Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

CANADIAN CENTRE FOR CYBER SECURITY

Conseils sur la configuration sécurisée des protocoles réseau (Version 3)

Praticien·nes

Canada

Avant-propos

Le présent document est NON CLASSIFIÉ. Il est publié par le Centre canadien pour la cybersécurité (Centre pour la cybersécurité) et se veut une mise à jour d'une version publiée antérieurement.

Nous vous recommandons la lecture de l'ITSP.40.111, Algorithmes cryptographiques pour l'information NON CLASSIFIÉ, PROTÉGÉ A ET PROTÉGÉ B [1]. Les configurations de la présente publication sont conformes aux exigences cryptographiques dans l'ITSP.40.111.

Date d'entrée en vigueur

Le présent document entre en vigueur janvier 2025.

Historique des révisions

Révision	Modifications	Date
1	Première version	2 août 2016
2	Version mise à jour (version 2)	13 octobre 2020
3	Version mise à jour (version 3)	janvier 2025

D97-3/40-062-2024F-PDF
978-0-660-70990-1

Sommaire

L'information contenue dans la présente publication détermine et décrit les protocoles de sécurité acceptables et la façon dont ceux-ci peuvent être utilisés pour assurer la protection continue de l'information sensible. Dans le cas des ministères et des organismes du gouvernement du Canada (GC), les conseils offerts s'appliquent aux documents NON CLASSIFIÉ, PROTÉGÉ A et PROTÉGÉ B.

L'habileté de votre organisme à transmettre les données et l'information sensibles en toute sécurité est essentielle pour la prestation de vos programmes et services. Les protocoles liés à la sécurité cryptographique fournissent des mécanismes de sécurité servant à assurer la confidentialité, l'intégrité et l'authenticité de l'information du GC en plus d'aider à protéger ce dernier contre certaines menaces de cyberintrusion.

Une configuration appropriée des protocoles de sécurité permet d'assurer la confidentialité, l'intégrité et l'authenticité des données, l'authentification et la responsabilisation des intervenantes et intervenants, de même que la non-répudiation. Différents protocoles peuvent s'avérer nécessaires pour satisfaire aux exigences de sécurité propres à votre organisation et ces protocoles devraient être sélectionnés et mis en œuvre de façon à respecter toutes ces exigences.

Pour de plus amples renseignements sur la configuration sécurisée des protocoles réseau, veuillez communiquer avec le Centre d'appel par courriel à l'adresse contact@cyber.gc.ca ou par téléphone au 613-949-7048 ou au 1-833-CYBER-88.

Table des matières

Liste des figures

Liste des tableaux

1 Introduction

Les organisations recourent à des systèmes de technologies de l'information (TI) pour atteindre leurs objectifs opérationnels. Ces systèmes interconnectés sont souvent l'objet de sérieuses menaces et de cyberattaques susceptibles de nuire à la disponibilité, à la confidentialité et à l'intégrité des actifs informationnels. Des réseaux, des systèmes ou des renseignements compromis peuvent influer négativement les activités opérationnelles et entraîner une atteinte à la protection des données ainsi que des pertes financières.

Dans le présent document, vous trouverez des conseils sur les sujets suivants :

- la configuration sécurisée des protocoles réseau en vue de protéger l'information sensible[a];
- les algorithmes approuvés que le Centre canadien pour la cybersécurité (CCC) recommande d'utiliser avec ces protocoles réseau;
- les normes et les publications spéciales du National Institute of Standards and Technology (NIST) qui offrent de l'information supplémentaire sur ces protocoles réseau.

Complément au document du Secrétariat du Conseil du Trésor du Canada (SCT) intitulé Ligne directrice sur la définition des exigences en matière d'authentification [2], l'ITSP.40.062 vise à aider les praticiens des technologies dans le choix et l'utilisation des protocoles de sécurité appropriés pour la protection de l'information sensible (NON CLASSIFIÉ, PROTÉGÉ A et PROTÉGÉ B). Il fournit également des conseils en matière de cryptographie pour des solutions de TI de niveaux NON CLASSIFIÉ, PROTÉGÉ A et PROTÉGÉ B.[b] Chaque organisation est responsable pour déterminer ses objectifs et exigences en matière de sécurité dans son cadre de gestion des risques

1.1 Processus de gestion des risques liés à la sécurité des TI

Lors de la mise en place de protocoles de sécurité, les praticiennes et praticiens devraient tenir compte des activités relatives à la gestion des risques en sécurité des TI qui sont décrites dans l'ITSG-33 IT, Gestion des risques liés à la sécurité des TI – Une méthode axée sur le cycle de vie (ITSG-33) [3]. L'ITSG-33 décrit deux niveaux d'activités de gestion des risques liés à la sécurité des TI, à savoir les activités du niveau ministériel et du niveau des systèmes d'information. Il comprend également un catalogue de contrôles de sécurité, comme les exigences de sécurité normalisées visant à protéger la confidentialité, l'intégrité et la disponibilité des biens de TI. Consultez la Figure 1: pour une vue d'ensemble des niveaux de gestion des risques en sécurité des TI.

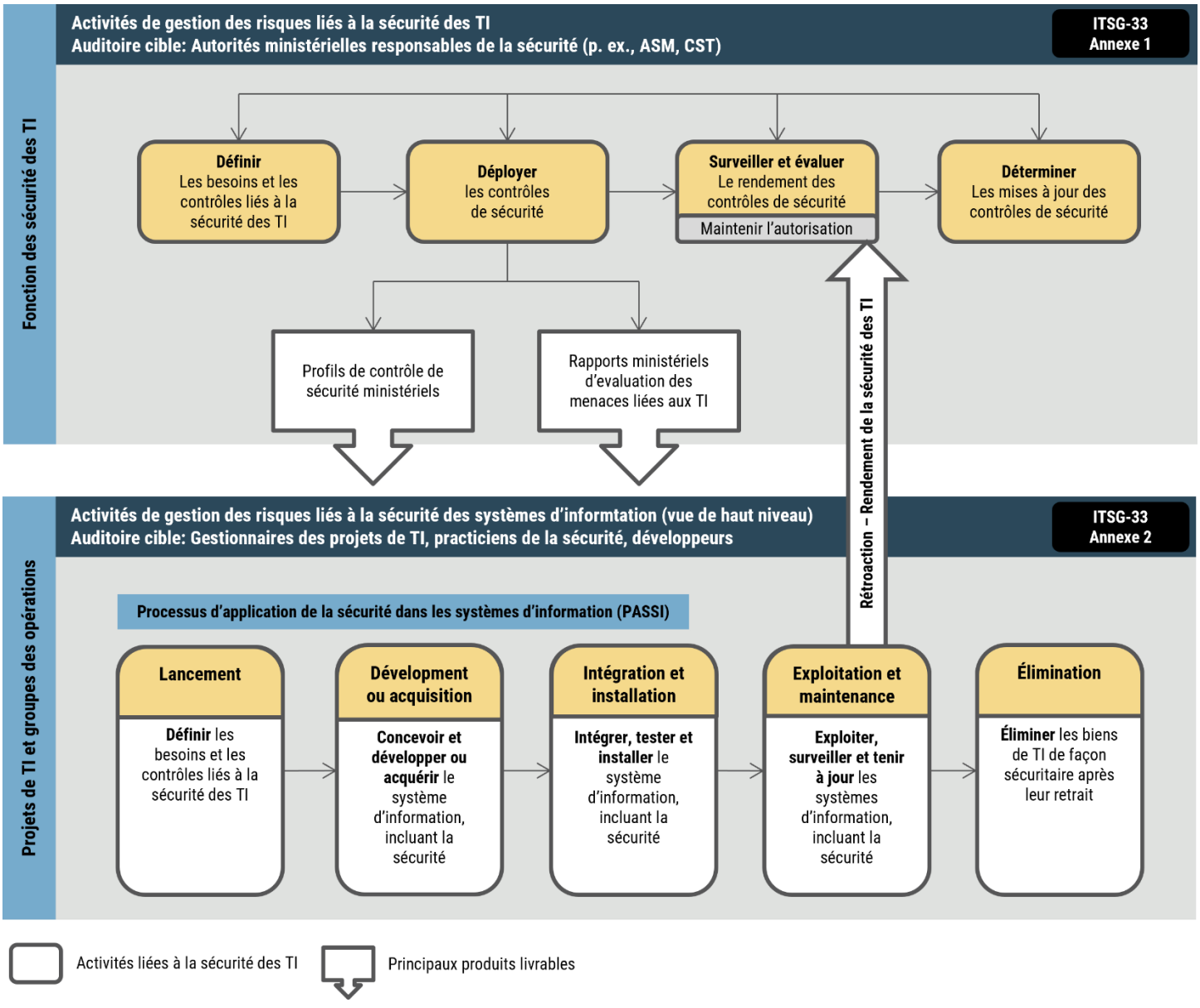
Les organismes devraient également prendre en considération les activités de gestion des risques suivantes : définir, déployer, surveiller et évaluer. Consultez l'annexe 1 de l'ITSG-33 [3] pour en savoir plus sur celles-ci.

[a] Dans le cas des ministères et des organismes du GC, les conseils offerts s'appliquent aux documents NON CLASSIFIÉ, PROTÉGÉ A et PROTÉGÉ B. Les systèmes d'un environnement PROTÉGÉ C et les domaines classifiés pourraient exiger des considérations supplémentaires du point de vue de la conception qui n'entrent pas dans le cadre du présent document.
[b] Les systèmes d'un environnement PROTÉGÉ C et les domaines classifiés pourraient exiger des considérations supplémentaires du point de vue de la conception qui n'entrent pas dans le cadre du présent document.

Les activités de gestion des risques au niveau ministériel (ou au niveau organisationnel pour les organismes qui ne font pas partie du GC) font partie des programmes de sécurité ministériels ou organisationnels dans l'objectif de planifier, de gérer, d'évaluer et d'améliorer la gestion des risques à la sécurité des TI.

Les activités de gestion des risques au niveau des systèmes d'information sont comprises dans le cycle de vie des systèmes d'information par l'intermédiaire du processus d'application de la sécurité dans les systèmes d'information (PASSI). Lors de la mise en place des protocoles de sécurité sur les réseaux, vous devriez tenir compte des étapes du PASSI. Pour en apprendre plus, consultez l'annexe 2 de l'ITSG-33 [3].

Figure 1: Processus de gestion des risques liés à la sécurité des TI



Description longue : Processus de gestion des risques liés à la sécurité des TI
Cette image décrit les activités de gestion des risques liés à la sécurité des TI de haut niveau du ministère au sein de la fonction de sécurité des TI ministérielle. Elle décrit également les activités de gestion des risques liés à la sécurité des systèmes d'information dans les projets de TI et les groupes opérationnels. Elle souligne également le fait que les activités de gestion des risques liés à la sécurité des TI aux deux niveaux agissent de concert dans un cycle continu pour maintenir et améliorer efficacement la posture de sécurité des systèmes d'information ministériels.

Les activités de gestion des risques liés à la sécurité des TI du ministère s'adressent à un public cible d'autorités en matière de sécurité du ministère et comportent les étapes suivantes :

1. Définir les besoins opérationnels en matière de sécurité et les contrôles de sécurité
2. Déployer les contrôles de sécurité, y compris l'établissement de profil de contrôle de sécurité ministériel et de rapports d'évaluation des menaces de TI du ministère
3. Surveiller et évaluer continuellement le rendement des contrôles de sécurité et maintenir l'autorisation
4. Déterminer les mises à jour des contrôles de sécurité

Les activités de gestion des risques liés à la sécurité de l'information visent les gestionnaires de projet de TI, les praticiennes et praticiens de la sécurité ainsi que les développeuses et développeurs. Elles comprennent les étapes suivantes :

1. Initiation : Définir les besoins et les contrôles liés à la sécurité des TI
2. Développement et acquisition : Concevoir et développer ou acquérir le système d'information dans le respect de la sécurité
3. Intégration et installation : Intégrer, tester et installer le système d'information dans le respect de la sécurité
4. Exploitation et maintenance : Exploiter, surveiller et tenir à jour
5. Élimination : Éliminer les biens de TI de façon sécuritaire après leur retrait

1.2 Recommandations

Tout au long du présent document, nous présentons des recommandations selon trois catégories : les configurations recommandées, adéquates et abandonnées.

1.2.1 Recommandées

Les configurations inscrites dans la colonne recommandées présentent des avantages que celles de la colonne adéquates n'ont pas. Les configurations recommandées devraient toujours être mises en place si le profil de connexion à distance le permet.

1.2.2 Adéquates

Les configurations de la colonne adéquates sont appropriées pour fournir le soutien nécessaire au profil des connexions à distance. Les configurations adéquates devraient être mises en place si les configurations recommandées ne peuvent l'être.

1.2.3 Abandonnées

Les configurations de la colonne abandonnées sont dues pour une transition selon l'orientation de l'ITSP.40.111 [1] ou en raison d'inquiétudes liées au protocole.

Si vous avez des systèmes qui utilisent des configurations de cette colonne, nous vous recommandons d'effectuer le plus tôt possible une transition vers les configurations inscrites aux colonnes *recommandées* ou adéquates.

Remarque : Il n'est pas nécessaire d'effectuer toutes les configurations recommandées ou adéquates sur vos systèmes. Vous devrez choisir les configurations nécessaires en fonction du profil de connexion à distance de votre organisme. Les protocoles sélectionnés devraient être mis en œuvre de manière à limiter la surface d'attaque du réseau.

2 Infrastructure à clé publique

Les infrastructures à clé publique (ICP) prennent en charge la gestion des clés publiques pour les services de sécurité des protocoles qui utilisent cette infrastructure, notamment les protocoles de sécurité de la couche de transport (TLS, pour *Transport Layer Security*), de la sécurité du protocole Internet (IPsec pour *Internet Protocol Security*) et S/MIME (*Secure/Multipurpose Internet Mail Extensions*).

Des conseils sur la gestion des clés de l'ICP sont proposés dans le document intitulé NIST Special Publication (SP) 800-57 Part 3 Rev 1 Recommendation for Key Management Part 3 : Application-Specific Key Management Guidance (en anglais seulement) [4]. Nous vous recommandons de suivre les conseils sur l'installation et l'administration d'une ICP fournis à la section 2, rév. 1 [4] de ce document.

Vous devez éviter de réutiliser des paires de clés publiques dans plusieurs protocoles au sein de l'ICP. Par exemple, ne réutilisez pas les paires de clés d'IKEv2 dans le protocole SSH.

Les certificats de clé publique devraient respecter la version 3 du format X.509 établi dans le document RFC 5280, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile (en anglais seulement) [5].

Les mises en œuvre des protocoles devraient permettre l'utilisation de multiples certificats ainsi que des clés privées qui leur sont associées afin de soutenir une plus grande adaptabilité sur le plan des algorithmes et de la taille des clés. Les certificats de clés publiques utilisés aux fins de signature, d'accord de clés ou de chiffrement de clés devraient se distinguer par l'extension d'usage de clé servant à déterminer l'une des valeurs suivantes :

- digitalSignature
- keyAgreement
- keyEncipherment

Conformément aux conseils en matière de cryptographie fournis dans l'ITSP.40.111 Algorithmes cryptographiques pour l'information NON CLASSIFIÉ, PROTÉGÉ A ET PROTÉGÉ B [1], la fonction de hachage cryptographique SHA-1 ne devrait pas être utilisée pour générer ou vérifier des signatures numériques au moyen de certificats de clés publiques.

3 Protocole de sécurité de la couche de transport (TLS)

Le protocole de sécurité de la couche de transport (TLS pour *Transport Layer Security*) vise à protéger la confidentialité, l'intégrité et l'authenticité des communications Internet entre les applications serveur et les applications client.

Conformément au document RFC 8446 The Transport Layer Security (TLS) Protocol Version 1.3 (en anglais seulement) [6], nous vous recommandons de configurer les serveurs et les clients TLS de manière à utiliser le protocole TLS 1.3. Utiliser la version TLS 1.2, qui est mise à jour dans le document RFC 8446 [6], est adéquat si celle-ci est nécessaire pour améliorer la compatibilité, pour se conformer aux audits internes ou pour utiliser les systèmes de surveillance des menaces. Vous devriez abandonner les versions TLS antérieures à la version 1.2 et toute version de protocole SSL (*Secure Sockets Layer*).

Les serveurs utilisant le protocole TLS pour protéger le trafic HTTP (c.-à-d. HTTPS) devraient prendre en charge le protocole HSTS (*HTTP Strict Transport Security*) conformément au document RFC 6797 HTTP Strict Transport Security (HSTS) (en anglais seulement) [7].

Un serveur de courriel qui fait office d'agent de transfert de messages (ATM) pour le protocole de transfert de courrier simple (SMTP pour *Simple Mail Transfer Protocol*) devrait prendre en charge la négociation du protocole TLS avec d'autres ATM. Le trafic SMTP peut être mis à niveau au protocole TLS au moyen de l'extension STARTTLS conformément au document RFC 3207 SMTP Service Extension for Secure SMTP over Transport Layer Security (en anglais seulement) [8]. Pour s'assurer de l'utilisation du protocole TLS pour le trafic SMTP, les ATM devraient soit prendre en charge le mécanisme MTA-STS conformément au document RFC 8461 SMTP MTA Strict Transport Security (MTA-STS) (en anglais seulement) [9], dans quel cas ils devraient être configurés en mode « renforcé » (*enforce* en anglais) de contrôle d'application des politiques, ou encore prendre en charge le protocole DANE-TLS, conformément au document RFC 7672 SMTP Security via Opportunistic DNS Based Authentication of Named Entities (DANE) Transport Layer Security (TLS) (en anglais seulement) [10].

Remarque : Il est toutefois important de noter que ces méthodes de chiffrement opportuniste ne sont prises en charge qu'au point par point. La protection de bout en bout du message est assurée par le protocole S/MIME. Pour obtenir plus de renseignements, voir la Section 7 - Secure/Multi-Purpose Internet Mail Extensions.

Lorsque le protocole TLS est utilisé pour protéger la confidentialité de l'information ou l'intégrité de l'information NON CLASSIFIÉ, PROTÉGÉ A et PROTÉGÉ B, les mises en œuvre devraient garantir une authentification mutuelle entre le serveur et le client au moyen des certificats X.509 version 3.

3.1 Suites de chiffrement TLS

Si le serveur ou le client est configuré pour prendre en charge la version 1.3 du protocole TLS, il devrait être configuré pour permettre seulement l'utilisation des suites de chiffrement listées au tableau 1.

Table 1: Suites de chiffrement recommandées pour la version 1.3 du protocole TLS

Recommandées	Adéquates
TLS_AES_256_GCM_SHA384 TLS_AES_128_GCM_SHA256 TLS_AES_128_CCM_SHA256	TLS_AES_128_CCM_8_SHA256

Si la version 1.2 du protocole TLS doit être prise en charge, le serveur ou le client TLS devrait être configuré pour ne prendre en charge que les suites de chiffrement de la version 1.2 du protocole TLS qui sont présentées dans le tableau 2.

Table 2: Suites de chiffrement recommandées pour la version 1.2 du protocole TLS

Recommandées	Adéquates	Abandonnées
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 TLS_ECDHE_ECDSA_WITH_AES_256_CCM TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 TLS_ECDHE_ECDSA_WITH_AES_128_CCM TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	TLS_ECDHE_ECDSA_WITH_AES_256_CCM_8 TLS_ECDHE_ECDSA_WITH_AES_128_CCM_8 TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 TLS_DHE_DSS_WITH_AES_256_GCM_SHA384 TLS_DHE_RSA_WITH_AES_256_CCM TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 TLS_DHE_DSS_WITH_AES_128_GCM_SHA256 TLS_DHE_RSA_WITH_AES_128_CCM TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 TLS_RSA_WITH_AES_256_GCM_SHA384 TLS_RSA_WITH_AES_128_GCM_SHA256 TLS_RSA_WITH_AES_256_CBC_SHA256 TLS_RSA_WITH_AES_256_CBC_SHA TLS_RSA_WITH_AES_128_CBC_SHA256 TLS_RSA_WITH_AES_128_CBC_SHA TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA TLS_DHE_RSA_WITH_AES_256_CBC_SHA TLS_DHE_RSA_WITH_AES_128_CBC_SHA

Vous pouvez utiliser n'importe laquelle des suites de chiffrement de la liste ou toutes les suites de la liste pour les serveurs et les clients TLS en fonction du profil déployé. Toutefois, si un déploiement avec accès par Internet exige des suites de chiffrements de la colonne de suites abandonnées, nous vous recommandons de faire une transition dès que possible. Votre centre de données peut continuer à utiliser des déploiements internes du protocole TLS avec les suites de chiffrement accompagnées d'un transport de clé RSA si requis pour être conforme à un audit ou pour des systèmes de détection de menaces, mais cette directive pourrait éventuellement changer.

Les suites de chiffrement ne précisent pas de taille de clé pour l'algorithme d'échange de clé publique. Les serveurs et les clients TLS devraient s'assurer que les paires de clés éphémères qui sont utilisées pour établir la clé secrète de session sont conformes aux exigences quant à la longueur de la clé spécifiées à l'ITSP.40.11 [1]. Vous trouverez dans le tableau 3 la liste des groupes pris en charge qui sont conformes à ITSP.40.111 [1].

Table 3: Groupes pris en charge par TLS qui sont conformes à l'ITSP.40.111

Recommandés	Adéquates	Abandonnées
secp256r1	ffdhe3072	secp224r1
secp384r1	ffdhe4096	sect233r1
secp521r1	ffdhe6144	sect233k1
	ffdhe8192	sect283k1
		sect283r1
		sect409k1
		sect409r1
		sect571k1
		sect571r1
		ffdhe2048

Le tableau 4 présente la liste des algorithmes de signature qui sont conformes à l'ITSP.40.111 [1].

Table 4: Algorithmes de signature TLS qui sont conformes à l'ITSP.40.111

Recommandés	Adéquates	Abandonnées
ecdsa_secp256r1_sha256	rsa_pkcs1_sha256	ecdsa_secp224r1_sha224
ecdsa_secp384r1_sha384	rsa_pkcs1_sha384	rsa_pkcs1_sha224
ecdsa_secp521r1_sha512	rsa_pkcs1_sha512	dsa_sha224
ed25519		dsa_sha256
ed448		dsa_sha384
rsa_pss_pss_sha256		dsa_sha512
rsa_pss_pss_sha384		
rsa_pss_pss_sha512		
rsa_pss_rsae_sha256		
rsa_pss_rsae_sha384		
rsa_pss_rsae_sha512		

3.2 Extensions TLS

Nous recommandons que les serveurs et les clients TLS prennent en charge les extensions indiquées dans le tableau 5.

Table 5: Extensions TLS recommandées

Nom de l'extension	Point de code d'extension	Références	Remarques
Négociation de protocole de la couche d'application	application_layer_protocol_negotiation	RFC 7301 (en anglais seulement) [11]	
Algorithmes de signature de certificat	signature_algorithms_cert	RFC 8446 [6] sec 4.2.3	
Interrogation du statut d'un certificat	status_request	RFC 6066 (en anglais seulement) [12] sec 8	
Témoin	Cookie	RFC 8446 [6] sec 4.2.2	TLS 1.3 seulement
Encrypt-then-MAC	encrypt_then_mac	RFC 7366 (en anglais seulement) [13]	TLS 1.2 seulement
Clé secrète de session étendue[c]	extended_main_secret / extended_master_secret	RFC 7627 (en anglais seulement) [14]	TLS 1.2 seulement
Partage de clé	key_share	RFC 8446 [6] sec 4.2.8	TLS 1.3 seulement
État des certificats multiples	status_request_v2	RFC 6961 (en anglais seulement) [15]	TLS 1.2 seulement
Clé prépartagée	pre_shared_key	RFC 8446 [6] sec 4.2.11	TLS 1.3 seulement
Modes d'échange de clés prépartagées	psk_key_exchange_modes	RFC 8446 [6] sec 4.2.9	TLS 1.3 seulement
Indication de renégociation	renegotiation_info	RFC 5746 (en anglais seulement) [16]	TLS 1.2 seulement
Indication du nom de serveur	server_name	RFC 6066 [12] sec 3	
Algorithmes de signature	signature_algorithms	RFC 8446 [6] sec 4.2.3	
Groupes pris en charge	supported_groups	RFC 8422 (en anglais seulement) [17] sec 5.1.1, RFC 7919 (en anglais seulement) [18]	Renommé à partir de « elliptic_curves »
Formats des points pris en charge	ec_point_formats	RFC 8422 [17] sec 5.1.2	TLS 1.2 seulement
Versions prises en charge	supported_versions	RFC 8446 [6] sec 4.2.1	TLS 1.3 seulement
Information sur la transparence	transparency_info	RFC 9162 (en anglais seulement) [19] sec 6.5	
Indication d'AC approuvée	trusted_ca_keys	RFC 6066 [12] sec 6	TLS 1.2 seulement

Remarque : N'activez pas les extensions dans vos configurations qui ne font pas partie de la liste présentée ci-dessus.

Nous recommandons que les serveurs et les clients TLS abandonnent les extensions indiquées dans le tableau 6.

[c] Le terme « *master secret* » est parfois utilisé au lieu du terme « *main secret* » dans certaines références au sujet du protocole TLS.

Table 6: Extensions TLS abandonnées

Nom de l'extension	Point de code d'extension	Références	Justification
Signature numérique de l'horodatage des certificats	signed_certificate_timestamp	RFC 6962 (en anglais seulement) [20]	Rendu désuet par l'extension « transparency_info ».

3.3 Authentification client et serveur

Le client doit valider le certificat du serveur en suivant la procédure de vérification précisée par les documents RFC 5280 [5] et RFC 8446 [6]. La révocation du certificat doit être vérifiée à l'aide de la liste de révocation de certificats ou du protocole de vérification de certificat en ligne (OCSP pour *Online Certificate Status Protocol*) et le client devrait vérifier que le certificat s'affiche dans un journal de transparence des certificats conformément au document RFC 9162 Certificate Transparency Info Version 2.0 [19]. Le client doit vérifier qu'il y a bel et bien dans le certificat une valeur dans l'extension « *Subject Alternative Name* » ou dans le champ « *Subject Distinguished Name* » qui correspond au DNS ou à l'adresse IP demandée.

Si le client a inclus l'extension des algorithmes de signature de certificat, il devrait vérifier que l'algorithme de signature de certificat correspond à une des valeurs proposées. Autrement, le client devrait vérifier que l'algorithme de signature de certificat correspond à une des valeurs proposées dans l'extension des algorithmes de signature.

Finalement, le client devrait vérifier que la longueur de la clé publique dans le certificat respecte les exigences de longueur précisées dans l'ITSP.40.111 [1].

Si l'authentification du client (aussi appelée authentification mutuelle) est configurée, le serveur doit valider le certificat du client selon les documents RFC 5280 [5] et RFC 8446 [6]. Le serveur doit vérifier que le chemin de validation du certificat est relié à l'autorité de certification qui, selon le serveur, validera avec confiance l'accès à la ressource demandée. La révocation du certificat doit être vérifiée au moyen d'une liste de révocation de certificats ou du protocole OCSP. Le serveur devrait vérifier que le certificat contient une valeur dans l'extension « *Subject Alternative Name* » ou dans le champ « *Subject Distinguished Name* » qui correspond à un client autorisé.

Finalement, le serveur devrait vérifier que la longueur de la clé publique dans le certificat respecte les exigences de longueur précisées dans l'ITSP.40.111 [1].

3.4 Autres lignes directrices pour la configuration du protocole TLS

Les clients et les serveurs TLS doivent être configurés de manière à désactiver la compression TLS. Pour ce faire, configurez la méthode de compression normalisée « null ».

En raison de la complexité de l'atténuation du risque d'attaque par rejeu, nous recommandons que les configurations ne prennent pas en charge le mode 0-RTT de la version 1.3 du protocole TLS.

La renégociation de la version 1.2 du TLS sans l'extension d'indication de la renégociation (consultez le document RFC 5746 Transport Layer Security [TLS] Renegotiation Indication Extension [16]) doit être désactivée. De plus, nous recommandons que les serveurs TLS soient configurés de manière à ne pas accepter du tout la renégociation initiée par le client. À la place, ils devraient favoriser l'établissement d'une nouvelle connexion TLS.

Si vous décidez de permettre la reprise de session, dans le cas de la version 1.2 du protocole TLS, nous recommandons d'utiliser la méthode d'identification de session et dans le cas de la version 1.3 du protocole TLS, la reprise de session par l'intermédiaire de clés prépartagées. Pour assurer une confidentialité persistante, les clés prépartagées devraient être utilisées avec le protocole d'échange Diffie-Hellman avec ou sans courbes elliptiques (ECDHE/DHE).

4 Internet Protocol Security (protocole IPsec)

Vous pouvez utiliser la combinaison du protocole IKEv2 (*Internet Key Exchange Protocol Version 2*) et de la sécurité du protocole Internet (IPsec) pour créer un tunnel de transfert de données sécurisé au niveau de la couche réseau. Le protocole IKEv2 établit le matériau de clé sécuritaire qui peut être utilisé dans le protocole IPsec pour sécuriser les données qui sont échangées.

4.1 IKEv2

Le protocole IKEv2 est détaillé dans le document RFC 7296 Internet Key Exchange Protocol Version 2 (IKEv2) (en anglais seulement) [21].

Remarque : Le protocole IKEv1 ne devrait plus être utilisé.

4.1.1 Authentification

Lorsque l'IKEv2 est utilisé pour mettre en place une association de sécurité IPsec dans le but de protéger la confidentialité de l'information PROTÉGÉ A OU PROTÉGÉ B ou encore l'intégrité de l'information NON CLASSIFIÉ, PROTÉGÉ A ou PROTÉGÉ B, des signatures numériques devraient être utilisées pour l'authentification. Les clés prépartagées ne devraient pas être utilisées pour l'authentification.

Le tableau 7 présente la liste des schémas d'authentification qui sont conformes à l'ITSP.40.111 [1].

Table 7: Schémas d'authentification recommandés du protocole IKEv2

Recommandés	Adéquats	Abandonnés
ECDSA avec SHA-256 sur la courbe P-256 ECDSA avec SHA-384 sur la courbe P-384 ECDSA avec SHA-512 sur la courbe P-521 Ed25519 avec le hachage d'identité ED448 avec le hachage d'identité RSASSA-PSS avec une longueur de 3072 bits et SHA-384 RSASSA-PSS avec une longueur de 4096 bits et SHA-384	RSASSA-PKCS1-v1.5 avec une longueur de 3072 bits et SHA-384 RSASSA-PKCS1-v1.5 avec une longueur de 4096 bits et SHA-384	RSASSA-PSS avec une longueur de 2048 bits et SHA-256 RSASSA-PKCS1-v1.5 avec une longueur de 2048 bits et SHA-256

4.1.2 Chiffrement du message

Le tableau 8 présente les algorithmes de chiffrement du message du protocole IKEv2 qui sont conformes à l'ITSP.40.111 [1] lorsqu'ils sont utilisés avec une longueur de clé de 128, 192 ou 256 bits.

Table 8: Algorithmes de chiffrement du message recommandés du protocole IKEv2

Recommandés	Adéquats	Abandonnés
ENCR_AES_GCM_16 ENCR_AES_CCM_16	ENCR_AES_GCM_12 ENCR_AES_CCM_12 ENCR_AES_CBC ENCR_AES_CTR	ENCR_3DES ENCR_CAST

Nous recommandons l'utilisation de l'algorithme de chiffrement avancé (AES pour *Advanced Encryption Standard*) en mode GCM (*Galois/Counter Mode*) pour chiffrer les messages du protocole IKEv2. Si les modes GCM ou CCM (combinaison des modes *Counter* et CBC-MAC) ne sont pas pris en charge, il faut avoir recours à un des mécanismes de protection de l'intégrité présentés à la sous-section 4.1.5.

4.1.3 Échange de clés

Le tableau 9 présente la liste des groupes d'échange de clés du protocole IKEv2 qui sont conformes à l'ITSP.40.111 [1].

Table 9: Groupes d'échange de clés recommandés du protocole IKEv2

Recommandés	Adéquats	Abandonnés
Groupe ECP aléatoire de 256 bits Groupe ECP aléatoire de 384 bits Groupe ECP aléatoire de 521 bits	Groupe MODP de 3072 bits Groupe MODP de 4096 bits Groupe MODP de 6144 bits Groupe MODP de 8192 bits	Groupe MODP de 2048 bits Groupe MODP de 2048 bits avec un sous-groupe d'ordre premier de 224 bits Groupe MODP de 2048 bits avec un sous-groupe d'ordre premier de 256 bits Groupe ECP aléatoire de 224 bits

Dans le cadre de toute application de ce protocole on doit vérifier que les valeurs publiques reçues se situent entre 1 et p-1 et, dans le cas de l'algorithme ECDH, que les valeurs satisfont à l'équation de la courbe elliptique.

Nous recommandons que chacun des échanges de clés soit effectué avec une paire de clés éphémères nouvellement générée pour le protocole ECDH/DH.

4.1.4 Fonctions pseudoaléatoires pour la génération de clés

Le protocole IKEv2 utilise une fonction pseudoaléatoire pour générer du matériau de clé. Le tableau 10 présente la liste des fonctions pseudoaléatoires qui sont conformes à ITSP.40.111 [1].

Table 10: Fonctions pseudoaléatoires adéquates pour la génération de clés du protocole IKEv2

Adéquates
PRF_HMAC_SHA2_256
PRF_HMAC_SHA2_384
PRF_HMAC_SHA2_512
PRF_AES128_CMAC

4.1.5 Protection de l'intégrité

Si vous n'utilisez pas un algorithme de chiffrement authentifié (AEAD pour *Authenticated Encryption with Associated Data*), comme l'AES GCM, pour le chiffrement du message, un mécanisme de protection de l'intégrité supplémentaire est nécessaire. Le tableau 11 présente la liste des mécanismes de protection de l'intégrité qui sont conformes à l'ITSP.40.111 [1].

Table 11: Mécanismes de protection de l'intégrité adéquats et abandonnés pour l'IKEv2

Adéquats	Abandonnés
AUTH_HMAC_SHA2_256_128	AUTH_HMAC_SHA1_160
AUTH_HMAC_SHA2_384_192	
AUTH_HMAC_SHA2_512_256	
AUTH_AES_128_GMAC	
AUTH_AES_192_GMAC	
AUTH_AES_256_GMAC	
AUTH_AES_CMAC_96	

4.1.6 Protocole EAP (*Extensible Authentication Protocol*)

Le document RFC 7396 JSON Merge Patch (en anglais seulement) [22] précise que le protocole d'authentification extensible (EAP pour *Extensible Authentication Protocol*) peut être utilisé dans le cadre du protocole IKEv2 s'il est utilisé avec le mécanisme d'authentification d'IKEv2 basé sur la clé publique du répondeur. Le document RFC 5998 An Extension for EAP-Only Authentication in IKEv2 (en anglais seulement) [23] présente la liste des méthodes qui peuvent être utilisées avec le protocole IKEv2 pour fournir une authentification mutuelle et qui n'exigent pas d'authentification basée sur la clé publique de la part du répondeur.

Bien que plusieurs méthodes d'authentification soient présentées comme des méthodes sécuritaires d'EAP dans le document RFC 5998 [23], nous recommandons que vous utilisiez des méthodes qui prennent en charge la liaison de canaux de communication. Nous recommandons également que vous continuiez d'utiliser l'authentification basée sur la clé publique du répondeur.

4.1.7 Protection contre les attaques par déni de service distribué (DDoS)

L'IKEv2 est souvent sujet aux attaques par déni de service distribué (DDoS). Dans le cadre d'une attaque DDoS, une auteure ou un auteur de menace submerge un répondeur avec un très grand nombre de requêtes pour la création d'une association de sécurité (SA pour *Security Association*) qui sont envoyées à partir d'une adresse IP usurpée laissant ainsi des négociations d'association de sécurité incomplètes.

Vous devriez mettre en œuvre les mesures de protection contre les attaques DDoS décrites dans le document RFC 8019 Protecting IKEv2 Implementations from DDoS Attacks (en anglais seulement) [24]. Plus particulièrement, nous recommandons de réduire la durée de vie des négociations IKE SA incomplètes. Nous recommandons également d'imposer une limite sur le nombre de négociations IKE SA incomplètes permises pour une adresse IP précise et d'introduire des mesures de protection additionnelles lorsque cette limite a été atteinte.

La fragmentation des paquets IP n'est pas recommandée étant donné qu'elle est sujette aux attaques DDOS. À la place, optez pour la fragmentation des paquets IKEv2 et configurez la taille des fragments. Le document RFC 7383 Internet Key Exchange Protocol Version 2 (IKEv2) Message Fragmentation (en anglais seulement) [25] recommande de sélectionner une taille des fragments IKEv2 qui fait en sorte que la taille maximale d'un datagramme est de 1280 octets pour le trafic IPv6 et de 576 octets pour le trafic IPv4.

4.1.8 Durée de vie des clés et de l'authentification

Dans le contexte de l'IKEv2, le remplacement de clé génère du nouveau matériau de clé pour l'association de sécurité IKE ou une association de sécurité enfant (CHILD SA) par l'échange CREATE_CHILD_SA. La réauthentification requiert la création d'une nouvelle association de sécurité IKE. Dans ce cas, les anciennes associations de sécurité sont supprimées.

Nous recommandons que vous vous assuriez que la période de remplacement de clé ou que la durée de vie de la clé de la CHILD SA (y compris les SA du protocole ESP [*Encapsulating Security Payload*]) ne dépasse pas 8 heures. La période de réauthentification ou la durée de vie de l'authentification IKE SA ne devrait pas dépasser 24 heures.

4.1.9 Reprise de session

Le document RFC 5723 Internet Key Exchange Protocol Version 2 (IKEv2) Session Resumption (en anglais seulement) [26] offre un moyen pour permettre aux pairs de reconnecter une connexion brisée en utilisant une IKE SA précédemment établie.

Si vous prenez en charge une reprise de session, la méthode par ticket de référence (*ticket by reference*) est recommandée à la condition qu'on ait confiance que les pairs puissent garder en sécurité l'information stockée liée aux associations de sécurité. Nous recommandons également que vous limitiez la durée de vie du ticket à une durée qui ne dépasse pas la période de remplacement de clé.

4.2 Sécurité du protocole Internet (IPsec)

La sécurité du protocole Internet (IPsec pour *Internet Protocol Security*) est une suite de protocoles réseau qui vise à protéger la confidentialité, l'intégrité et la disponibilité des communications Internet entre les hôtes réseau, les passerelles

et les dispositifs. L'IPsec procure également un contrôle d'accès, une protection contre les attaques par rejeu et une protection contre l'analyse du trafic.

Les hôtes, les passerelles et les dispositifs IPsec devraient être configurés conformément aux directives stipulées dans les documents :

- RFC 4301 Security Architecture for the Internet Protocol (en anglais seulement) [27]
- RFC 4303 IP Encapsulating Security Payload (ESP) (en anglais seulement) [28]
- RFC 7321 Cryptographic Algorithm Implementation Requirements and Usage Guidance for Encapsulating Security Payload (ESP) and Authentication Header (AH) (en anglais seulement) [29]

Des conseils sur la gestion des clés de l'IPsec sont proposés dans le document intitulé NIST SP 800-57 Part 3 Rev 1 [4]. Consultez la section 3 pour des conseils plus élaborés sur l'installation et l'administration de l'IPsec.

4.2.1 Génération de clés

Une association de sécurité IPsec précise le matériau de clé utilisé pour chiffrer les échanges protégés dans une session IPsec précise et fournir une protection de l'intégrité. Une association de sécurité IPsec doit être établie par un échange IKEv2 précédent comme nous l'avons précisé plus haut.

4.2.2 Protection des données et de leur intégrité

L'authentification devrait être effectuée à l'aide de signatures numériques et non pas à partir de clés prépartagées lorsque l'IPsec est utilisé pour protéger la confidentialité de l'information PROTÉGÉ A et PROTÉGÉ B, ou l'intégrité de l'information NON CLASSIFIÉ, PROTÉGÉ A et PROTÉGÉ B. Vous ne devriez pas utiliser les clés prépartagées (PSK pour *Pre-Shared Key*) pour l'authentification.

L'IPsec devrait utiliser le protocole ESP en mode tunnel pour protéger la confidentialité, l'intégrité et la disponibilité des paquets et des en-têtes de paquets. Il faut éviter d'utiliser le protocole d'en-tête d'authentification (AH pour *Authentication Header*). Le protocole AH ne peut pas assurer la protection de la confidentialité.

Le tableau 12 présente les algorithmes de chiffrement des paquets ESP qui sont conformes à l'ITSP.40.111 [1] lorsqu'ils sont utilisés avec une longueur de clé de 128, 192 ou 256 bits.

Table 12: Algorithmes de chiffrement recommandés des paquets ESP

Recommandés	Adéquats	Abandonnés
ENCR_AES_GCM_16 ENCR_AES_CCM_16	ENCR_AES_GCM_12 ENCR_AES_CCM_12 ENCR_AES_CBC ENCR_AES_CTR	ENCR_3DES ENCR_CAST

Nous recommandons que vous utilisiez l'algorithme AES en mode GCM pour le chiffrement des paquets ESP comme le décrit le document RFC 4106 The Use of Galois/Counter Mode (GCM) in IPSec Encapsulating Security Payload (en anglais

seulement) [30]. Si les modes GCM ou CCM ne sont pas pris en charge, un mécanisme de protection de l'intégrité doit être configuré. Le tableau 13 présente la liste des mécanismes de protection de l'intégrité qui sont conformes à l'ITSP.40.111 [1].

Table 13: Mécanismes de protection de l'intégrité adéquats et abandonnés pour le ESP

Adéquats	Abandonnés
AUTH_HMAC_SHA2_256_128 AUTH_HMAC_SHA2_384_192 AUTH_HMAC_SHA2_512_256 AUTH_AES_128_GMAC AUTH_AES_192_GMAC AUTH_AES_256_GMAC AUTH_AES_CMAC_96	AUTH_HMAC_SHA1_160

4.2.3 Protection contre le rejeu

La protection contre le rejeu des suites de protocoles IPsec devrait être utilisée. Si la performance le permet, utilisez la taille de fenêtre anti-rejeu recommandée de 128 paquets.

5 Protocole SSH (Secure Shell)

Le protocole SSH (*Secure Shell*) vise à protéger la confidentialité, l'intégrité et la disponibilité des accès à distance, du transfert de fichiers et de la tunnellisation point à point sur Internet.

Les serveurs et clients SSH devraient être configurés de manière à utiliser la version 2.0 du protocole SSH. SSH est une famille de protocoles précisée dans les documents :

- RFC 4251 The Secure Shell (SSH) Protocol Architecture (en anglais seulement) [31]
- RFC 4252 The Secure Shell (SSH) Authentication Protocol (en anglais seulement) [32]
- RFC 4253 The Secure Shell (SSH) Transport Layer Protocol (en anglais seulement) [33]
- RFC 4254 The Secure Shell (SSH) Connection Protocol (en anglais seulement) [34]

La version 1.0 du protocole SSH présente de sérieuses vulnérabilités. Les administrateurs devraient vérifier qu'elle n'est pas utilisée sur leurs systèmes.

Des conseils sur la gestion des clés SSH sont proposés dans le document intitulé NIST SP 800-57 Part 3 Rev 1 [4]. Consultez la section 10 de ce document pour des conseils plus élaborés sur l'installation et l'administration du protocole SSH.

5.1 Authentification du protocole SSH

Le protocole SSH offre l'option d'authentifier seulement le serveur ou d'effectuer une authentification mutuelle serveur-client.

Vous devriez utiliser l'authentification mutuelle serveur-client. Dans ce cas, le serveur est d'abord authentifié par le protocole de la couche de transport SSH (*SSH Transport Layer Protocol*) et suivi de l'authentification du client par le protocole d'authentification SSH (*SSH Authentication Protocol*).

L'authentification du serveur est effectuée par le biais de la cryptographie à clé publique. L'authentification du client auprès du serveur peut quant à elle être effectuée par divers mécanismes. L'authentification du client qui est basé sur des clés publiques ou l'authentification Kerberos sont préférées aux diverses formes d'authentification à l'aide de mots de passe. Vous ne devriez pas utiliser l'authentification basée sur l'hôte du protocole SSH puisque celle-ci est vulnérable à l'usurpation d'adresse IP.

Si vous utilisez l'authentification par clé publique, vous devriez utiliser des certificats de clés publiques qui sont gérés par un cadre d'ICP tant pour l'authentification du serveur que celle du client.

Un cadre d'ICP fournit la signature numérique des clés par une source fiable ainsi que des fonctions de gestion de clé comme des listes des certificats révoqués (CRL pour *Certificate Revocation List*), des contrôles de la durée de vie des clés et des restrictions d'usage de la clé. Le document RFC 6187 x509.v3 certificates for Secure Shell Authentication (en anglais seulement) [35] décrit l'usage des certificats x509.v3 dans le contexte du protocole SSH.

Comme les clés SSH sont habituellement des clés au niveau du système, les clés devraient être générées lors de l'initialisation de la session pour s'assurer de l'unicité des clés dans l'ensemble des dispositifs et des images de machine virtuelle.

5.2 Redirection de port du protocole SSH

La redirection de port du protocole SSH permet à un hôte d'accéder à un service Internet non sécurisé à partir d'une machine qui réside derrière le serveur et qui agit en tant que passerelle de réseau privé virtuel (RPV) du protocole SSH. La redirection de port devrait être désactivée dans le cadre de comptes d'utilisatrice et d'utilisateur interactifs. Pour les dispositifs qui nécessitent la tunnellisation SSH, le trafic devrait être sécurisé dans un deuxième tunnel (p. ex. en utilisant le protocole IPsec).

5.3 Accès racine du protocole SSH

Vous devriez désactiver les connexions à distance des comptes d'utilisateurs racines (*root*).

5.4 Sélection des paramètres du protocole SSH

Dans la présente section, vous trouverez des détails concernant les algorithmes cryptographiques recommandés pour le protocole SSH qui sont conformes aux conseils en matière de cryptographie de l'ITSP.40.111 [1] et qui respectent les recommandations du document NIST SP 800-57 Part 3 Rev 1 [4]. Nous vous recommandons de suivre les conseils en matière de cryptographie pour le protocole de la couche de transport SSH fournis à la section 10.2.1 de ce dernier document.

5.4.1 Sélection de l'algorithme de chiffrement

N'utilisez pas le mode de chiffrement par chaînage de blocs (CBC pour *Cipher Block Chaining*) dans le cadre du protocole SSH. Le mode CBC est vulnérable aux attaques de récupération de texte clair. Le document RFC 4344 The Secure Shell (SSH) Transport Layer Encryption Modes (en anglais seulement) [36] recommande d'utiliser le mode de chiffrement basé sur un compteur (CTR pour *Counter*) au lieu du mode CBC dans le cadre du protocole SSH. Mieux encore, les algorithmes de chiffrement authentifié avec données associées (AEAD), comme l'AES GCM, protègent l'authenticité et la confidentialité. D'autant plus qu'en utilisant un algorithme AEAD, vous n'avez pas besoin d'utiliser un algorithme MAC (*Message Authentication Code*) séparé.

Le tableau 14 présente la liste des algorithmes de chiffrement SSH qui sont conformes aux conseils en matière de cryptographie de l'ITSP.40.111 [1].

Table 14: Algorithmes de chiffrement recommandés du protocole SSH

Recommandés	Adéquats	Abandonnés
AEAD_AES_128_GCM AEAD_AES_256_GCM	aes128-ctr aes192-ctr aes256-ctr	cast128-ctr 3des-ctr

Les algorithmes de chiffrement authentifiés AEAD GCM sont vulnérables à la réutilisation de nonce. Vous devriez vous assurer que chaque message chiffré utilise une paire (clé, nonce) unique.

5.4.2 Sélection de l'algorithme de code d'authentification de message (MAC)

En plus des algorithmes de chiffrement authentifiés AEAD présentés plus haut, vous trouverez au tableau 15, la liste des algorithmes MAC pour le protocole SSH qui correspondent aux conseils en matière de cryptographie fournis dans l'ITSP.40.111 [1].

Table 15: Algorithmes MAC adéquats et abandonnés du protocole SSH

Adéquats	Abandonnés
hmac-sha2-256 hmac-sha2-512	hmac-sha1

5.4.3 Algorithmes d'échange de clés

Le tableau 16 présente la liste des algorithmes d'échange de clé du protocole SSH qui sont conformes aux conseils en matière de cryptographie de l'ITSP.40.111 [1].

Table 16: Algorithmes d'échange de clé recommandés du protocole SSH

Recommandés	Adéquats	Abandonnés
ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 ecmqv-sha2 gss-nistp256-sha256-* gss-nistp384-sha384-* gss-nistp521-sha512-*	diffie-hellman-group15-sha512 diffie-hellman-group16-sha512 diffie-hellman-group17-sha512 diffie-hellman-group18-sha512 gss-group15-sha512-* gss-group16-sha512-* gss-group17-sha512-* gss-group18-sha512-*	rsa2048-sha256 diffie-hellman-group14-sha256 gss-group14-sha256-*

Le protocole SSH permet le renouvellement de clés de session par le client ou par le serveur. Comme le décrit le document RFC 4344 [36], l'horaire de remplacement de clé est basé sur un délai ou sur un volume de données [36].

Pour éviter les collisions MAC, le document RFC 4344 [36] recommande un remplacement de clé après avoir reçu 2^{32} paquets lorsqu'on utilise un numéro de séquence de 32 bits.

5.4.4 Algorithme de clé publique

Le protocole SSH permet facultativement d'assurer l'authentification au moyen de clés publiques. Le tableau 17 présente la liste des algorithmes de clé publique du protocole SSH qui sont conformes aux conseils en matière de cryptographie de l'ITSP.40.111 [1].

Table 17: Algorithmes de clé publique recommandés du protocole SSH

Recommandés	Adéquats	Abandonnés
ecdsa-sha2-nistp256 ecdsa-sha2-nistp384 ecdsa-sha2-nistp521 ssh-ed25519 ssh-ed448 x509v3-ecdsa-sha2-nistp256 x509v3-ecdsa-sha2-nistp384 x509v3-ecdsa-sha2-nistp521	rsa-sha2-256 rsa-sha2-512 x509v3-rsa2048-sha256	x509v3-ecdsa-sha2-nistp224

6 Protocole SNMP (*Simple Network Management Protocol*)

Le protocole de gestion de réseau simple (SNMP pour *Simple Network Management Protocol*) est conçu pour gérer et surveiller des dispositifs sur un réseau informatique. La plus récente version, SNMPv3, est précisée dans :

- An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks. Request for Comments (RFC) 3411 (en anglais seulement) [37]
- Message Processing and Dispatching for the Simple Network Management Protocol (SNMP). Request for Comments (RFC) 3412 (en anglais seulement) [38]
- Simple Network Management Protocol (SNMP) Applications. Request for Comments (RFC) 3413 (en anglais seulement) [39]
- User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3). Request for Comments (RFC) 3414 (en anglais seulement) [40]
- View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP). Request for Comments (RFC) 3415 (en anglais seulement) [41]
- Protocol Operations for the Simple Network Management Protocol (SNMP). Request for Comments (RFC) 3416 (en anglais seulement) [42]
- Transport Mappings for the Simple Network Management Protocol (SNMP). Request for Comments (RFC) 3417 (en anglais seulement) [43]
- Management Information Base (MIB) for the Simple Network Management Protocol (SNMP). Request for Comments (RFC) 3418 (en anglais seulement) [44]

La version SNMPv3 apporte des améliorations sur le plan de la sécurité par rapport à des versions antérieures (p. ex. SNMPv1, SNMPv2, SNMPv2c, SNMPv2u et SNMPv2*). Toutes les versions SNMP antérieures à SNMPv3 devraient être abandonnées.

Le protocole SNMPv3 ajoute des capacités en matière de sécurité et de configuration à distance aux versions antérieures et introduit un nouveau modèle de contrôle d'accès. L'architecture SNMPv3 présente deux mécanismes de sécurité : le modèle de sécurité basé sur les utilisatrices et utilisateurs (USM pour U*ser-based Security Model*) et le modèle de sécurité basé sur le transport (TSM pour *Transport Security Model*).

L'utilisation du modèle USM est définie dans le document RFC 3414 User-based Security Model (USM) for version 3 of the Simple Network Management Protocol [40]. L'utilisation du modèle TSM est définie pour les protocoles TLS/DTLS dans le document RFC 6353 Transport Layer Security (TLS) Transport Model for the Simple Network Management Protocol (SNMP) (en anglais seulement) [45] et pour le protocole SSH dans le document RFC 5592 Secure Shell Transport Model for the Simple Network Management Protocol (SNMP) (en anglais seulement) [46]. Le modèle TSM permet d'avoir un contrôle d'accès basé sur les utilisatrices et utilisateurs similaire à celui offert par le modèle USM. Le document RFC 3415 View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP) [41] définit un processus permettant de contrôler l'accès à l'information de gestion en fonction de groupes ayant une sécurité et des droits d'accès spécifiques.

6.1 Interfaces et contrôle d'accès pour le protocole SNMPv3

Nous recommandons de permettre l'accès aux interfaces du protocole SNMP uniquement à partir d'un réseau d'entreprise interne. En plus, un réseau local (LAN pour Local Area Network) ou réseau local virtuel (VLAN pour Virtual LAN) dédié aux fonctions administratives et distinct du trafic réseau régulier dans les autres portions du réseau d'entreprise interne devrait être utilisé pour accéder à ces interfaces. Si un accès externe s'avère nécessaire, nous recommandons que l'accès à l'interface soit accordé uniquement par le biais d'un tunnel IPsec.

Nous vous recommandons de désactiver le protocole SNMP sur tout dispositif qui n'est pas géré activement. Une attention particulière doit être portée aux nouveaux dispositifs sur lesquels le protocole SNMP aurait pu être activé par défaut.

Les mises en œuvre du protocole SNMP peuvent offrir deux modèles de sécurité : USM et TSM. On compte trois niveaux de sécurité pour les messages :

- sans authentification et sans confidentialité (noAuthNoPriv),
- avec authentification, mais sans confidentialité (authNoPriv),
- avec authentification et avec confidentialité (authPriv).

Nous recommandons l'utilisation du modèle TSM comme modèle de sécurité lorsqu'il est offert. Des recommandations spécifiques pour le modèle TSM sont décrites à la section 6.3 Modèle de sécurité TSM. Le recours au modèle USM est suffisant au niveau de sécurité authPriv s'il est configuré en suivant les recommandations de la section 6.2 Modèle de sécurité USM du protocole SNMPv3.

Nous vous recommandons d'imposer des restrictions sur l'accès en lecture/écriture à l'information de gestion et de n'accorder cet accès qu'à un nombre limité de groupes administratifs. Nous recommandons également de préciser explicitement dans la configuration l'information accessible à chaque utilisatrice ou utilisateur. Nous ne recommandons pas d'utiliser uniquement une restriction d'accès globale à l'information à diffusion restreinte. Les configurations devraient être périodiquement passées en revue afin de déterminer si les niveaux d'accès attribués aux groupes ainsi qu'aux utilisatrices et utilisateurs sont encore adéquats.

6.2 Modèle de sécurité USM du protocole SNMPv3

Le modèle de sécurité USM (*User-Based Security Model*) du protocole SNMPv3 décrit dans le RFC 3414 [40] offre l'authentification et la confidentialité pour les messages SNMPv3. Le modèle USM a été conçu pour fonctionner indépendamment des autres infrastructures de sécurité existantes, et il peut fonctionner lorsque d'autres infrastructures de sécurité de réseau ne sont pas accessibles. Lors de la configuration de groupes, d'utilisatrices et d'utilisateurs, nous recommandons que le niveau de sécurité requis soit réglé au niveau authPriv pour s'assurer que l'authentification et la confidentialité seront appliquées. Les algorithmes recommandés pour l'authentification et la confidentialité sont définis dans les sections 6.2.1 Algorithmes d'authentification du modèle USM du protocole SNMPv3 et 6.2.2 Algorithmes de confidentialité du modèle USM su protocole SNMPv3 respectivement.

6.2.1 Algorithmes d'authentification du modèle USM du protocole SNMPv3

Le protocole SNMPv3 permet l'authentification de messages à l'aide de codes d'authentification de message avec hachage de clé (HMAC pour *Keyed-Hash Message Authentication Code*). Le tableau 18 présente la liste des algorithmes qui sont conformes aux conseils en matière de cryptographie de l'ITSP.40.111 [1]. L'option usmNoAuthProtocol ne fournit aucune authentification et ne devrait donc pas être utilisée.

Table 18: Algorithmes d'authentification adéquats et abandonnés pour le modèle USM du protocole SNMPv3

Adéquats	Abandonnés
usmHMAC192SHA256AuthProtocol usmHMAC256SHA384AuthProtocol usmHMAC384SHA512AuthProtocol	usmHMAC128SHA224AuthProtocol usmHMACSHAAuthProtocol usmHMACMD5AuthProtocol

6.2.2 Algorithmes de confidentialité du modèle USM du protocole SNMPv3

Le modèle USM offre une protection de la confidentialité des données par chiffrement de message. Le tableau 19 présente la liste des algorithmes qui sont conformes aux conseils en matière de cryptographie de l'ITSP.40.111 [1]. L'option usmNoPrivProtocol ne fournit aucune protection de la confidentialité et ne devrait donc pas être utilisée.

Si la méthode recommandée de génération de salage pour la construction des vecteurs d'initialisation (IV pour *Initialization Vector*) qui est recommandée dans le document RFC 3826 The Advanced Encryption Standard (AES) Cipher Algorithm in the SNMP User-based Security Model (en anglais seulement) [47] n'est pas utilisée, les mises en œuvre devraient faire appel à une méthode pour s'assurer que les IV soient imprévisibles conformément à l'ITSP.40.111 [1].

Table 19: Mécanismes de protection de la confidentialité adéquats et abandonnés pour le modèle USM du protocole SNMPv3

Adéquats	Abandonnés
usmAesCfb128Protocol	usmNoPrivProtocol usmDESPrivProtocol

6.2.3 Secrets liés à l'authentification et à la confidentialité du modèle USM

Choisir de fortes valeurs secrètes d'utilisatrice et d'utilisateur et protéger celles-ci contre la divulgation sont deux mesures essentielles pour l'authentification et la protection de la confidentialité dans le cadre du modèle USM.

Nous recommandons que les valeurs secrètes utilisées pour l'authentification et la protection de la confidentialité dans le modèle USM soient basées sur une clé prépartagée générée de façon aléatoire plutôt que sur un mot de passe choisi par une utilisatrice ou un utilisateur. Si de tels mots de passe sont utilisés, ils devraient répondre aux exigences énoncées dans les documents Guide sur l'authentification des utilisateurs dans les systèmes de technologie de l'information (ITSP.30.031 v3) [48] et Pratiques exemplaires de création de phrases de passe et de mots de passe (ITSAP.30.032) [49]. Nous recommandons fortement de ne pas utiliser les mêmes valeurs secrètes à la fois pour la protection de la confidentialité et pour l'authentification.

Nous recommandons que les valeurs secrètes d'utilisatrices et d'utilisateurs ne soient jamais stockées sur un dispositif pouvant exécuter les services de chiffrement et d'authentification du protocole SNMP. Plutôt, seules les clés localisées

dérivées de ces valeurs secrètes par la manière décrite dans le RFC 3414 [40] devraient être stockées sur de tels dispositifs. Nous recommandons aux organismes de créer un système permettant de gérer de manière sécuritaire les valeurs secrètes d'utilisatrices et d'utilisateurs.

Nous recommandons que les clés localisées d'une utilisatrice ou d'un utilisateur soient dérivées et configurées localement, par le biais de l'interface de configuration, sur chaque dispositif géré. Les clés localisées devraient être configurées immédiatement après la création du nouvel utilisateur, car aucune clé par défaut ne devrait être utilisée pour chiffrer ou authentifier des messages.

Si les clés localisées d'une utilisatrice ou d'un utilisateur sont compromises sur un dispositif, nous recommandons à cet utilisateur de ne pas directement changer les clés compromises, mais de changer plutôt les valeurs secrètes et d'utiliser l'interface de configuration afin de générer de nouvelles clés à partir de ces valeurs secrètes.

Si de nouvelles configurations d'utilisatrice ou d'utilisateur sont créées en clonant une configuration préexistante, comme il est défini dans RFC 3414 [40], nous recommandons que la configuration faisant l'objet du clonage ait un accès minimal à l'information de gestion et ne soit pas autorisée à envoyer des messages sur le réseau.

Nous recommandons que les valeurs secrètes d'utilisatrices et d'utilisateurs soient mises à jour périodiquement en suivant les recommandations établies dans l'ITSP.30.031 [48] ou prescrites en vertu de la politique organisationnelle sur les mots de passe.

6.3 Modèle de sécurité TSM

Le modèle de sécurité TSM du protocole SNMPv3 décrit dans le document RFC 5591 Transport Security Model for the Simple Network Management Protocol (SNMP) (en anglais seulement) [50] s'appuie sur l'utilisation d'autres protocoles de transport sécurisé pour l'authentification mutuelle, la liaison de clés, la confidentialité et l'intégrité. RFC 5591 dicte comment les protocoles de transport sécurisé comme SSH, DTLS et TLS peuvent servir à sécuriser le trafic SNMPv3 de façon à atteindre un des niveaux de sécurité mentionnés dans la section 6.1 Interfaces et contrôle d'accès pour le protocole SNMPv3.

Le modèle TSM est un bon choix pour les organismes qui ont déjà déployé un ICP de certificats X.509 ou prévoient le faire. L'utilisation du modèle TSM exclut la nécessité de gérer des clés privées du modèle USM. Les organismes qui utilisent le modèle TSM peuvent envisager de maintenir une configuration du modèle USM équivalente comme sauvegarde, plus particulièrement si le protocole de transport sécurisé est rendu inopérable en raison d'un réseau surchargé ou non disponible. Si le recours au modèle USM est permis comme solution de rechange, son utilisation devrait être journalisée et signalée immédiatement aux administratrices et administrateurs comme comportement suspect.

6.3.1 SNMPv3 avec (D)TLS

Le RFC 6353 [45] explique les recommandations générales pour la configuration du protocole SNMPv3 lorsque les protocoles TLS ou DTLS sont utilisés dans le cadre du modèle de sécurité TSM. Lors de l'utilisation des protocoles TLS ou DTLS, les recommandations de la section 3 Protocole de sécurité de la couche de transport devraient être suivies pour atteindre un niveau de sécurité équivalent au niveau authPriv et pour s'assurer que des services adéquats de chiffrement et d'authentification sont appliqués. Les suites de chiffrement acceptables sont indiquées au Table 1: Suites de chiffrement

recommandées pour la version 1.2 du protocole TLS et au tableau 2 Table 2: Groupes pris en charge par TLS qui sont conformes à l'ITSP.40.111.

Comme il est mentionné dans le document RFC 6353 [45], une extension subjectAltName d'un certificat devrait être utilisée pour associer chaque certificat à son identifiant de sécurité (securityName) du protocole SNMP.

L'algorithme de hachage choisi pour générer les empreintes numériques « SnmpTLSFingerprint » d'un certificat devrait résister aux collisions et respecter les conseils en matière de cryptographie de l'ITSP.40.111 [1].

6.3.2 SNMPv3 avec SSH

L'utilisation du protocole SSH avec SNMPv3 est précisée dans RFC 5592 [46] et nous vous recommandons de suivre les lignes directrices d'élaboration d'un tunnel SSH détaillées dans la section 5 Protocole SSH (Secure Shell) pour assurer la confidentialité et l'intégrité. Les mécanismes acceptables pour l'authentification des clients sont donnés dans le tableau 17 du présent document.

Il faut s'assurer que le protocole SSH n'est pas configuré de manière à omettre la vérification de la clé publique.

6.4 SNMPv3 avec tunnel IPsec

Un tunnel IPsec peut être utilisé pour protéger le trafic SNMPv3 déjà configuré en vertu des modèles USM ou TSM comme recommandé ci-dessus. Les recommandations pour l'établissement d'un tunnel IPsec sont définies dans la section 4 Internet Protocol Security (protocole IPsec).

6.5 Notifications du protocole SNMPv3 : « trap » et informatives

Les notifications « trap » et informatives devraient être transmises de manière sécuritaire. Les mises en œuvre peuvent faire appel à une différente configuration pour les notifications. Lors de la configuration du niveau de sécurité USM pour les notifications, nous recommandons fortement l'utilisation du même niveau de sécurité que nous avons utilisé pour les commandes SNMPv3, mais protégé par un différent ensemble de clés.

6.6 Processus de découverte SNMPv3

Le processus de découverte SNMPv3 consiste en au moins une requête et permet à une entité SNMP d'obtenir l'identité configurée d'une autre entité lorsqu'elles communiquent ensemble pour la première fois.

La seconde requête de découverte visant à déterminer l'horloge de l'entité gérée est authentifiée et peut être effectuée aussi souvent que nécessaire pour assurer la synchronisation de l'heure (même si la requête initiale n'a pas été effectuée).

Lorsque le modèle USM est utilisé, la requête et la réponse initiales du processus de découverte ne sont pas authentifiées ou chiffrées. Cela signifie que la réponse qui contient l'identité de l'entité pourrait être mystifiée ou modifiée par un agent malveillant. Lorsque le modèle TSM est utilisé, tous les messages de découverte sont authentifiés et chiffrés.

Les entités SNMP qui font des requêtes de découverte devraient soit :

- maintenir une liste d'identités avec leurs adresses de réseau pour éviter d'avoir à faire la requête initiale ou
- faire la requête initiale dans un tunnel IPsec pour qu'elle soit protégée de manière cryptographique.

7 Secure/Multipurpose Internet Mail Extensions (S/MIME)

Le protocole S/MIME (*Secure/Multipurpose Internet Mail Extensions*) est une norme visant à protéger la confidentialité, l'intégrité et l'authenticité des messages électroniques transmis sur Internet.

Vous devriez utiliser la version 4.0 de S/MIME qui est décrite dans les documents RFC 8551 Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 4.0 Message Specification (en anglais seulement) [51] et RFC 8550 Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 4.0 Certificate Handling (en anglais seulement) [52]. La version 4.0 de S/MIME prend en charge l'algorithme AES GCM.

Le document RFC 5753 Use of Elliptic Curve Cryptography (ECC) Algorithms in Cryptographic Message Syntax (CMS) (en anglais seulement) [53] fournit des conseils sur l'utilisation de la cryptographie à courbe elliptique (ECC pour *Elliptic Curve Cryptography*) dans le format CMS (*Cryptographic Message Syntax*) aux fins de génération de signatures numériques et d'échange de clés pour le chiffrement ou l'authentification des messages.

Pour traiter le contenu HTML et les messages multi-parties ou mixtes (*multi part/mixed*), les fournisseurs de logiciels devraient mettre en œuvre des mécanismes d'isolation multi-parties avec des considérations de sécurité, comme il est expliqué dans le document RFC 8551 [51]. Jusqu'à ce que ces isolations à parties multiples soient prises en charge, les clients S/MIME doivent être configurés de manière à désactiver le téléchargement de contenu à distance ou pour n'afficher que les messages en texte simple.

7.1 Algorithmes d'empreinte numérique (*Digest*)

Les algorithmes d'empreinte numérique sont utilisés par S/MIME pour la création de l'empreinte numérique du corps d'un message ou dans le contexte d'un algorithme de signature. Le tableau 20 présente la liste des algorithmes d'empreinte numérique qui sont conformes aux conseils en matière de cryptographie de l'ITSP.40.111 [1].

Table 20: Algorithmes d'empreinte numérique du protocole S/MIME adéquats et abandonnés

Adéquats	Abandonnés
SHA-256 SHA-384 SHA-512 SHA3-256 SHA3-384 SHA3-512	SHA-224 SHA3-224

Utiliser SHA-1 pour générer des signatures numériques n'est pas conforme aux conseils en matière de cryptographie de l'ITSP.40.111 [1]. Dans le cas de S/MIME 3.2 et des versions précédentes, SHA-1 ne devrait pas être utilisé en tant qu'algorithme d'empreinte numérique pour signer des messages.

7.2 Algorithmes de signature

Chaque algorithme de signature devrait être utilisé avec un algorithme d'empreinte numérique. Le tableau 21 présente la liste des algorithmes de signature qui sont conformes aux conseils en matière de cryptographie de l'ITSP.40.111 [1] lorsqu'ils sont utilisés avec un des algorithmes d'empreinte numérique de la section 7.1.

Table 21: Algorithmes de signature S/MIME recommandés

Recommandés	Adéquats	Abandonnés
ECDSA avec la courbe NIST P-256 ECDSA avec la courbe NIST P-384 ECDSA avec la courbe NIST P-521 EdDSA avec la courbe 25519 RSASSA PSS avec un modulo de 3072 bits ou plus grand	RSASSA PKCS1v1.5 avec un modulo d'au moins 3072 bits	ECDSA avec la courbe NIST P-224 RSASSA PSS avec un modulo de 2048 bits RSASSA PKCS1v1.5 avec un modulo d'au moins 2048 bits DSA avec n'importe quelle taille de groupe

Nous recommandons d'utiliser le RSASSA-PSS (*RSA Signature Scheme with Appendix - Probabilistic Signature Scheme*), au lieu du PKCS #1 v1.5, en tant que mécanisme d'encodage pour les signatures numériques RSA. Cette recommandation s'applique autant aux certificats X.509, comme précisé dans le document RFC 5756 Updates for RSAES-OAEP and RSASSA-PSS Algorithm Parameters (en anglais seulement) [54], qu'aux types de contenu de données signées (*signed-data*), comme indiqué dans le document RFC 4056 Use of the RSASSA-PSS Signature Algorithm in Cryptographic Message Syntax (CMS) (en anglais seulement) [55]. Si vous effectuez des signatures à l'aide de plusieurs algorithmes de signature, les mises en œuvre devraient utiliser l'attribut de syntaxe de message chiffré (CMS) « multipleSignatures » comme précisé dans le document RFC 5752 Multiple Signatures in Cryptographic Message Syntax (CMS) (en anglais seulement) [56].

Les mises en œuvre RSASSA-PSS devraient protéger contre les attaques de substitution d'algorithme de hachage. Ces mises en œuvre devraient vérifier que l'algorithme de hachage utilisé pour calculer l'empreinte numérique du contenu du message est le même algorithme que celui utilisé pour calculer l'empreinte numérique des attributs signés.

7.3 Algorithmes de chiffrement de clé

La majorité des algorithmes de chiffrement de clé du protocole S/MIME exigent qu'un algorithme d'enveloppement de clé soit spécifié en tant que paramètre. Vous trouverez à la sous-section 7.3.1 les algorithmes d'enveloppement de clé acceptables. Le tableau 22 présente la liste des algorithmes de chiffrement de clé qui sont conformes aux conseils en matière de cryptographie de l'ITSP.40.111 [1].

Table 22: Algorithmes de chiffrement de clé S/MIME recommandés

Recommandés	Adéquats	Abandonnés
dhSinglePass stdDH SHA256 KDF avec la courbe NIST P-256 dhSinglePass stdDH SHA384 KDF avec la courbe NIST P-384 dhSinglePass stdDH SHA512 KDF avec la courbe NIST P-521	RSAES OAEP avec un modulo d'au moins 3072 bits dhSinglePass cofactorDH SHA256 KDF avec la courbe NIST P-256 dhSinglePass cofactorDH SHA384 KDF avec la courbe NIST P-384 dhSinglePass cofactorDH SHA512 KDF avec la courbe NIST P-521 mqvSinglePass SHA256 KDF avec la courbe NIST P-256 mqvSinglePass SHA384 KDF avec la courbe NIST P-384 mqvSinglePass SHA512 KDF avec la courbe NIST P-521	dhSinglePass stdDH SHA224 KDF avec la courbe NIST P-224 dhSinglePass cofactorDH SHA224 KDF avec la courbe NIST P-224 RSA KEM avec un modulo d'au moins 2048 bits RSAES OAEP avec un modulo de 2048 bits RSAES PKCS1v1.5 avec un modulo d'au moins 2048 bits

Nous recommandons l'utilisation de l'algorithme standard Diffie-Hellman avec courbes elliptiques, comme précisé dans le document RFC 5753 Use of Elliptic Curve Cryptography (ECC) Algorithms in Cryptographic Message Syntax (CMS) (en anglais seulement) [53].

Si vous utilisez un chiffrement RSA, vous devriez mettre en œuvre le schéma RSAES-OAEP comme précisé dans les documents RFC 3560 Use of the RSAES-OAEP Key Transport Algorithm in Cryptographic Message Syntax (CMS) (en anglais seulement) [57] et RFC 5756 [54], afin d'être conforme aux conseils en matière de cryptographie de l'ITSP.40.111 [1].

Si vous utilisez des mises en œuvre de S/MIME qui permettent le déchiffrement de l'encodage PKCS #1 v1.5, vous devriez mettre en œuvre des mesures d'atténuation telles que la vérification prudente ou le remplissage aléatoire, comme décrit dans le document RFC 3218 Preventing the Million Message Attack on Cryptographic Message Syntax (en anglais seulement) [58].

7.3.1 Algorithmes d'enveloppement de clé

Le tableau 23 présente la liste des algorithmes d'enveloppement de clé qui peuvent être utilisés avec un algorithme de chiffrement de clé approprié conformément aux conseils en matière de cryptographie de l'ITSP.40.111 [1].

Table 23: Algorithmes d'enveloppement de clé S/MIME recommandés

Recommandés	Abandonnés
AES-128 AES-192 AES-256 AES-128 avec algorithme de remplissage AES-192 avec algorithme de remplissage AES-256 avec algorithme de remplissage	3DES CAST5 CMS avec une longueur de clé de 128 bits

7.4 Algorithmes de chiffrement de contenu

Les algorithmes de chiffrement de contenu S/MIME indiqués au tableau 24 sont conformes aux conseils en matière de cryptographie de l'ITSP.40.111 [1].

Table 24: Algorithmes de chiffrement de contenu S/MIME

Recommandés	Abandonnés
AES-128 GCM	AES-128 CBC
AES-192 GCM	AES-192 CBC
AES-256 GCM	AES-256 CBC

8 Programmes d'assurance des technologies commerciales

Les mises en œuvre d'ICP et des protocoles TLS, IPsec, SSH et S/MIME devraient respecter les conseils en matière d'assurance de mise en œuvre proposés à la section 11 du document Algorithmes cryptographiques pour l'information NON CLASSIFIÉ, PROTÉGÉ A et PROTÉGÉ B (ITSP.40.111) [1].

9 Préparation à la cryptographie post-quantique

Les ordinateurs quantiques menacent de percer les cryptosystèmes à clé publique et d'affaiblir les cryptosystèmes symétriques que nous utilisons actuellement. Bien que les technologies quantiques ne soient pas encore suffisamment puissantes pour percer la cryptographie recommandée dans cette publication, d'importants travaux de recherche sont réalisés dans ce domaine. En août 2024, le NIST a publié des normes pour la normalisation de la cryptographie post-quantique. Ces normes sont conçues pour résister aux avantages qu'auront les ordinateurs quantiques à venir. Les organismes qui développent les normes pour les protocoles discutés dans le présent document travaillent actuellement à la révision de ces protocoles afin d'y intégrer la cryptographie post-quantique. Nous prévoyons inclure des recommandations pour la configuration de la cryptographie post-quantique dans une mise à jour du présent document, lorsque les normes révisées auront été finalisées.D'ici là, nous recommandons les étapes de haut niveau suivantes :

- évaluer la sensibilité des renseignements de l'organisation et en déterminer la longévité afin d'identifier les renseignements pouvant être à risque (p. ex. dans le cadre de processus continus d'évaluation des risques);
- passer en revue le budget et le plan de gestion du cycle de vie des TI de l'organisation pour déterminer les mises à jour logicielles et matérielles pouvant s'avérer importantes;
- sensibiliser le personnel à la menace quantique.

Pour obtenir de plus amples renseignements sur la préparation à cet égard, consultez le document Préparez votre organisation à la menace que pose l'informatique quantique pour la cryptographie (ITSAP.00.017) [59].

Les organismes devraient attendre que les normes pour l'utilisation de la cryptographie post-quantique dans les protocoles soient publiées avant de faire une révision des configurations pour protéger l'information ou les systèmes.

10 Résumé

Les protocoles de sécurité cryptographique fournissent des mécanismes de sécurité servant à protéger la disponibilité, la confidentialité et l'intégrité de l'information. Avant de choisir les protocoles que vous comptez utiliser, vous devriez d'abord déterminer quelles sont vos exigences organisationnelles en matière de sécurité. L'utilisation de plusieurs protocoles pourrait être nécessaire afin de satisfaire à une de ces exigences. Vous devriez sélectionner et mettre en œuvre chaque protocole de manière à prendre en charge et répondre aux exigences spécifiques de votre organisation.

11 Contenu complémentaire

11.1 Liste d'abréviations, d'acronymes et de sigles

Abréviation, acronyme ou sigle	Définition
AC	Autorité de certification
AEAD	Chiffrement authentifié avec données associées (*Authenticated Encryption with Associated Data*)
AES	Algorithme de chiffrement avancé (*Advanced Encryption Standard*)
AH	En-tête d'authentification (*Authentication Header*)
ATM	Agent de transfert de messages (*Message Transfer Agent*)
CBC	Chiffrement par chaînage de blocs (*Cipher Block Chaining*)
CMS	Format CMS (*Cryptographic Message Syntax*)
CRL	Liste des certificats révoqués (*Certificate Revocation List*)
CST	Centre de la sécurité des télécommunications
DANE	Protocole DANE (*DNS-based Authentication of Named Entities*)
DDoS	Attaques par déni de service distribué (*Distributed Denial of Service*)
DH	Diffie-Hellman
DNS	Système de noms de domaine (*Domain Name System*)
DTLS	Protocole de datagramme de sécurité de la couche de transport (*Datagram Transport Layer Security*)
ECC	Cryptographie à courbe elliptique (*Elliptic Curve Cryptography*)
ECDH	Protocole Diffie-Hellman avec courbes elliptiques (*Elliptic-Curve Diffie-Hellman*)
ECDHE	Protocole Diffie-Hellman éphémère avec courbes elliptiques (*Ephemeral Elliptic Curve Diffie-Hellman*)
ECDSA	Algorithme de signature numérique avec courbes elliptiques (*Elliptic Curve Digital Signature Algorithm*)
ECP	Groupe de courbe elliptique modulo un nombre premier (*Elliptic Curve Groups modulo a Prime*)
ESP	Protocole ESP (*Encapsulating Security Payload*)
GC	Gouvernement du Canada
GCM	Mode Galois/compteur (*Galois/Counter Mode*)
HMAC	Code d'authentification de message avec hachage de clé (*Keyed-Hash Message Authentication Code*)
HSTS	Protocole HSTS (*HTTP Strict Transport Security*)
ICP	Infrastructure à clé publique
IKE	Échange de clés Internet (*Internet Key Exchange*)
IPsec	Sécurité du protocole Internet (*Internet Protocol Security*)

Abréviation, acronyme ou sigle	Définition
MAC	Code d'authentification de message (*Message Authentication Code*)
NIST	*National Institute of Standards and Technology*
PFS	Confidentialité persistante (*Perfect Forward Secrecy*)
PRF	Fonction pseudoaléatoire (*Pseudo-Random Function*)
PSK	Clé prépartagée (*Pre-shared Key*)
PVMC	Programme de validation des modules cryptographiques
RFC	Demande de commentaires (*Request for Comments*)
RSA	Algorithme RSA (*Rivest-Shamir-Adleman*)
SA	Association de sécurité (*Security Association*)
SCT	Secrétariat du Conseil du Trésor du Canada
SHA	Algorithme de hachage sécurisé (*Secure Hash Algorithm*)
SSH	Protocole SSH (*Secure Shell*)
S/MIME	Norme S/MIME (*Secure Multipurpose Internet Mail Extensions*)
SMTP	Protocole de transfert de courrier simple (*Simple Mail Transfer Protocol*)
SP	Publication spéciale (*Special Publication*)
SSL	Protocole SSL (*Secure Sockets Layer*)
STI	Sécurité des technologies de l'information
TI	Technologies de l'information
TLS	Protocole de sécurité de la couche de transport (*Transport Layer Security*)

11.2 Glossaire

Terme	Définition
Attaque par déni de service distribué (DDoS)	Attaque dans le cadre de laquelle plusieurs systèmes compromis sont utilisés pour attaquer une cible en particulier. Le flux de messages envoyés est tel qu'il provoque une panne du système ciblé et l'interruption des services offerts aux utilisatrices et utilisateurs légitimes.
Attaque par rejeu	Forme d'attaque réseau dans laquelle une transmission de données valide est malicieusement répétée ou retardée par un attaquant qui l'a interceptée.
Authentification	Processus ou mesure permettant de vérifier l'identité d'une utilisatrice ou d'un utilisateur.
Authenticité	Fait d'être authentique, vérifiable et fiable; confiance dans la validité d'une transmission, d'un message ou de l'expéditeur d'un message.

Terme	Définition
Chiffrement	Procédure par laquelle une information est convertie d'une forme à une autre afin d'en dissimuler le contenu et d'en interdire l'accès aux entités non autorisées.
Confidentialité	Capacité à protéger l'information sensible contre tout accès non autorisé.
Confidentialité persistante	Propriété des protocoles d'établissement de clés qui garantit que la compromission d'une clé privée de longue durée ne permettra pas à un adversaire de régénérer les clés ou les sessions enregistrées antérieurement.
Cryptographie	Discipline qui traite des principes, des moyens et des méthodes permettant de rendre des renseignements inintelligibles et de les reconvertir en renseignements cohérents.
Déchiffrement	Conversion en clair de l'information (voix ou données) chiffrée par l'opération inverse du chiffrement.
Disponibilité	Caractéristique de l'information ou des systèmes qui sont accessibles aux personnes autorisées au moment où celles-ci en ont besoin. La disponibilité est un attribut des biens d'information, des logiciels et du matériel informatique (l'infrastructure et ses composantes).
Gestion des clés	Procédures et mécanismes de génération, de distribution, de remplacement, de stockage, d'archivage et de destruction des clés cryptographiques.
Information classifiée	Terme utilisé par le Gouvernement du Canada pour identifier toute information liée à l'intérêt national et qui pourrait faire l'objet d'une exception ou d'une exclusion, mais dont la compromission, selon toute vraisemblance, porterait atteinte à l'intérêt national (p. ex. la défense nationale, les relations avec d'autres pays, des intérêts économiques).
Intégrité	Capacité de protéger l'information contre les modifications ou les suppressions non intentionnelles et inopportunes. L'intégrité permet de savoir si l'information est conforme à ce qu'elle est censée être. Elle s'applique également aux processus opérationnels, à la logique des applications logicielles, au matériel et au personnel.
Signature numérique	Mécanisme cryptographique qui fournit les services d'authentification de l'origine, d'intégrité des données et de non-répudiation du signataire.

11.3 Références

Numéro	Référence
1	Centre canadien pour la cybersécurité, Algorithmes cryptographiques pour l'information NON CLASSIFIÉ, PROTÉGÉ A et PROTÉGÉ B (ITSP.40.111), septembre 2023.
2	Secrétariat du Conseil du Trésor du Canada, Ligne directrice sur la définition des exigences en matière d'authentification, novembre 2012.
3	Centre canadien pour la cybersécurité, La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie (ITSG-33), novembre 2012.
4	National Institute of Standards and Technology, Recommendation for Key Management Part 3: Application-Specific Key Management Guidance Special Publication 800-57 Part 3 Rev 1 (en anglais seulement), janvier 2015.

Numéro	Référence
5	Cooper, D., et al. Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. Request for Comments (RFC) 5280 (en anglais seulement). Internet Engineering Task Force (IETF), mai 2008.
6	Rescorla, E. The Transport Layer Security (TLS) Protocol Version 1.3. Request for Comments (RFC) 8446 (en anglais seulement). Internet Engineering Task Force (IETF), août 2018.
7	Hodges, J., Jackson, C. et Barth, A. HTTP Strict Transport Security (HSTS). Request for Comments (RFC) 6797 (en anglais seulement). Internet Engineering Task Force (IETF), novembre 2012.
8	Hoffman, P. SMTP Service Extension for Secure SMTP over Transport Layer Security. Request for Comments (RFC) 3207 (en anglais seulement). Internet Engineering Task Force (IETF), février 2002.
9	Margolis, D., et al. SMTP MTA Strict Transport Security (MTA-STS). Request for Comments (RFC) 8461 (en anglais seulement). Internet Engineering Task Force (IETF), septembre 2018.
10	Dukhovni, V. et Hardaker, W. SMTP Security via Opportunistic DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS). Request for Comments (RFC) 7672 (en anglais seulement). Internet Engineering Task Force (IETF), octobre 2015.
11	Friedl, S., et al. Transport Layer Security (TLS) Application-Layer Protocol Negotiation Extension. Request for Comments (RFC) 7301 (en anglais seulement). Internet Engineering Task Force (IETF), juillet 2014.
12	Eastlake, D. et tiers. Transport Layer Security (TLS) Extensions: Extension Definitions. Request for Comments (RFC) 6066 (en anglais seulement). Internet Engineering Task Force (IETF), janvier 2011.
13	Gutmann, P. Encrypt-then-MAC for Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS). Request for Comments (RFC) 7366 (en anglais seulement). Internet Engineering Task Force (IETF), septembre 2014.
14	Bhargavan Ed, K., et al. Transport Layer Security (TLS) Session Hash and Extended Master Secret Extension. Request for Comments (RFC) 7627 (en anglais seulement). Internet Engineering Task Force (IETF), septembre 2015.
15	Pettersen, Y. The Transport Layer Security (TLS) Multiple Certificate Status Request Extension. Request for Comments (RFC) 6961 (en anglais seulement). Internet Engineering Task Force (IETF), juin 2013.
16	Ray, M. et Dispensa, S. Transport Layer Security (TLS) Renegotiation Indication Extension. Request for Comments (RFC) 5746 (en anglais seulement). Internet Engineering Task Force (IETF), février 2010.
17	Nir, Y., Josefsson, S. et Pegourie-Gonnard, M. Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS) Versions 1.2 and Earlier. Request for Comments (RFC) 8422 (en anglais seulement). Internet Engineering Task Force (IETF), août 2018.
18	Gillmor, D. Negotiated Finite Field Diffie-Hellman Ephemeral Parameters for Transport Layer Security (TLS) (en anglais seulement). Request for Comments (RFC) 7919. Internet Engineering Task Force (IETF), août 2016.
19	Laurie, B., Messeri, E. and Stradling, R. Certificate Transparency Version 2.0. Request for Comments (RFC) 9162. Internet Engineering Task Force (IETF) (en anglais seulement), décembre 2021.
20	Laurie, B., Langley, A. and Kasper, E. Certificate Transparency. Request for Comments (RFC) 6962 (en anglais seulement). Internet Engineering Task Force (IETF), juin 2013.
21	Kaufman, C. et al. Internet Key Exchange Protocol Version 2 (IKEv2). Request for Comments (RFC) 7296 (en anglais seulement). Internet Engineering Task Force (IETF), octobre 2014.
22	Hoffman, P. et Snell, J. JSON Merge Patch. Request for Comments (RFC) 7396 (en anglais seulement). Internet Engineering Task Force (IETF), octobre 2014.

Numéro	Référence
23	Eronen, P. et Tschofenig, H. An Extension for EAP-Only Authentication in IKEv2. Request for Comments (RFC) 5998 (en anglais seulement). Internet Engineering Task Force (IETF), septembre 2010.
24	Nir, Y. et Smyslov, V. Protecting IKEv2 Implementations from Distributed Denial-of-Service Attacks. Request for Comments (RFC) 8019 (en anglais seulement). Internet Engineering Task Force (IETF), novembre 2016.
25	Smyslov, V. Internet Key Exchange Protocol Version 2 (IKEv2) Message Fragmentation. Request for Comments (RFC) 7383 (en anglais seulement). Internet Engineering Task Force (IETF), novembre 2014.
26	Sheffer, Y. et Tschofenig, H. Internet Key Exchange Protocol Version 2 (IKEv2) Session Resumption. Request for Comments (RFC) 5723 (en anglais seulement). Internet Engineering Task Force (IETF), janvier 2010.
27	Kent, S. et Seo, K. Security Architecture for the Internet Protocol. Request for Comments (RFC) 4301 (en anglais seulement). Internet Engineering Task Force (IETF), décembre 2005.
28	Kent, S. IP Encapsulating Security Payload (ESP). Request for Comments (RFC) 4303 (en anglais seulement). Internet Engineering Task Force (IETF), décembre 2005.
29	McGrew, D. et Hoffman, P. Cryptographic Algorithm Implementation Requirements and Usage Guidance for Encapsulating Security Payload (ESP) and Authentication Header (AH) (en anglais seulement). Request for Comments (RFC) 7321. Internet Engineering Task Force (IETF), août 2014.
30	Viega, J. et McGrew, D. The Use of Galois Counter Mode (GCM) in IPSec Encapsulating Security Payload. Request for Comments (RFC) 4106 (en anglais seulement). Internet Engineering Task Force (IETF), juin 2005.
31	Ylonen, T. et Lonvick, C., Ed. The Secure Shell (SSH) Protocol Architecture. Request for Comments (RFC) 4251 (en anglais seulement). Internet Engineering Task Force (IETF), janvier 2006.
32	Ylonen, T. et Lonvick, C., Ed. The Secure Shell (SSH) Authentication Protocol. Request for Comments (RFC) 4252 (en anglais seulement). Internet Engineering Task Force (IETF), janvier 2006.
33	Ylonen, T. et Lonvick, C., Ed. The Secure Shell (SSH) Transport Layer Protocol. Request for Comments (RFC) 4253 (en anglais seulement). Internet Engineering Task Force (IETF), janvier 2006.
34	Ylonen, T. et Lonvick, C., Ed. The Secure Shell (SSH) Connection Protocol. Request for Comments (RFC) 4254 (en anglais seulement). Internet Engineering Task Force (IETF), janvier 2006.
35	Igoe, K. et Stebila, D. x509.v3 certificates for Secure Shell Authentication. Request for Comments (RFC) 6187 (en anglais seulement). Internet Engineering Task Force (IETF), mars 2011.
36	Bellare, M., Kohno, T. et Namprempre, C. The Secure Shell (SSH) Transport Layer Encryption Modes. Request for Comments (RFC) 4344 (en anglais seulement). Internet Engineering Task Force (IETF), janvier 2006.
37	Harrington, D., Presuhn, R. et Wijnen, B. An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks. Request for Comments (RFC) 3411 (en anglais seulement). Internet Engineering Task Force (IETF), décembre 2002.
38	Case, J., et al. Message Processing and Dispatching for the Simple Network Management Protocol (SNMP). Request for Comments (RFC) 3412 (en anglais seulement). Internet Engineering Task Force (IETF), décembre 2002.
39	Levi, D., Meyer, P. et Stewart, B. Simple Network Management Protocol (SNMP) Applications. Request for Comments (RFC) 3413 (en anglais seulement). Internet Engineering Task Force (IETF), décembre 2002.
40	Blumenthal, U. et Wijnen, B. User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3). Request for Comments (RFC) 3414 (en anglais seulement). Internet Engineering Task Force (IETF), décembre 2002.

Numéro	Référence
41	Wijnen, B., Presuhn, R. et McCloghrie, K. View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP). Request for Comments (RFC) 3415 (en anglais seulement). Internet Engineering Task Force (IETF), décembre 2002.
42	Presuhn, R., et al. Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP). Request for Comments (RFC) 3416 (en anglais seulement). Internet Engineering Task Force (IETF), décembre 2002.
43	Presuhn, R., et al. Transport Mappings for the Simple Network Management Protocol (SNMP). Request for Comments (RFC) 3417 (en anglais seulement). Internet Engineering Task Force (IETF), décembre 2002.
44	Presuhn, R., et al. Management Information Base (MIB) for the Simple Network Management Protocol (SNMP). Request for Comments (RFC) 3418 (en anglais seulement). Internet Engineering Task Force (IETF), décembre 2002.
45	Hardaker, W. Transport Layer Security (TLS) Transport Model for the Simple Network Management Protocol (SNMP). Request for Comments (RFC) 6353 (en anglais seulement). Internet Engineering Task Force (IETF), juillet 2011.
46	Harrington, D., Salowey, J. et Hardaker, W. Secure Shell Transport Model for the Simple Network Management Protocol (SNMP). Request for Comments (RFC) 5592 (en anglais seulement). Internet Engineering Task Force (IETF), juin 2009.
47	Blumenthal, U., Maino, F. and McCloghrie, K. The Advanced Encryption Standard (AES) Cipher Algorithm in the SNMP User-based Security Model. Request for Comments (RFC) 3826 (en anglais seulement). Internet Engineering Task Force (IETF), juin 2004.
48	Centre canadien pour la cybersécurité, Guide sur l'authentification des utilisateurs dans les systèmes de technologie de l'information (ITSP.30.031) v3, avril 2018.
49	Centre canadien pour la cybersécurité, Pratiques exemplaires de création de phrases de passe et de mots de passe (ITSAP.30.032), septembre 2019.
50	Harrington, D. et Hardaker, W. Transport Security Model for the Simple Network Management Protocol (SNMP). Request for Comments (RFC) 5591 (en anglais seulement). Internet Engineering Task Force (IETF), juin 2009.
51	Schaad, J., Ramsdell, B. et Turner, S. Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 4.0 Message Specification. Request for Comments (RFC) 8551 (en anglais seulement). Internet Engineering Task Force (IETF), avril 2019.
52	Schaad, J., Ramsdell, B. et Turner, S. Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 4.0 Certificate Handling. Request for Comments (RFC) 8550 (en anglais seulement). Internet Engineering Task Force (IETF), avril 2019.
53	Turner, S. et Brown, D. Use of Elliptic Curve Cryptography (ECC) Algorithms in Cryptographic Message Syntax (CMS). Request for Comments (RFC) 5753 (en anglais seulement). Internet Engineering Task Force (IETF), janvier 2010.
54	Turner, S., et al. Updates for RSAES-OAEP and RSASSA-PSS Algorithm Parameters. Request for Comments (RFC) 5756 (en anglais seulement). Internet Engineering Task Force (IETF), janvier 2010.
55	Schaad, J. Use of the RSASSA-PSS Signature Algorithm in Cryptographic Message Syntax (CMS). Request for Comments (RFC) 4056 (en anglais seulement). Internet Engineering Task Force (IETF), juin 2005.
56	Turner, S. and Schaad, J. Multiple Signatures in Cryptographic Message Syntax (CMS). Request for Comments (RFC) 5752 (en anglais seulement). Internet Engineering Task Force (IETF), janvier 2010.
57	Housley, R. Use of the RSAES-OAEP Key Transport Algorithm in Cryptographic Message Syntax (CMS). Request for Comments (RFC) 3560 (en anglais seulement). Internet Engineering Task Force (IETF), juillet 2003.
58	Rescorla, E. Preventing the Million Message Attack on Cryptographic Message Syntax. Request for Comments (RFC) 3218 (en anglais seulement). Internet Engineering Task Force (IETF), janvier 2002.

Numéro	Référence
59	Centre canadien pour la cybersécurité, Préparez votre organisation à la menace que pose l'informatique quantique pour la cryptographie - ITSAP.00.017. février 2021.