créer un sous-domaine désigné qui sera utilisé en tant qu'adresse `Return-Path` personnalisée ainsi qu'un enregistrement CNAME correspondant qui renvoie à un enregistrement SPF détenu par le tiers.

Vous pouvez aussi transférer les rapports DMARC à un tiers aux fins de traitement. Pour ce faire, il suffit d'indiquer l'adresse de courriel d'un tiers dans les paramètres de notification de l'enregistrement DMARC d'un domaine. Dans un tel cas, le tiers doit également publier un enregistrement correspondant indiquant que son domaine accepte les rapports DMARC au nom de votre domaine.

3.2.4 SÉPARATION DE SOUS-DOMAINES

Pour protéger les adresses des utilisateurs contre l'usurpation, vous devriez envisager d'attribuer des sous-domaines dédiés aux expéditeurs tiers autorisés. Par exemple, un tiers pourrait être autorisé à envoyer des messages à partir de `list.domain.example`, mais non `domain.example`. Le tiers ne serait donc pas en mesure d'envoyer un message autorisé d'une adresse d'utilisateur comme `chief.executive@domain.example`, même si son système était compromis.

3.3 TRANSFERT DE MESSAGES

Selon la façon dont le message est traité, le transfert des messages peut parfois entraîner l'échec des vérifications SPF, DKIM ou DMARC. Un utilisateur pourra généralement transférer un message depuis son client de courrier sans problème. Toutefois, des problèmes risquent de se présenter lorsque les systèmes de courrier transfèrent automatiquement des messages. Par exemple, si l'adresse du champ *envelope from* est modifiée, mais que l'adresse *header from* ne l'est pas, la validation ou la mise en correspondance SPF peut échouer. De même, si le contenu sous-jacent de la signature est modifié dans un en-tête DKIM, la validation de la signature échouera.

Vous ne pouvez pas empêcher les messages d'être transférés de cette façon, mais vous devez savoir que les systèmes de réception risquent de rejeter les messages transférés automatiquement dans de tels cas. Les échecs DMARC sont consignés dans les rapports globaux que vous recevez. Il importe d'examiner ces rapports pour évaluer tout problème potentiel.

Dans l'ensemble, le protocole DKIM est mieux adapté au transfert de messages que le protocole SPF. Si le protocole DKIM est déployé correctement, il est plus probable que les messages transférés de source légitime soient bien livrés.

3.3.1 PROTOCOLE ARC (AUTHENTICATED RECEIVED CHAIN)

Le protocole ARC est une norme provisoire qui tente de régler les problèmes causés par les messages transférés. Le protocole ARC est décrit dans le document *RFC 8617: The Authenticated Received Chain (ARC) Protocol* [4], qui a obtenu le statut expérimental en juillet 2019. Le protocole ARC permet à des systèmes intermédiaires de valider les en-têtes d'un courriel associés aux protocoles SPF et DKIM et d'attester de leur validité au moyen d'une signature numérique lors du transfert du message. Les systèmes en aval peuvent se fier à cette chaîne

d'attestations et choisir de transmettre un message même s'il a échoué à la vérification DMARC du système de réception.

Le protocole ARC est une norme émergente. Un certain nombre de grands fournisseurs de services de courriel d'Internet ont toutefois adopté la signature et la validation des messages au moyen du protocole ARC. Par conséquent, vous remarquerez peut-être que le protocole ARC est mentionné dans les rapports DMARC d'un fournisseur, particulièrement lorsque la stratégie DMARC du domaine a été remplacée par une validation ARC fructueuse. De l'information supplémentaire sur le protocole ARC se trouve à la section C.2 de l'annexe C.

3.4 COURRIER ENTRANT

Vous devriez configurer l'infrastructure de courriel de votre organisation de manière à ce qu'elle prenne en charge les mécanismes d'authentification des courriels reçus, notamment :

- Tenter d'effectuer la validation SPF, DKIM et DMARC pour tous les messages reçus;
- Rejeter les messages conformément aux stratégies SPF et DMARC du domaine;
- Conserver le contenu des messages et les en-têtes DKIM lors du transfert des messages;
- Envisager d'envoyer des rapports DMARC globaux aux propriétaires de domaines au sujet des messages reçus.

3.5 CHIFFREMENT DE COURRIELS DANS LA COUCHE TRANSPORT

Dans le passé, le trafic réseau transitant entre les serveurs de courrier n'était pas chiffré, ce qui le rendait vulnérable à l'interception ou à la modification pendant sa transmission. Au fil du temps, plusieurs protocoles ont été créés pour chiffrer le trafic de courrier.

3.5.1 STARTTLS

En 2002, le protocole de transfert de courrier simple (SMTP pour *Simple Mail Transfer Protocol*) a été élargi afin de permettre le chiffrement opportuniste au moyen d'une commande STARTTLS. Vous devriez configurer les MTA de votre organisation de manière à prendre en charge STARTTLS et à exiger son utilisation. Toutefois, un attaquant disposant d'un accès privilégié sur un réseau pourrait empêcher l'exécution de cette commande, ce qui limiterait l'efficacité de cette approche.

3.5.2 PROTOCOLE DANE (DNS-BASED AUTHENTICATION OF NAMED ENTITIES)

Le protocole DANE a été lancé en 2012 dans le but de permettre aux propriétaires de systèmes de lier les certificats du protocole de sécurité de la couche transport (TLS pour *Transport Layer Security*) aux noms de domaine sans passer par une autorité de certification centrale. En réponse aux limites de STARTTLS, la publication *RFC 7672: SMTP Security via Opportunistic DANE TLS* [5] propose l'application du protocole DANE au trafic SMTP, ce qui permet aux propriétaires de systèmes d'exiger le chiffrement du trafic transmis aux serveurs de courrier de leur domaine.

Pour déployer le protocole DANE, vous devez également adopter au préalable les extensions de sécurité du système de noms de domaine (DNSSEC pour *Domain Name System Security Extensions*). Les propriétaires de systèmes qui ont activé le protocole DNSSEC pour leur domaine peuvent mettre en œuvre le protocole DANE en publiant un enregistrement TLSA (*TLS Authentication*) pour le protocole DANE dans le système DNS. Comme le protocole DMARC, le protocole DANE prend en charge l'envoi de rapports globaux aux propriétaires de systèmes.

3.5.3 PROTOCOLE MTA-STS (*MTA STRICT TRANSPORT SECURITY*)

Comme solution de rechange au protocole DANE, vous pouvez mettre en œuvre le mécanisme MTA-STS pour le protocole SMTP, une norme émergente qui prend en charge le chiffrement strict sans avoir recours au protocole DNSSEC. Le protocole MTA-STS vous permet d'exiger que le trafic de courrier envoyé à un domaine soit chiffré avec une clé publique spécifique.

Bien qu'ils atteignent le même objectif, les protocoles DANE et MTA-STS sont compatibles et peuvent être mis en œuvre en parallèle. Pour mettre en œuvre le protocole MTA-STS, il faut déployer des certificats TLS signés sur les serveurs Web et de courrier d'un domaine, publier une stratégie MTA-STS sur le serveur Web et publier des enregistrements MTA-STS dans le système DNS. Tout comme le protocole DMARC, le protocole MTA-STS prend en charge l'envoi de rapports globaux aux propriétaires de systèmes.

3.6 DOMAINES AUTRES QUE LES DOMAINES DE COURRIER

En ce qui concerne les domaines qui ne sont pas utilisés ou ceux qui ne servent pas à envoyer des courriels, il convient de créer les enregistrements DNS nécessaires afin de les protéger contre l'usurpation. Des conseils sur la création d'enregistrements DNS pour les domaines autres que les domaines de courrier se trouvent à la section B.4 de l'annexe B.

3.7 BRAND INDICATORS FOR MESSAGE IDENTIFICATION (BIMI)

La norme BIMI (indicateurs de marque pour l'identification du message) est une norme émergente qui permettra aux propriétaires de systèmes de fournir une image, habituellement le logo d'une organisation, que les clients de messagerie afficheront à côté des messages authentifiés pour que les utilisateurs les reconnaissent. Pour être autorisé à utiliser la norme BIMI, un domaine doit avoir pleinement mis en œuvre le protocole DMARC et avoir configuré une stratégie de **rejet**. La norme BIMI n'est pas encore adoptée à grande échelle, mais son développement est soutenu par de nombreux intervenants importants dans le domaine du courrier électronique.

4 RÉSUMÉ

Vous pouvez suivre les conseils formulés dans le présent document pour mettre en œuvre des mesures de sécurité techniques afin de protéger les domaines de votre organisation contre l'usurpation d'adresse électronique. En mettant en œuvre les protocoles SPF, DKIM et DMARC, vous pouvez réduire les risques qu'un auteur de menace réussisse à mener des campagnes de courriels malveillants en exploitant la réputation de votre organisation.

L'annexe A du présent document fournit des conseils sur la façon de mettre en œuvre ces trois protocoles de sécurité, l'annexe B comprend une référence sur les protocoles et l'annexe C explique comment analyser l'information sur les courriels.

4.1 COORDONNÉES

Pour obtenir de plus amples renseignements sur la mise en œuvre de mesures de protection pour les domaines de courrier, communiquez avec notre centre d'appel par courriel ou par téléphone :

Centre d'appel du Centre pour la cybersécurité
contact@cyber.gc.ca
613-949-7048 ou 1-833-CYBER-88

5 CONTENU COMPLÉMENTAIRE

5.1 ABRÉVIATIONS, ACRONYMES ET SIGLES

Forme abrégée	Expression au long
A	Enregistrement DNS d'un hôte (IPv4)
ARC	Protocole ARC (*Authenticated Received Chain*)
BIMI	Indicateurs de marque pour l'identification du message (*Brand Indicators for Message Identification*)
CST	Centre de la sécurité des télécommunications
DANE	Protocole DANE (*DNS-based Authentication of Named Entities*)
DKIM	Protocole DKIM (*DomainKeys Identified Mail*)
DMARC	Protocole DMARC (*Domain-based Message Authentication, Reporting, and Conformance*)
DNS	Système de noms de domaine (*Domain Name System*)
DNSSEC	Extensions de sécurité du système de noms de domaine (*Domain Name System Security Extensions*)
GC	Gouvernement du Canada
IETF	Internet Engineering Task Force
IP	Protocole IP (*Internet Protocol*)
MTA	Agent de transfert de courrier (*Mail Transfer Agent*)
MTA-STS	Protocole MTA-STS (*SMTP MTA Strict Transport Security*)
MX	Enregistrement Mail Exchanger du système DNS
PII	Information nominative (*Personally Identifiable Information*)
RFC	Demande de commentaires (*Request for Comments*)
SMTP	Protocole de transfert de courrier simple (*Simple Mail Transfer Protocol*)
SPF	Protocole SPF (*Sender Policy Framework*)
TLD	Domaine de premier niveau (*Top-level Domain*)
TLS	Protocole de sécurité de la couche transport (*Transport Layer Security*)
TLSA	Authentification TLS (Transport Layer Security Authentication)
TTL	Durée de vie (*Time to Live*)
TXT	Enregistrement texte du système DNS
XML	Langage XML (*Extensible Markup Language*)

5.2 RÉFÉRENCES

Numéro	Référence
1	Internet Engineering Task Force. *RFC 7208 Sender Policy Framework (SPF) for Authorizing Use of Domains in Email, Version 1*, avril 2014.
2	Internet Engineering Task Force. *RFC 6376 DomainKeys Identified Mail (DKIM) Signatures,* septembre 2011.
3	Internet Engineering Task Force. *RFC 7489 Domain-based Message Authentication, Reporting, and Conformance (DMARC),* mars 2015.
4	Internet Engineering Task Force. *RFC 8617 The Authenticated Received Chain Protocol (ARC) Protocol*, juillet 2019.
5	Internet Engineering Task Force. *RFC 7672 SMTP Security via Opportunistic Domain-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS)*, octobre 2015.
6	Mozilla Foundation. *Public Suffix List*. https://publicsuffix.org/
7	Internet Engineering Task Force. *RFC 8601 Message Header Field for Indicating Message Authentication Status*, mai 2019.
8	National Institute of Standards and Technology. *SP 800-177 Rev. 1 Trustworthy Email*, février 2019.

Annexe 1Plan de mise en œuvre

1.1 Vue d'ensemble

Pour mettre en œuvre les protocoles SPF, DKIM et DMARC, vous devrez suivre plusieurs étapes. Pour minimiser les perturbations potentielles, nous vous recommandons de respecter l'ordre ci-dessous. Des précisions sont données sur chaque étape dans les sous-sections de la présente annexe.

1. **Évaluer :**
    a. Déterminer tous les domaines et sous-domaines utilisés pour envoyer des courriels;
    b. Évaluer l'état actuel;
    c. Déployer les enregistrements DMARC initiaux en utilisant la stratégie **Aucune (None)**;
    d. Recueillir et analyser les rapports DMARC.
2. **Déployer :**
    a. Déterminer tous les expéditeurs autorisés;
    b. Déployer les enregistrements SPF pour tous les domaines;
    c. Déployer les enregistrements DKIM et les clés pour tous les domaines et expéditeurs;
    d. Surveiller les rapports DMARC et corriger les erreurs de configuration.
3. **Mettre en application :**
    a. Faire passer la stratégie DMARC à **Mettre en quarantaine (Quarantine)**;
    b. Faire passer la stratégie DMARC à **Rejeter (Reject)**;
    c. Rejeter tous les messages provenant de domaines autres que les domaines de courrier.
4. **Assurer la maintenance :**
    a. Surveiller les rapports DMARC;
    b. Corriger les erreurs de configuration et mettre à jour les enregistrements au besoin;
    c. Effectuer la rotation des clés DKIM annuellement.

1.2 Évaluer

1.2.1 Déterminer les domaines de courrier

Dressez la liste de tous les domaines et sous-domaines qu'utilise votre organisation pour envoyer des courriels. Vous pouvez trouver cette information en consultant les sources ci-dessous :

- Enregistrements DNS existants de type MX;
- Journaux liés au trafic réseau sur les ports 25 ou 587 (généralement utilisés pour le protocole SMTP);
- Administrateurs de courriel.

1.2.2 Évaluer l'état actuel

Une fois que vous avez déterminé les domaines employés, utilisez les outils DNS pour évaluer l'état actuel du déploiement des protocoles SPF, DKIM et DMARC pour chacun des domaines.

Il est à noter que vous ne pourrez pas effectuer des tests de cette façon pour les enregistrements DKIM à moins de connaître la chaîne de sélecteurs correspondante, que vous pouvez trouver dans l'en-tête`DKIM-Signature` d'un message envoyé à partir du domaine (voir la section C.1 de l'annexe C pour en savoir plus sur les en-têtes de courrier). Certains fournisseurs de services de courriel utilisent également des sélecteurs courants pour tous leurs clients.

Examinez les enregistrements générés par les tests pour vous assurer qu'ils sont exacts (voir l'annexe B pour en savoir plus sur la structure et le contenu requis). Il existe de nombreux outils en ligne qui permettent d'évaluer l'état d'un nom de domaine donné, notamment en validant l'exactitude des enregistrements générés.

Vous pouvez utiliser les commandes `dig` suivantes pour récupérer les enregistrements existants pour chaque protocole :

- **SPF :** `dig +short -t txt domain.example`
- **DKIM :** `dig +short -t txt selector._domainkey.domain.example`
- **DMARC :** `dig +short -t txt _dmarc.domain.example`

1.2.3 Déployer l'enregistrement DMARC initial

Déployez un enregistrement DMARC initial pour chaque domaine et sous-domaine utilisé pour envoyer des courriels. En déployant un enregistrement DMARC initial avec la stratégie **Aucune (None)**, vous pourrez commencer à recevoir immédiatement des rapports DMARC, même avant le déploiement des protocoles SPF ou DKIM. L'enregistrement initial n'a aucune incidence sur la livraison du courrier, mais il permet de demander aux systèmes de réception de vous envoyer des rapports DMARC globaux, à vous ou à un tiers désigné. Ces rapports peuvent vous guider dans le déploiement des protocoles SPF et DKIM et vous permettre de découvrir des infrastructures de messagerie que vous ne connaissiez peut-être pas.

Votre organisation devra indiquer l'adresse électronique à laquelle envoyer les rapports. Il devrait s'agir d'une boîte aux lettres générique réservée à cette fin (p. ex., `dmarc@domain.example`) plutôt que celle d'une personne.

Nous recommandons à votre organisation de configurer son enregistrement DMARC initial comme suit :

```
v=DMARC1; p=none; sp=none; rua=mailto:dmarc@domain.example
```

Dans l'enregistrement, vous pouvez indiquer l'adresse électronique d'un tiers pour que les rapports lui soient envoyés. Pour recevoir ces rapports, le propriétaire du domaine tiers doit également publier un enregistrement DMARC indiquant qu'il accepte les rapports au nom du domaine en question.

Vous pouvez inscrire deux adresses, mais certains expéditeurs ne peuvent envoyer des rapports qu'à la première adresse indiquée. Voici un exemple d'un tel enregistrement :

```
v=DMARC1; p=none; sp=none;
rua=mailto:dmarc@thirdparty.example,mailto:dmarc@domain.example
```

1.2.4 Recueillir et analyser les rapports DMARC

Dans les 24 heures suivant la publication d'un premier enregistrement DMARC, vous devriez commencer à recevoir des rapports globaux de systèmes qui ont reçu des courriels en provenance du domaine de votre organisation. Surveillez les rapports DMARC reçus tout au long du processus de déploiement, car ils contiennent des renseignements qui vous seront très utiles.

Les rapports DMARC globaux sont générés au format XML normalisé et devraient être traités par un système automatisé. De nombreux produits de source ouverte, gratuits et commerciaux sont offerts pour traiter les rapports DMARC.

Lorsque vous analysez les rapports DMARC à cette étape, il convient de porter une attention particulière aux éléments suivants :

- **Sous-domaines** : Déterminez les sous-domaines utilisés pour envoyer des courriels et vérifiez si les protocoles SPF, DKIM ou DMARC sont configurés pour ces sous-domaines.
- **Adresses IP internes** : Déterminez les adresses IP internes qui sont utilisées pour envoyer des courriels et vérifiez si les messages envoyés réussissent la mise en correspondance des domaines pour les protocoles SPF et DKIM.
- **Adresses IP externes** : Déterminez les adresses IP externes utilisées pour envoyer des courriels et utilisez des outils de recherche DNS inversée et le service WHOIS pour recueillir des renseignements supplémentaires à leur sujet. Tentez de classer ces adresses selon les catégories suivantes :
  - **Expéditeurs autorisés** : Il s'agit des tiers autorisés à envoyer des courriels au nom de votre organisation. Vérifiez que les messages envoyés réussissent la mise en correspondance des domaines pour les protocoles SPF et DKIM.
  - **Serveurs de redirection / serveurs relais** : Certains serveurs de courrier, comme ceux qui prennent en charge les listes de diffusion, peuvent être configurés pour transférer automatiquement les messages. Ces messages transférés peuvent échouer aux vérifications SPF et DKIM à la réception, mais ils sont inoffensifs.
  - **Usurpation possible** : Il se peut que des adresses IP qui ne font pas partie de l'une des catégories ci-dessus envoient des messages non autorisés en usurpant le domaine de votre organisation. Les

adresses IP qui figurent sur les listes de rejet publiques de pourriels sont plus susceptibles de rentrer dans cette catégorie.

Des conseils supplémentaires sur l'analyse des rapports DMARC sont présentés à l'annexe C.

1.3 Déployer

1.3.1 Déterminer les expéditeurs autorisés

En analysant les rapports DMARC que vous recevez, vous pourrez déterminer tous les expéditeurs autorisés, y compris les sous-domaines et les adresses IP. Il s'agira sans doute d'infrastructure interne, mais la liste peut également comprendre les services de messagerie basés sur le nuage ou les expéditeurs tiers.

Vous devrez peut-être consulter les personnes responsables d'autres services au sein de votre organisation pour confirmer si certains expéditeurs (p. ex., une entreprise tierce chargée d'envoyer des courriels de marketing) sont autorisés.

1.3.2 Configurer la durée de vie (TTL) des enregistrements DNS

Les enregistrements DNS sont mis en cache pour une période appelée « durée de vie » (TTL pour *Time to Live*), exprimée en secondes. Lors des étapes du déploiement et de la mise en application, vous devriez utiliser une TTL de 30 minutes (1 800 secondes) pour les nouveaux enregistrements ou les enregistrements modifiés. Cette pratique évitera que des erreurs commises par inadvertance persistent dans les caches DNS pendant trop longtemps avant d'être remplacées par une version corrigée.

Lorsque vous modifiez un enregistrement existant, vous devriez d'abord faire passer la TTL à 30 minutes et permettre à la TTL précédente de s'écouler. Le nouvel enregistrement remplacera ainsi l'ancienne version dans tous les caches au bout de 30 minutes.

Vous devriez utiliser une TTL de 24 heures (86 400 secondes) pour les enregistrements stables.

1.3.3 Déployer le protocole SPF pour tous les domaines

Pour chaque domaine et sous-domaine qui envoie des courriels, déployez les enregistrements SPF dans l'ordre suivant :

1. Créez un enregistrement SPF en suivant les directives à l'annexe B.
   Remarque : L'enregistrement doit indiquer toutes les adresses IP autorisées, directement ou par référence.
2. Publiez l'enregistrement dans le système DNS.

1.3.4 Déployer le protocole DKIM pour tous les domaines et expéditeurs

Pour chaque domaine qui envoie des courriels, déployez les clés et enregistrements DKIM dans l'ordre suivant :

1. Générez ou obtenez des clés cryptographiques pour le protocole DKIM par l'une des méthodes suivantes :
   a. Certains MTA peuvent générer des paires de clés DKIM directement et produire la clé publique.
   b. Vous pouvez générer des paires de clés à l'aide d'un outil comme OpenSSL comme suit :

```
openssl genrsa -out private2048.key 2048

openssl rsa -in private2048.key -pubout-out public2048.key
```

c. Les expéditeurs tiers qui gèrent les clés DKIM à l'interne pourraient vous fournir une clé publique.

Remarque : Les paires de clés doivent satisfaire aux exigences cryptographiques précisées à l'annexe B.

2. Utilisez la ou les clés publiques pour créer les enregistrements DKIM conformément à l'annexe B.
3. Déterminez les chaînes à utiliser comme sélecteurs DKIM ou obtenez les sélecteurs précisés auprès d'un tiers.
4. Publiez les enregistrements DKIM dans le système DNS.
5. Prenez les mesures suivantes pour chaque MTA :
    a. Configurez une clé privée et le sélecteur correspondant à utiliser pour le protocole DKIM.
    b. Activez la signature DKIM pour les messages sortants.

1.3.5 Surveiller les rapports DMARC et corriger les erreurs de configuration

Une fois que vous avez déployé les enregistrements SPF et DKIM, surveillez les rapports DMARC que vous recevez pour détecter toute erreur ou tout oubli. Dans les rapports, prêtez une attention particulière aux messages envoyés par des expéditeurs autorisés qui auraient échoué à la mise en correspondance des domaines pour le protocole SPF ou DKIM. Corrigez toute erreur de configuration.

1.4 Mettre en application

Lorsque vous êtes convaincu que le déploiement des protocoles SPF et DKIM est terminé au sein de votre organisation et que toutes les erreurs de configuration ont été corrigées, vous pouvez passer à l'étape de la mise en application. Cette stratégie indique aux systèmes de réception du courrier de ne livrer que les messages qui réussissent l'authentification DMARC (c.-à-d. qui réussissent la mise en correspondance des domaines lors de la vérification SPF ou DKIM) et de mettre en quarantaine ou de rejeter les messages qui échouent à l'authentification DMARC (c.-à-d. qui échouent à la mise en correspondance des domaines lors de la vérification SPF et DKIM).

La stratégie d'application pour un domaine donné doit être précisée au moyen de la balise `p` dans l'enregistrement DMARC et doit correspondre à l'un des trois niveaux suivants, du moins strict au plus strict :

- **Aucune (None)** : Tous les messages sont livrés (c.-à-d. en mode surveillance seulement).
- **Mettre en quarantaine (Quarantine)** : Les messages qui échouent à l'authentification DMARC sont livrés, mais sont désignés comme étant suspects.
- **Rejeter (Reject)** : Les messages qui échouent à l'authentification DMARC sont refusés.

Les rapports DMARC indiqueront dans le champ *Disposition* la stratégie qui a été appliquée à un ensemble particulier de messages.

1.4.1 Renforcer progressivement la mise en application

Vous devriez progressivement mettre en œuvre une stratégie d'application de plus en plus stricte, qui passera du niveau de base **Aucune**, à **Mettre en quarantaine**, et enfin à **Rejeter**.

1. Utilisez la série d'enregistrements DMARC ci-dessous :
    a. `v=DMARC1; p=none; rua=mailto:dmarc@domain.example`
    b. `v=DMARC1; p=quarantine; pct=100; rua=mailto:dmarc@domain.example`
    c. `v=DMARC1; p=reject; pct=100; rua=mailto:dmarc@domain.example`
2. À chaque étape, surveillez les rapports DMARC pour vous assurer que les messages de source légitime ne sont pas mis en quarantaine.
3. Il conviendra de corriger toute erreur détectée et de confirmer que c'est bien fait dans les rapports ultérieurs avant d'appliquer la prochaine valeur.

En plus de définir le niveau d'application, la stratégie DMARC peut préciser à quel pourcentage de messages ayant échoué à la vérification la stratégie s'appliquera, le niveau inférieur s'appliquant au reste. Pour ce faire, vous pouvez utiliser la balise facultative `pct` dans l'enregistrement DMARC pour que la progression soit encore plus précise.

Par exemple, une stratégie **Mettre en quarantaine** associée à un pourcentage de 50 % indiquera à un système de réception de mettre en quarantaine 50 % des messages qui ont échoué et de livrer les autres 50 %.
L'enregistrement DMARC serait donc établi comme suit :

```
v=DMARC1; p=quarantine; pct=50; rua=mailto:dmarc@domain.example
```

1.4.2 Exceptions liées aux sous-domaines

Si des sous-domaines du domaine racine sont utilisés pour envoyer des courriels et nécessitent une configuration différente du domaine organisationnel, vous pouvez les configurer à l'aide d'un enregistrement DMARC unique. Cet enregistrement aura préséance sur celui du domaine organisationnel. Cette pratique peut être utile dans les cas où l'établissement de la conformité SPF et DKIM d'un sous-domaine particulier prend plus de temps que le domaine organisationnel. Dans l'intervalle, le sous-domaine peut rester temporairement à un niveau d'application inférieur afin de permettre au domaine organisationnel (et à d'autres sous-domaines) de prendre préséance.

Dans le cas des sous-domaines qui n'ont pas d'enregistrement DMARC, la stratégie du domaine organisationnel s'appliquera. La stratégie précisée par la balise `sp` sera appliquée si elle est présente; autrement, la stratégie comportant la balise `p` sera appliquée.

Des considérations particulières liées aux enregistrements DMARC et aux sous-domaines se trouvent à la section B.3 de l'annexe B.

1.4.3 Domaines autres que les domaines de courrier

Après avoir déployé le protocole DMARC pour tous les domaines de courrier, vous devriez également déployer des enregistrements SPF et DMARC afin de protéger les domaines qui n'envoient pas de courrier. Ces enregistrements indiqueront que les messages reçus depuis ces domaines ne proviennent pas d'une source légitime et qu'ils doivent être rejetés. Les enregistrements recommandés pour ces domaines sont présentés à la section B.4 de l'annexe B.

1.5 Assurer la maintenance

1.5.1 Surveiller les rapports DMARC

Une fois que les protocoles SPF, DKIM et DMARC sont déployés, vous devriez surveiller les rapports DMARC pour détecter tout changement. Portez une attention particulière aux éléments suivants :

- Une augmentation du nombre de messages qui échouent à la mise en correspondance des domaines lors de la vérification SPF ou DKIM;
- L'utilisation de nouveaux sous-domaines;
- L'utilisation de nouvelles adresses IP internes;
- L'utilisation continue de nouvelles adresses IP externes, ce qui peut indiquer la présence de nouveaux expéditeurs tiers;
- Le volume de messages associés à l'usurpation de domaine soupçonnée.

1.5.2 Corriger les erreurs de configuration et mettre les enregistrements à jour

À mesure que des changements sont apportés à l'infrastructure et que des erreurs de configuration sont détectées, vous devrez modifier périodiquement les enregistrements SPF, DKIM et DMARC. Vous pourriez également devoir déployer de nouveaux enregistrements en réponse aux changements apportés à la structure de domaine de votre organisation.

Comme les enregistrements SPF sont liés aux adresses IP, ils risquent de nécessiter un suivi plus rigoureux. L'utilisation d'enregistrements CNAME ou de balises `include` pour les expéditeurs tiers et `a` ou `mx` pour l'infrastructure interne peut aider à protéger les enregistrements SPF contre ces types de changements, car ils ne sont pas associés directement à des adresses IP. De même, vous pourriez devoir ajouter ou modifier des enregistrements DKIM à mesure que vous ajoutez ou retirez des expéditeurs autorisés ou des MTA.

Une fois que votre organisation aura pleinement mis en œuvre la stratégie **Rejeter**, les enregistrements DMARC devraient demeurer assez stables.

1.5.3 Assurer la rotation des clés DKIM

Pour vous protéger contre la compromission d'une ou de plusieurs clés privées, vous devriez faire une rotation annuelle des paires de clés DKIM. Pour effectuer la rotation des paires de clés que vous gérez, suivez les étapes ci-dessous :

1. Générez de nouvelles paires de clés;
2. Choisissez ou obtenez de nouveaux sélecteurs;
3. Préparez et publiez de nouveaux enregistrements avec les clés publiques;
4. Configurez les MTA pour qu'ils utilisent les nouvelles clés privées et les nouveaux sélecteurs;
5. Supprimez les anciens enregistrements au bout d'une semaine.

Vérifiez la politique de rotation des clés adoptée par les expéditeurs tiers et assurez-vous qu'ils effectuent la rotation de leurs clés au moins une fois par année.

Annexe 2Référence sur les protocoles

2.1 SPF

2.1.1 Enregistrements SPF

Les enregistrements SPF sont publiés sous forme d'enregistrements TXT à la racine d'un domaine d'envoi et pour chaque sous-domaine. Chaque enregistrement comprend la liste de toutes les adresses IP qui sont autorisées à envoyer des courriels au nom du domaine, soit directement, soit en renvoyant à d'autres enregistrements DNS qui contiennent ces adresses.

Les enregistrements SPF stables devraient avoir une longue durée de vie (TTL), comme 24 heures (86 400 secondes).

Les éléments des enregistrements SPF doivent être séparés par des espaces, et ils sont présumés être positifs ou permissifs s'ils ne sont pas précédés d'un caractère modificateur (p. ex., –) indiquant le contraire. Un enregistrement SPF typique pour le domaine `domain.example` serait :

```
v=spf1 mx a:mail.domain.example include:spf.third-party.example -all
```

Le tableau 1 décrit les éléments les plus courants d'un enregistrement SPF.

Tableau 1 : Éléments d'un enregistrement SPF

Élément	Description
`v=spf1`	En-tête obligatoire d'un enregistrement SPF.
`mx`	Inclut tout enregistrement MX (courrier) publié pour le domaine. Il peut être associé à un domaine ou nom d'hôte particulier en utilisant la formule « `a:host1.domain.example` ».
`a`	Inclut tout enregistrement A (adresse IPv4) ou AAAA (adresse IPv6) publié pour le domaine. Il peut être associé à un domaine ou nom d'hôte particulier en utilisant la formule « `a:host1.domain.example` ».
`ip4`	Adresse ou plage d'adresses IPv4, p. ex., `ip4:192.0.2.0/24`.
`ip6`	Adresse ou plage d'adresses IPv6, p. ex., `ip6:2001:DB8::/32`.
`include`	Inclut les enregistrements SPF publiés à un autre emplacement DNS. Sert habituellement à autoriser les expéditeurs tiers.
`-all`	Exclut toutes les autres adresses IP. Devrait être le dernier élément d'un enregistrement pour indiquer que tous les autres expéditeurs ne sont pas autorisés.

2.1.2 Expéditeurs tiers

L'infrastructure d'un tiers est habituellement autorisée au moyen de la clause `include`, qui indique au serveur de réception du courrier d'inclure tous les enregistrements SPF trouvés à l'emplacement précisé. Par exemple :

```
include:spf.third-party.example
```

2.1.3 Limite de recherches DNS

Une limite de 10 recherches DNS par enregistrement s'applique au protocole SPF. Si des énoncés `include` sont utilisés pour plusieurs expéditeurs tiers, on risque de dépasser par inadvertance cette limite, surtout si les enregistrements inclus comportent eux aussi des énoncés `include`.

Pour contourner cette limite, on peut séparer les expéditeurs tiers en fonction de sous-domaines distincts. Les enregistrements SPF pour chacun des sous-domaines nécessiteront ainsi moins d'éléments SPF et de recherches connexes comparativement à un enregistrement combiné.

2.2 DKIM

2.2.1 Enregistrements DKIM

Les enregistrements DKIM sont des enregistrements TXT précisés par une chaîne de sélecteurs. Ils sont créés sous un emplacement `_domainkey`, à un niveau inférieur au domaine associé. Par exemple, l'emplacement d'un enregistrement DKIM pour le domaine `domain.example` avec le sélecteur `abc` est `abc._domainkey.domain.example`. Nous recommandons d'inclure dans le sélecteur la date à laquelle la paire de clés a été générée à titre de rappel sur la période de rotation des clés.

Les enregistrements DKIM stables devraient avoir une longue durée de vie (TTL), comme 24 heures (86 400 secondes).

Les éléments des enregistrements DKIM doivent être séparés par des points-virgules. Le tableau 2 décrit les éléments typiques d'un enregistrement DKIM.

Tableau 2 : Éléments d'un enregistrement DKIM

Élément	Description
`v=DKIM1`	En-tête obligatoire d'un enregistrement DKIM.
`p`	Valeur de la clé publique

2.2.2 Considérations cryptographiques

Vous devriez configurer le protocole DKIM pour qu'il utilise l'algorithme RSA-SHA256 et vous devriez utiliser des clés d'une longueur de 2048 bits. Si une appliance ou un service ne prend pas en charge les clés de 2048 bits, vous devriez utiliser des clés de 1024 bits.

Veuillez noter que, comme les clés de 2048 bits dépassent la limite de 255 caractères d'un seul enregistrement TXT, elles doivent chevaucher deux enregistrements adjacents et n'inclure aucune espace supplémentaire. Vous devriez également vous assurer de supprimer tout caractère de nouvelle ligne non visible à la fin des chaînes d'enregistrements.

Pour réduire les risques associés à la compromission d'une clé privée, utilisez des paires de clés DKIM uniques en suivant les directives ci-dessous :

- Utilisez une paire de clés unique, au minimum, pour chaque domaine.
- Utilisez des paires de clés uniques dans tous les cas où un tiers gère la clé privée.
- Utilisez une paire de clés unique pour chaque MTA, si possible.

Il convient de faire une rotation annuelle des clés DKIM conformément aux précisions données à l'annexe A.

2.2.3 Expéditeurs tiers

L'infrastructure d'expéditeurs tiers est habituellement autorisée par un sélecteur spécifique associé à la paire de clés utilisée par l'expéditeur. Dans certains cas, l'expéditeur tiers peut gérer les clés et vous fournir la clé publique et le sélecteur à utiliser dans un enregistrement DKIM correspondant. Autrement, l'expéditeur tiers peut vous fournir un emplacement DNS que vous pourrez publier en tant qu'enregistrement CNAME sous votre domaine et qui renverra à l'enregistrement DKIM du tiers.

Certains expéditeurs tiers feront automatiquement la rotation des clés DKIM qu'ils gèrent, tandis que d'autres ne le feront qu'à la suite d'une intervention du propriétaire du système.

2.3 DMARC

2.3.1 Enregistrements DMARC

Les enregistrements DMARC sont des enregistrements TXT créés à l'emplacement `_dmarc` sous le domaine associé (c.-à-d. `_dmarc.domain.example`).

Les enregistrements DMARC stables devraient avoir une longue durée de vie (TTL), comme 24 heures (86 400 secondes).

Les éléments de l'enregistrement DMARC doivent être séparés par des points-virgules. Le tableau 3 présente les éléments typiques d'un enregistrement DMARC.

Tableau 3 : Éléments d'un enregistrement DMARC

Élément	Exigence	Description
`v=DMARC1`	Obligatoire	En-tête obligatoire d'un enregistrement DMARC.
`p`	Obligatoire	Stratégie à appliquer aux messages qui échouent à la vérification DMARC. Les seules valeurs possibles sont : « none » (aucune), « quarantine » (mettre en quarantaine) ou « reject » (rejeter).
`aspf`	Facultatif	Précise si la mise en correspondance des noms de domaine aux fins de la vérification SPF doit être souple ou stricte. La mise en correspondance est souple par défaut, ce qui est recommandé dans la plupart des cas.
`adkim`	Facultatif	Précise si la mise en correspondance des noms de domaine aux fins de la vérification DKIM doit être souple ou stricte. La mise en correspondance est souple par défaut, ce qui est recommandé dans la plupart des cas.
`sp`	Facultatif	Stratégie à appliquer aux sous-domaines qui n'ont pas leur propre enregistrement DMARC. Les seules valeurs possibles sont : « none » (aucune), « quarantine » (mettre en quarantaine) ou « reject » (rejeter). Cette balise s'applique uniquement aux enregistrements de domaines organisationnels (c.-à-d. les domaines directement sous un domaine publié dans la liste de suffixes publics [6]). Elle ne sera pas prise en compte à tous les autres niveaux de la hiérarchie du domaine. En son absence, la valeur de la balise `p` sera utilisée pour les sous-domaines.
`pct`	Facultatif	Pourcentage de messages rejetés auxquels les paramètres « quarantine » ou « reject » s'appliquent. Le niveau inférieur suivant de la stratégie s'appliquera au reste, c'est-à-dire « none » au lieu de « quarantine » ou « quarantine » au lieu de « reject ». Il doit s'agir d'un nombre entier entre 1 et 100. En son absence, la valeur de 100 est appliquée par défaut.
`rua`	Facultatif	Adresses auxquelles les rapports globaux doivent être envoyés. Un maximum de deux adresses peuvent être précisées; elles doivent être séparées par des virgules et chacune doit être précédée par `mailto:`. On encourage fortement l'utilisation de cette balise.
`ruf`	Facultatif	Adresses auxquelles les rapports de criminalistique ou d'échec doivent être envoyés. L'utilisation de cette balise n'est pas recommandée, car elle risque de recueillir des communications privées.

Nous recommandons l'enregistrement ci-dessous comme enregistrement DMARC initial (en indiquant l'adresse à laquelle vous souhaitez recevoir les rapports) :

```
v=DMARC1; p=none; sp=none; rua=mailto:dmarc@domain.example
```

Une fois que toutes les étapes de la mise en œuvre seront terminées, l'enregistrement devrait ressembler à ce qui suit :

```
v=DMARC1; p=reject; pct=100; sp=reject;
rua=mailto:dmarc@domain.example
```

2.3.2 Sélection de la stratégie DMARC

Pour déterminer la stratégie DMARC à appliquer, le système de réception cherchera l'enregistrement DMARC associé au domaine figurant dans l'en-tête de message `From (De)`. Le protocole DMARC repose sur le concept du « domaine organisationnel », qui est associé à la liste des suffixes de domaine publics (Public Suffix List) [6]. Cette liste est constituée des domaines de premier niveau (TLD), notamment `com`, `org`, et `ca`, et de certains suffixes de niveaux inférieurs comme `gc.ca`. Un domaine organisationnel correspond à tout domaine qui se trouve à un niveau sous un suffixe publié dans la liste, p. ex. `canada.ca` ou `cyber.gc.ca`.

Au moment de recevoir un message, le système de réception utilisera le premier enregistrement DMARC valide qu'il aura trouvé selon l'ordre suivant :

1. Un enregistrement qui correspond exactement au domaine de l'en-tête `From`;
2. Si le domaine de l'en-tête `From` est un sous-domaine d'un domaine organisationnel :
    a. L'enregistrement du domaine organisationnel sera utilisé. Cela s'applique aux sous-domaines de tous les niveaux, sans tenir compte des niveaux de sous-domaines intermédiaires;
    b. Si la balise d'une stratégie de sous-domaine (`sp`) figure dans l'enregistrement d'un domaine organisationnel, la stratégie définie par cette balise sera utilisée. Autrement, la stratégie de la balise `p` sera utilisée.

Par exemple, dans le cas d'un message comportant le domaine`sub2.sub1.domain.example` dans l'en-tête `From`, le système de réception appliquera la première stratégie qu'il aura trouvée selon l'ordre suivant :

1. `dmarc.sub2.sub1.domain.example` → balise `p`.
2. `_dmarc.domain.example` → balise `sp`.
3. `_dmarc.domain.example` → balise `p`.

2.3.3 Mise en correspondance des domaines dans le protocole DMARC

Aux fins du protocole DMARC, les domaines SPF et DKIM correspondent au domaine de l'en-tête `From` s'ils se correspondent en fonction du paramètre strict ou souple défini dans l'enregistrement DMARC. Deux valeurs sont possibles; elles peuvent être configurées de façon distincte pour le protocole SPF et le protocole DKIM :

- **Souple (Relaxed) (valeur par défaut)** : Les domaines se correspondent s'ils ont le même domaine organisationnel;
- **Strict** : Les domaines se correspondent uniquement s'il s'agit d'une correspondance exacte. Pour respecter le paramètre de correspondance stricte, il faudra peut-être créer des enregistrements SPF, DKIM et DMARC pour des sous-domaines.

2.4 Domaines autres que les domaines de courrier

2.4.1 Enregistrement MX indiquant l'absence de service

Bien que le protocole SPF permette d'autoriser les expéditeurs de messages sortants, il n'indique pas si un domaine est en mesure de recevoir du courriel. Les mentions « No service » (aucun service) ou « Null » (aucun) ont été proposées en tant qu'enregistrement MX en 2015 pour indiquer l'absence d'infrastructure de réception de messages. La configuration d'un enregistrement MX « Null » permet de mieux annoncer le fait qu'un domaine n'est pas en mesure de recevoir des messages.

Voici l'enregistrement MX recommandé pour les domaines autres que les domaines de courrier :

Préférence : `0` (zéro)Nom d'hôte : `.` (point)

Il doit s'agir de l'enregistrement MX du domaine.

2.4.2 SPF

Il convient de configurer les enregistrements SPF pour les domaines autres que les domaines de courrier de manière à ce que les messages envoyés depuis toute adresse IP soient rejetés. Voici l'enregistrement SPF recommandé pour les domaines autres que les domaines de courrier :

```
v=spf1 -all
```

Cet enregistrement devrait être créé comme entrée TXT générique de manière à ce qu'il soit renvoyé en réponse à des requêtes TXT pour le domaine racine ou tout sous-domaine.

2.4.3 DMARC

Les enregistrements DMARC pour les domaines autres que les domaines de courrier devraient être configurés de manière à rejeter tous les messages qui échouent à la vérification SPF et DKIM, ce qui correspondra à tous les messages une fois l'enregistrement SPF ci-dessus publié. Voici l'enregistrement DMARC recommandé pour les domaines autres que les domaines de courrier :

```
v=DMARC1; p=reject; sp=reject; pct=100; rua=mailto:dmarc@domain.example
```

Il n'est pas nécessaire de créer un enregistrement générique dans ce cas-ci, car le protocole DMARC indique qu'il faut utiliser l'enregistrement du domaine organisationnel si aucun enregistrement n'est trouvé pour un sous-domaine donné.

Annexe 3Analyser l'information liée aux courriels

Au moment de mettre en œuvre les protocoles SPF, DKIM et DMARC, les administrateurs de système peuvent se servir de l'information fournie dans les en-têtes de message et les rapports DMARC globaux pour détecter les erreurs de configuration et assurer le dépannage des problèmes de livraison.

3.1 En-têtes de message

Les utilisateurs ne les voient normalement pas, mais les en-têtes de message contiennent une foule d'information utile pour les administrateurs de système. Les en-têtes sont ajoutés aux messages à diverses étapes, généralement par les systèmes qui ont interagi d'une manière ou d'une autre avec ces messages. Il est souvent possible d'accéder aux en-têtes dans le client de courrier au moyen de l'option permettant d'afficher le message « d'origine » ou ses propriétés.

Le tableau 4 décrit les en-têtes les plus utiles dans le contexte de la protection du domaine de courrier.

Tableau 4 : En-têtes de message

En-tête	Description
`ARC-Authentication-Results`	Résultats des vérifications aux fins d'authentification effectuées par un système qui a transféré un message.
`ARC-Message-Signature`	Signature appliquée par un système qui transfère un message pour attester du contenu des en-têtes du message d'origine.
`ARC-Seal`	Signature générée par un système qui transfère un message pour attester de l'intégrité des en-têtes `ARC-Authentication-Results` et`ARC-Message-Signature`.
`Authentication-Results`	Fait état des résultats des vérifications aux fins d'authentification effectuées par un système de réception, y compris les vérifications SPF, DKIM et DMARC. Voir la section C.1.1.
`Delivered-To`	Boîte aux lettres à laquelle le message a été livré.
`DKIM-Signature`	Signature DKIM appliquée à un message par le système d'origine. Voir la section C.1.2.
`From`	Nom d'affichage et adresse source que la majorité des clients de courrier présentent à l'utilisateur. Le domaine de cette adresse est utilisé aux fins de l'authentification DMARC.
`Received`	Série d'en-têtes auxquels les MTA qui traitent un message de son origine à sa destination ajoutent des éléments. Ils sont habituellement ajoutés en préfixe et peuvent être lus en ordre chronologique inversé. Chaque en-tête comporte normalement le nom des hôtes d'envoi et de réception et un horodateur. Il peut également inclure les adresses IP connexes et des informations de connexion.
`Received-SPF`	Fait état des résultats de la vérification SPF effectuée par le système de réception. Voir la section C.1.3.

`Return-Path`	Indique l'adresse courriel à laquelle les messages d'erreur devraient être envoyés. Lorsqu'il est présent, le domaine indiqué dans cet en-tête sera utilisé aux fins de l'évaluation SPF au lieu du domaine du message SMTP HELO du serveur d'envoi. Si des expéditeurs tiers sont utilisés, le fait de préciser une adresse `Return-Path` qui correspond à l'en-tête `From` peut permettre aux messages de réussir la mise en correspondance SPF.
`To`	Adresse de destination du message.
`X-[propre à un système]`	Tout en-tête commençant par « `x-` » est non standard. Il s'agit normalement d'en-têtes propres à un système qu'un fournisseur ou un fournisseur de services a ajoutés à ses propres fins. Dans certains cas, ils peuvent fournir de l'information supplémentaire sur le traitement d'un message, par exemple, la manière dont il a été évalué par un service de sécurité ou un antipourriel.

3.1.1 Authentication-Results

L'en-tête Authentication-Results résume les résultats de l'authentification SPF, DKIM et DMARC. Conformément à la description présentée dans la publication *RFC 8601 Message Header Field for Indicating Message Authentication Status* [7], cet en-tête :

> « [...] est constitué d'un identifiant d'authentification, d'une version facultative et d'une série d'énoncés et de données à l'appui. Ces énoncés sont présentés selon le mode "méthode=résultat" et indiquent les méthodes d'authentification appliquées et leurs résultats respectifs. Pour chaque énoncé, les données à l'appui peuvent inclure une chaîne de "raisons" [entre parenthèses] et un ou plusieurs énoncés "propriété=valeur" indiquant les propriétés du message évaluées pour en arriver à cette conclusion. » [Traduction libre]

Les énoncés d'identifiant et d'authentification sont séparés par un point-virgule, et il peut être plus facile de les déchiffrer s'ils sont répartis sur plusieurs lignes, comme dans l'exemple suivant :

```
Authentication-Results:
mta2.receiver.example;
dkim=none (message not signed) header.i=none;
spf=Pass smtp.mailfrom=alice@sender.example;
spf=None smtp.helo=postmaster@mta1.sender.example;
dmarc=pass (p=quarantine dis=none) d=sender.example
```

En consultant cet en-tête, on constate que :

- le message a été évalué par `mta2.receiver.example`;
- le message n'a pas réussi la vérification DKIM, car il n'était pas signé;
- le message a réussi la vérification SPF au moyen du domaine indiqué dans l'en-tête `smtp.mailfrom` ou `From`, c'est-à-dire`sender.example`.

- aucun enregistrement SPF n'a été trouvé pour le domaine utilisé dans le message SMTP HELO : `mta1.sender.example`;
- l'évaluation DMARC a utilisé la stratégie du domaine (`d`) `sender.example`. Comme le message a réussi la vérification SPF et que les domaines utilisés pour les protocoles SPF et DMARC correspondent, le message a réussi la vérification DMARC, et la disposition ou la stratégie DMARC appliquée (`dis`) est `none`. On constate également que la stratégie d'application (`p`) du domaine est définie sur `quarantine`.

Prenons maintenant un exemple plus complexe comportant un en-tête ARC :

```
Authentication-Results:
mta3.receiver.example;
dkim=pass header.i=@sender.example header.s=selector5
header.b=B4f6tR4R;
arc=pass (i=1 spf=pass spfdomain=sender.example dkim=pass
dkdomain=sender.example dmarc=pass fromdomain=sender.example);
spf=pass (receiver.example: domain of bob@sender.example designates
192.0.2.1 as permitted sender) smtp.mailfrom=bob@sender.example;
dmarc=pass (p=NONE sp=NONE dis=NONE) header.from=sender.example
```

En consultant cet en-tête, on constate que :

- le message a été évalué par `mta3.receiver.example`;
- le message a réussi la vérification DKIM au moyen de la clé publique associée au domaine (`header.i`) `sender.example` et au sélecteur (`header.s`) `selector5`; cette clé est publiée dans un enregistrement DNS TXT se trouvant à l'emplacement `selector5._domainkey.sender.example`; le champ `header.b` renvoie à la valeur de hachage se trouvant dans l'en-tête `DKIM-Signature`;
- le message a réussi l'authentification ARC en fonction de l'instance numéro 1 (`i=1`) des résultats de la chaîne ARC. Le reste du contenu résume l'information qui se trouve dans l'en-tête `ARC-Authentication-Results` correspondant;
- le message a réussi la vérification SPF au moyen du domaine indiqué dans l'en-tête `smtp.mailfrom` ou `From`, c'est-à-dire`sender.example`. Dans la section « raison » entre parenthèses, on constate que `receiver.example` a conclu que l'adresse IP `192.0.2.1` était autorisée par `sender.example`;
- l'évaluation DMARC a utilisé la stratégie du domaine `header.from`, c'est-à-dire`sender.example`. Comme le message a réussi au moins une vérification SPF ou DKIM et que les domaines utilisés correspondent, le message a réussi la vérification DMARC, et la disposition (`dis`) est `NONE`. On constate également que la stratégie d'application (`p`) du domaine est définie sur `NONE` et que celle du sous-domaine (`sp`) est définie sur `NONE`.

3.1.2 DKIM-Signature

L'en-tête `DKIM-Signature` correspond à une signature cryptographique qui permet à un système de réception de vérifier que le corps d'un message et certains en-têtes précisés n'ont pas été modifiés pendant la transmission. Un système de réception peut valider l'authenticité d'un message au moyen du contenu de ce dernier et de la clé publique précisée. Le tableau 5 décrit les balises utilisées dans cet en-tête.

Tableau 5 : Balises de l'en-tête DKIM-Signature

Balise	Description
`a`	Algorithme de chiffrement utilisé pour générer la signature.
`b`	Code haché en Base64 des en-têtes désignés par la balise `h`.
`bh`	Code haché en Base64 du corps du message.
`c`	Balise facultative indiquant le niveau de modifications à tolérer, comme le rajustement des espaces blancs ou le retour automatique à la ligne. Elle comporte deux valeurs distinctes pour les en-têtes et le corps du message au format « `[headers]/[body]` », et les valeurs valides pour chaque entrée sont « `simple` » et « `relaxed` », p. ex. « `relaxed/relaxed` ».
`d`	Domaine dans lequel la clé publique a été publiée, utilisé avec le sélecteur (`s`) pour déterminer l'emplacement DNS selon le format`selector._domainkey.domain.example`.
`h`	Liste d'en-têtes utilisés pour calculer la valeur de hachage de l'en-tête (`b`) .
`i`	Balise facultative permettant d'associer un message à une identité précise (c.-à-d. une adresse ou une boîte aux lettres). Le domaine utilisé doit correspondre au domaine de la balise `d`.
`s`	Sélecteur où la clé publique a été publiée, utilisé avec le domaine (`d`) pour déterminer l'emplacement DNS selon le format`selector._domainkey.domain.example`.
`t`	Horodateur facultatif au format epoch Unix (UTC), c'est-à-dire les secondes écoulées depuis le 1er janvier 1970.
`v`	Version de la spécification, toujours « `v=1` ».
`x`	Horodateur facultatif pour l'expiration au format epoch Unix (UTC), c'est-à-dire les secondes écoulées depuis le 1er janvier 1970. Cette valeur doit dépasser la valeur de `t`.

3.1.3 Received-SPF

L'en-tête `Received-SPF` fait état des résultats de l'authentification SPF et peut comporter de l'information supplémentaire qui ne se trouve pas dans les sections SPF de l'en-tête `Authentication-Results`. Le tableau 6 présente les résultats possibles de la validation SPF et le tableau 7 décrit les champs susceptibles d'être inclus dans cet en-tête. Cet en-tête peut également inclure une section « raison » entre parenthèses qui donne d'autres renseignements sur les opérations qui ont permis d'obtenir ce résultat.

Tableau 6 : Résultats liés à Received-SPF

Résultat	Description
`fail`	L'adresse IP n'est pas autorisée, généralement en raison d'un enregistrement SPF qui se termine par « `-all` ».
`neutral`	L'adresse IP n'est pas autorisée, mais l'enregistrement SPF se termine par « `?all` ». Ce résultat est généralement traité comme le résultat `pass`.
`none`	Aucun enregistrement SPF n'a été trouvé pour le domaine `From` ni pour celui de la commande SMTP HELO si une telle requête avait été faite, ou encore pour le domaine `Return-Path` si un tel en-tête était présent.
`pass`	L'adresse IP est autorisée.
`permerror`	L'enregistrement SPF n'a pu être interprété correctement, sûrement en raison d'une erreur de syntaxe ou parce que la limite de 10 recherches DNS a été dépassée.
`softfail`	L'adresse IP n'est pas autorisée, mais l'enregistrement SPF se termine par « `~all` ». Ce résultat est généralement traité comme le résultat `pass`.
`temperror`	Aucun enregistrement SPF n'a pu être récupéré, sûrement en raison d'une erreur DNS.

Tableau 7 : Champs liés à Received-SPF

Champ	Description
`client-ip`	Adresse IP du client SMTP d'envoi.
`envelope-from`	Adresse utilisée dans l'en-tête `From`.
`helo`	Nom d'hôte donné dans la commande SMTP HELO.
`identity`	Identité utilisée lors de la validation, normalement « `mailfrom` » ou « `helo` ».
`mechanism`	Partie de l'enregistrement SPF qui correspond, p. ex. « `ip4:192.0.2.1` ».
`problem`	Dans le cas d'une erreur, détails sur l'erreur en question.
`receiver`	Nom d'hôte du vérificateur SPF.

3.2 Rapports DMARC globaux

Les rapports DMARC globaux donnent aux propriétaires de systèmes de l'information sur les messages envoyés qui comportent l'un de leurs domaines dans le champ `From`. En général, ces rapports sont envoyés par les systèmes de réception une fois par période de 24 heures, mais certains systèmes les envoient plus fréquemment. Les rapports sont envoyés par courriel à l'adresse indiquée dans la balise `rua` de l'enregistrement DMARC. Ils sont envoyés en pièce jointe comme fichier comprimé au format ZIP ou GZIP.

Les rapports DMARC globaux sont produits en langage XML pour en faciliter le traitement automatisé et sont structurés conformément à la publication RFC 7489 [3]. Les sections du rapport, y compris des exemples, sont présentées ci-dessous.

3.2.1 Métadonnées du rapport

La section `report_metadata` comporte de l'information sur l'ensemble du rapport, notamment :

- le nom (`org_name`) et l'adresse courriel (`email`) de l'organisation d'origine;
- des coordonnées additionnelles (`extra_contact_info`), comme l'adresse d'un site Web;
- l'identificateur du rapport (`report_id`), qui devrait être propre à l'organisation qui fournit le rapport;
- une plage de dates (`date_range`) qui donne le début et la fin de l'horodatage de la période couverte par le rapport, en secondes au format epoch Unix.

Voici un exemple de la section `report_metadata` :

```
<report_metadata>
  <org_name>receiver.example</org_name>
  <email>noreply-dmarc@receiver.example</email>
  <extra_contact_info>https://receiver.example/dmarc</extra_contact_info>
  <report_id>75896041237538053212</report_id>
  <date_range>
    <begin>1602633600</begin>
    <end>1602719999</end>
  </date_range>
</report_metadata>
```

3.2.2 Stratégie publiée

La section `policy_published` indique la stratégie DMARC récupérée par le système de réception à partir du système DNS aux fins d'évaluation. Cette section comprend l'information suivante :

- `domain` correspond au domaine de l'emplacement DNS de la stratégie, p. ex. `domain.example` pour l'enregistrement trouvé à `_dmarc.domain.example`;
- Les autres champs représentent les valeurs explicites ou par défaut des balises correspondantes indiquées dans l'enregistrement de la stratégie DMARC, notamment :
  - `adkim` – mise en correspondance DKIM, valeur par défaut `r` pour *relaxed*;

- `aspf` – mise en correspondance SPF, valeur par défaut `r` pour *relaxed*;
- `p` – stratégie du domaine, qui doit être définie explicitement sur `none`, `quarantine` ou `reject`;
- `sp` – stratégie du sous-domaine, qui peut être définie sur `none`, `quarantine` ou `reject`. La valeur par défaut correspond à la section `p`;
- `pct` – pourcentage, dont la valeur par défaut est de `100`.

Voici un exemple de la section `policy_published` :

```
<policy_published>
  <domain>owner.example</domain>
  <adkim>r</adkim>
  <aspf>r</aspf>
  <p>none</p>
  <sp>none</sp>
  <pct>100</pct>
</policy_published>
```

3.2.3 Enregistrements

Les rapports globaux contiennent une ou plusieurs sections `record` qui précisent les résultats de l'authentification et de la livraison d'un ensemble de messages similaires.

Chaque enregistrement (`record`) contient une ou plusieurs sections `row` qui comprennent ce qui suit :

- `source_ip` : adresse IP du serveur duquel les messages ont été reçus. Il s'agit également de l'adresse IP utilisée aux fins d'authentification SPF par l'organisation qui a produit le rapport;
- `count` : nombre de messages reçus comportant des caractéristiques similaires et traités de façon semblable;
- `policy_evaluated` : comporte les résultats de l'authentification SPF, DKIM et DMARC dans plusieurs sections :
  - `disposition` : stratégie DMARC appliquée par le système de réception, soit `none`, `quarantine` ou `reject`;
  - `dkim` : résultat de l'authentification DKIM, y compris la mise en correspondance des domaines, soit `pass` ou `fail`;
  - `spf` : résultat de l'authentification SPF, y compris la mise en correspondance des domaines, soit `pass` ou `fail`;
  - `reason` : section facultative comportant les champs `type` et `comment`. Cette section est généralement utilisée lorsque le système de réception a pris une mesure autre que celle précisée dans la stratégie DMARC du domaine, comme avoir livré un message qui a échoué à la vérification DMARC parce qu'il a réussi la validation ARC.

La section `identifiers` comprend normalement un champ `header_from`, qui correspond au domaine se trouvant dans l'en-tête `From`. Il s'agit du domaine qui doit correspondre aux domaines utilisés pour la vérification SPF et DKIM. Cette section peut également comporter un champ `envelope_from`, qui inclut le domaine utilisé dans le message SMTP HELO. Si le champ `envelope_from` n'est pas inclus, l'information se trouvera sûrement dans le champ `spf` / `domain` de la section `auth_results`.

La section `auth_results` comporte deux sous-sections qui présentent les résultats de l'authentification DKIM et SPF. Il convient de noter que les messages transférés peuvent comporter plus d'une section `auth_results`, ce qui peut être utile pour déterminer le trajet d'un message.

La sous-section `dkim` comprend les champs suivants :

- `domain` : domaine indiqué par la balise `d` (domaine) de l'en-tête `DKIM-Signature`;
- `result` : résultat de la validation de la signature DKIM d'un message, normalement `pass` ou `fail`;
- `selector` : sélecteur défini par la balise `s` (sélecteur) de l'en-tête `DKIM-Signature`.

Il est à noter que si un a message n'a pas été signé au moyen du protocole DKIM, les champs`result` et `selector` risquent d'être vides ou omis, ou encore d'inclure la valeur « `none` ».

La sous-section `spf` comprend les champs suivants :

- `domain` : domaine utilisé aux fins de l'authentification SPF;
- `result` : résultat de l'authentification SPF, généralement `pass`, `fail` ou `none` (voir le tableau 6 pour consulter la liste complète des résultats possibles);
- `scope` : champ facultatif précisant la source du domaine utilisé aux fins d'authentification SPF, soit `helo` pour le message SMTP HELO ou `mfrom` pour l'en-tête `From`. S'il n'est pas précisé, on suppose qu'il s'agit de `mfrom`.

Dans l'exemple d'enregistrement ci-dessous, le message :

- a réussi la vérification SPF pour le domaine SMTP HELO, mais a échoué à la mise en correspondance, car le domaine ne correspondait pas à celui de l'en-tête `header_from`;
- a réussi la vérification DKIM, y compris la mise en correspondance;
- a réussi la vérification DMARC et a été livré (`disposition` de `none`).

```
<record>
  <row>
    <source_ip>192.0.2.1/source_ip>
    <count>1</count>
    <policy_evaluated>
      <disposition>none</disposition>
      <dkim>pass</dkim>
      <spf>fail</spf>
    </policy_evaluated>
  </row>
  <identifiers>
    <header_from>owner.example</header_from>
  </identifiers>
  <auth_results>
    <dkim>
      <domain>owner.example</domain>
      <result>pass</result>
      <selector>2021-02-01</selector>
    </dkim>
    <spf>
      <domain>third-party.example</domain>
      <result>pass</result>
    </spf>
  </auth_results>
</record>
```

Dans l'exemple ci-dessous, trois messages :

- ont réussi les vérifications SPF et DKIM pour le domaine `forwarder.example`;
- ont échoué à la vérification DMARC, car les domaines utilisés pour les vérifications SPF et DKIM ne correspondaient pas au domaine `header_from`, c'est-à-dire `owner.example`;
- ont été livrés (en fin de compte) par le système de réception (`disposition` de `none`), car ils ont réussi la validation ARC (comme l'indique `arc=pass` dans le champ `reason/comment`).
  - Cela signifie que le système de réception s'est fié à la signature ARC appliquée par `forwarder.example`, qui attestait que les messages avaient réussi les vérifications SPF et DKIM avant d'être transférés.

```
<record>
  <row>
    <source_ip>198.51.100.1</source_ip>
    <count>3</count>
    <policy_evaluated>
      <disposition>none</disposition>
      <dkim>fail</dkim>
      <spf>fail</spf>
      <reason>
        <type>local_policy</type>
        <comment>arc=pass</comment>
      </reason>
    </policy_evaluated>
  </row>
  <identifiers>
    <header_from>owner.example</header_from>
  </identifiers>
  <auth_results>
    <dkim>
      <domain>forwarder.example</domain>
      <result>pass</result>
      <selector>forward-dkim</selector>
    </dkim>
    <spf>
      <domain>forwarder.example</domain>
      <result>pass</result>
    </spf>
  </auth_results>
</record>
```

3.3 Interpréter les résultats DMARC

En général, il est difficile d'analyser manuellement les rapports globaux, même si vous n'en recevez que quelques-uns. Vous pouvez choisir l'un des nombreux outils de source ouverte, gratuits et commerciaux pour traiter automatiquement ces rapports. Ils permettent d'extraire les informations pertinentes et présentent des données sommaires que vous pouvez alors examiner et analyser.

3.3.1 Résultats SPF

On peut déterminer les résultats SPF en examinant le contenu des champs `auth_results` / `spf` / `result` et `policy_evaluated` / `spf`. Les combinaisons de résultats possibles et leur signification sont présentées dans le tableau 8.

Tableau 8 : Signification des résultats SPF

Auth Results	Policy Evaluated	Signification
Autre que `pass`	`fail`	Omission / erreur / échec de la vérification SPF
`pass`	`fail`	Domaine SPF non correspondant
`pass`	`pass`	Domaine SPF correspondant

Dans le cas d'erreurs ou d'échecs SPF, consultez le champ `auth_results` / `spf` / `domain` pour déterminer le domaine utilisé. Vérifiez qu'un enregistrement SPF a été créé pour ce domaine, qu'il est bien conçu et que l'ensemble d'adresses IP indiquées sont correctes.

Dans le cas d'un domaine SPF non correspondant, comparez le champ `auth_results` / `spf` / `domain` au champ `header_from`. Si le domaine SPF est un sous-domaine du domaine `header_from`, la non-correspondance pourrait être attribuable à une stratégie DMARC qui exige une correspondance stricte pour la vérification SPF (`aspf=s`). Pour corriger le problème, vous pouvez prendre l'une des mesures suivantes :

- Créer un enregistrement DMARC propre au sous-domaine;
- Modifier le domaine utilisé;
- Modifier la stratégie de mise en correspondance du domaine organisationnel pour qu'elle soit souple (*relaxed*).

S'il ne s'agit pas d'un sous-domaine, la non-correspondance pourrait être causée par un expéditeur tiers. Dans certains cas, les expéditeurs tiers permettent l'utilisation d'une adresse `Return-Path` personnalisée pour régler ce problème.

3.3.2 Résultats DKIM

On peut déterminer les résultats DKIM en examinant le contenu des champs `auth_results` / `dkim` / `result` et `policy_evaluated` / `dkim`. Les combinaisons de résultats possibles et leur signification sont présentées dans le tableau 9.

Tableau 9 : Signification des résultats DKIM

Auth Results	Policy Evaluated	Signification
Autre que `pass`	`fail`	Omission / erreur / échec de la vérification DKIM
`pass`	`fail`	Domaine DKIM non correspondant
`pass`	`pass`	Domaine DKIM correspondant

S'il manque le domaine DKIM, vérifiez qu'il a été déployé correctement pour le serveur d'envoi.

Dans le cas d'erreurs ou d'échecs DKIM, consultez les champs `auth_results` / `dkim` / `domain` et `selector` pour déterminer l'enregistrement DNS DKIM utilisé. Vérifiez que l'enregistrement DKIM a été créé, qu'il est bien conçu et que les serveurs qui devraient l'utiliser sont bien configurés.

Dans le cas d'un domaine DKIM non correspondant, comparez le champ `auth_results` / `dkim` / `domain` au champ `header_from`. Si le domaine DKIM est un sous-domaine du domaine `header_from`, la non-correspondance pourrait être attribuable à une stratégie DMARC qui exige une correspondance stricte pour la vérification DKIM (`adkim=s`). Pour corriger le problème, vous pouvez prendre les mesures suivantes :

- Créer un enregistrement DMARC propre au sous-domaine;
- Modifier le domaine utilisé;
- Modifier la stratégie de mise en correspondance du domaine organisationnel pour qu'elle soit souple (*relaxed*).

S'il ne s'agit pas d'un sous-domaine, la non-correspondance pourrait être causée par un expéditeur tiers. Dans certains cas, on peut corriger le problème en créant un enregistrement CNAME qui renvoie à un enregistrement DKIM détenu par le tiers.

3.3.3 Échecs DMARC

Si les vérifications SPF et DKIM échouent, qu'il s'agisse d'un échec à proprement parler ou de domaines non correspondants, le message échouera à la vérification DMARC et la stratégie d'application définie sera mise en œuvre. Ce résultat est indiqué par la valeur `fail` dans les champs `policy_evaluated` / `spf` et `policy_evaluated` / `dkim`. Vous devriez surveiller les données de vos rapports DMARC pour détecter toute augmentation inhabituelle du nombre d'échecs DMARC, ce qui pourrait indiquer un problème lié à votre domaine.

Voici les causes courantes d'échecs DMARC :

- **Déploiement incomplet / erreurs de configuration** : L'adresse IP d'un serveur d'envoi n'a pas été incluse dans l'enregistrement SPF pour le domaine, le protocole DKIM n'a pas été déployé et/ou l'exigence de mise en correspondance stricte d'une stratégie n'a pas été remplie.
- **Transferts** : Les messages transférés par un serveur intermédiaire (p. ex. au moyen d'une liste de diffusion) échouent souvent à la vérification DMARC au moment de leur réception. Comme le protocole SPF est plus susceptible de rencontrer ce problème que le protocole DKIM, la mise en œuvre de ce dernier peut permettre de l'atténuer en partie. Si l'option est prise en charge, on peut également demander à l'organisation qui achemine les messages de créer un en-tête `Return-Path` personnalisé ou de remplacer l'en-tête `From` pour régler les problèmes liés au protocole SPF. Le protocole ARC comporte également un mécanisme permettant de faire reconnaître les messages transférés comme étant fiables, mais il n'est pas déployé à grande échelle.
- **Expéditeurs tiers :** Il est impossible de faire la distinction entre les expéditeurs tiers qui n'ont pas configuré correctement leurs systèmes de manière à prendre en charge les protocoles SPF et DKIM et les expéditeurs non autorisés qui envoient des messages falsifiés. Les rapports DMARC peuvent vous aider à identifier les services tiers utilisés par votre organisation, ce qui permettra aux services approuvés de corriger la configuration. Il convient d'éviter, dans la mesure du possible, les expéditeurs tiers qui ne prennent pas pleinement en charge les protocoles SPF (y compris l'en-tête `Return-Path` personnalisé), DKIM et DMARC.
- **Usurpation :** Les échecs DMARC qui ne peuvent être attribués à des erreurs de configuration, aux messages transférés ou à des expéditeurs tiers sont sans doute attribuables à l'usurpation.

3.3.4 Caractéristiques d'une campagne d'usurpation

Les activités que nous avons observées relativement à l'usurpation de domaines appartenant au gouvernement du Canada présentaient les caractéristiques suivantes :

- **Usurpation opportuniste :** Nous avons observé un faible niveau continu d'activités d'usurpation qui semblent toucher tout domaine ayant une présence Web ou DNS. Nous sommes d'avis que ces activités ne sont pas ciblées et qu'il convient de s'attendre à ce que tous les domaines puissent être touchés.
- **Courte durée :** Les campagnes ciblées avaient tendance à ne durer que quelques jours, et le volume de messages suivait typiquement une courbe qui atteignait un sommet au milieu.
- **Infrastructure dispersée :** Les campagnes ciblées sont généralement lancées depuis de nombreux serveurs à partir de divers fournisseurs d'hébergement, de réseaux et de lieux géographiques.
- **Identificateurs connexes :** Dans certains cas, on peut regrouper les activités de manière à repérer des campagnes en ayant recours à des identificateurs courants ou connexes, comme les domaines utilisés dans les messages SMTP HELO des serveurs ou l'en-tête `From`.