Centre de la sécurité des télécommunications
Communications Security Establishment

CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

CONSEILS SUR LA CONFIGURATION SÉCURISÉE DES PROTOCOLES RÉSEAU

(Version 2)

PRATICIENS

TLP:WHITE

Canada

AVANT-PROPOS

Le présent document *Conseils sur la configuration sécurisée des protocoles réseau* (ITSP.40.062) 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*. Les configurations du présent document sont conformes aux exigences cryptographiques de l'ITSP.40.111 [1].

DATE D'ENTRÉE EN VIGUEUR

Le présent document entre en vigueur le 21 septembre 2020.

HISTORIQUE DES RÉVISIONS

Révision	Modifications	Date
1	Première diffusion.	2 août 2016
2	Mise à jour (version 2).	13 octobre 2020

APERÇU

L'information contenue dans le présent document détermine et décrit les protocoles de sécurité acceptables et la façon dont ceux-ci doivent 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.

La prestation des programmes et des services d'un organisme repose essentiellement sur sa capacité à transmettre les données et l'information sensibles en toute sécurité. 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 intervenants, de même que la non-répudiation. Différents protocoles peuvent s'avérer nécessaires pour satisfaire aux exigences de sécurité et le respect de toutes ces exigences exige parfois la mise en œuvre de chacun de ces protocoles.

Pour de plus amples renseignements sur la configuration sécurisée des protocoles réseau, veuillez communiquer avec le :

Centre d'appel du Centre canadien pour la cybersécurité

contact@cyber.gc.ca

(613) 949-7048 ou 1-833-CYBER-88

TABLE DES MATIÈRES

LISTE DES FIGURES

LISTE DES TABLEAUX

1 INTRODUCTION

Les organismes dépendent de systèmes de technologies de l'information (TI) pour atteindre leurs objectifs organisationnels. Ces systèmes interconnectés sont souvent l'objet de sérieuses menaces et de cyberattaques susceptibles de nuire à l'authenticité, à la confidentialité et à l'intégrité des ressources d'information. La compromission des réseaux, des systèmes et de l'information peut avoir des effets néfastes sur les activités de l'organisme et peut entraîner des fuites de données et des pertes pécuniaires.

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[1];
- les algorithmes approuvés que le Centre pour la cybersécurité 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.[2] Il est de la responsabilité des organismes que de déterminer leurs objectifs et leurs exigences en matière de sécurité dans le cadre de leur gestion du risque.

1.1 PROCESSUS DE GESTION DES RISQUES EN SÉCURITÉ DES TI

Lors de la mise en place de protocoles de sécurité, les praticiens doivent tenir compte des activités relatives à la gestion des risques en sécurité des TI qui sont décrites à l'ITSG-33 intitulé *Gestion des risques liés à la sécurité des TI – Une méthode axée sur le cycle de vie* [3]. L'ITSG-33 propose un ensemble d'activités de gestion des risques pour deux niveaux organisationnels, le niveau ministériel et celui des systèmes d'information. Il comprend également un catalogue de mesures de contrôle de la sécurité (c.-à-d. des exigences de sécurité normalisées qui permettent de protéger la confidentialité, l'intégrité et l'authenticité 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 pour en savoir plus sur celles-ci.

---

[1] Dans le cas d'un ministère ou d'un organisme du GC, l'orientation fournie peut être appliquée aux systèmes et à l'information dont la classification est 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.

[2] 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].

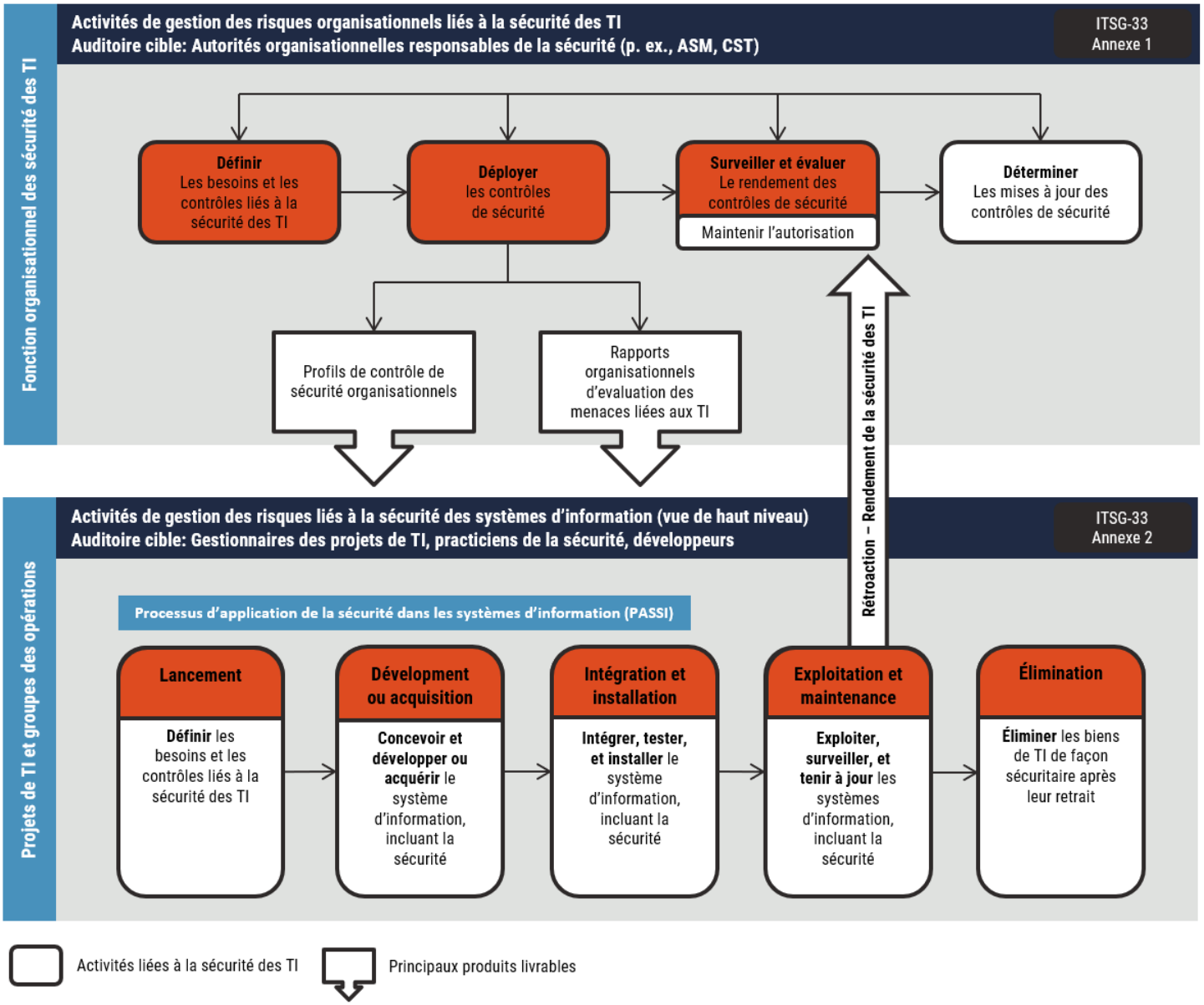

Figure 1 Processus de gestion des risques liés à la sécurité des TI

1.2 RECOMMANDATIONS

Tout au long du présent document, nous présentons des recommandations selon trois catégories : les configurations *recommandées*, *adéquates et abandonnées*. Vous trouverez plus de détails sur ces catégories dans le tableau 1 ci-dessous.

Tableau 1 : Les trois catégories de recommandation des configurations utilisées dans le présent document.

Recommandées	Adéquates	Abandonnées
Les configurations inscrites dans la colonne *recommandées* présentent des avantages que celles de la colonne *adéquates* n'ont pas. Les configurations *recommandées* doivent toujours être mises en place si le profil de connexion à distance le permet.	Les configurations de la colonne *adéquates* sont appropriées pour fournir le soutien nécessaire au profil des connexions à distance. Les configurations *adéquates* doivent être mises en place si les configurations *recommandées* ne peuvent l'être.	Les configurations de la colonne *abandonnées* sont mûres 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 à mettre en place doivent permettre de limiter la surface d'attaque du réseau.

2 INFRASTRUCTURE À CLÉ PUBLIQUE (ICP)

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* [4]. Nous vous recommandons les conseils sur l'installation et sur l'administration de l'ICP fournis à la section 2 de ce document.

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

Les certificats de clé publique doivent respecter le format du certificat X.509 version 3 établi dans les appels de commentaires du document RFC 5280, Internet X.509 *Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile* [5].

Les mises en œuvre des protocoles doivent prendre en charge de multiples certificats ainsi que les 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'agrément de clés ou de chiffrement de clés doivent se distinguer par l'extension d'usage de clé servant à déterminer l'une des valeurs suivantes :

- digitalSignature;
- keyEncipherment;
- keyAgreement.

Conformément aux conseils en matière de chiffrement fournis dans l'ITSP.40.111 [1], la fonction de hachage cryptographique SHA-1 ne doit pas être utilisée pour générer ou vérifier des signatures numériques au moyen de certificats de clé publique.

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 le serveur et les applications clients.

Conformément au document *RFC 8446 The Transport Layer Security (TLS) Protocol Version 1.3* [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 élargir la compatibilité, pour se conformer aux audits internes ou pour surveiller les menaces qui pèsent contre les systèmes. 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) doivent prendre en charge le protocole HSTS (*HTTP Strict Transport Security*) conformément au document RFC 6797 *HTTP Strict Transport Security (HSTS)* [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*) doit 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* [8]. Pour s'assurer de l'utilisation du protocole TLS pour le trafic SMTP, les ATM doivent prendre en charge les protocoles MTA-STS conformément au document *RFC 8461 SMTP MTA Strict Transport Security (MTA-STS)* et être configurés en mode « renforcé » (*enforce* en anglais) de contrôle d'application des politiques [35] ou encore prendre en charge, au moyen du protocole DANE (*DNS-Based Authentication of Named Entities*), la sécurité du SMTP conformément au document RFC 7672 *SMTP Security via Opportunistic DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS)* [9].

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 (voir la section 6 du présent document).

Lorsque le protocole TLS est utilisé pour protéger la confidentialité de l'information de type PROTÉGÉ A et PROTÉGÉ B, ou l'intégrité de l'information NON CLASSIFIÉ, PROTÉGÉ A et PROTÉGÉ B, les mises en œuvre doivent 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 doit être configuré pour prendre en charge seulement les suites de chiffrements listées au tableau 2 ci-dessous.

Tableau 2 : 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 doit 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 3 ci-dessous.

Tableau 3 : 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_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_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_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 effectuer des déploiements des protocoles 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.

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 de session sont conformes aux exigences quant à la longueur de la clé spécifiées à ITSP.40.11 [1]. Vous trouverez dans le tableau 4 la liste des groupes pris en charge qui sont conformes à ITSP.40.111 [1].

Tableau 4 : Groupes pris en charge qui sont conformes à l'ITSP.40.111

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

Le tableau 5 présente la liste des algorithmes de signature qui sont conformes à l'ITSP.40.111 [1].

Tableau 5 : Algorithmes de signature qui sont conformes à l'ITSP.40.111

Recommandés	Adéquats	Abandonnés
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
rsa_pss_pss_sha256		dsa_sha256
rsa_pss_pss_sha384		dsa_sha384
rsa_pss_pss_sha512		dsa_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 suivantes :

- Algorithmes de certificat de signature;
- Demandes d'interrogation d'état de certificats;
- Témoin (TLS 1.3 seulement);
- Chiffrer avant MAC (EtM pour *Ecrypt-then-MAC*) (TLS 1.2 seulement);
- Clé de session étendue (*Extended Master Secret*) (TLS 1.2 seulement);
- Partage de clé (TLS 1.3 seulement);
- État de certificat multiple (*Multiple Certificate Status*) (TLS 1.2 seulement);
- Clé prépartagé (TLS 1.3 seulement);
- Modes d'échange de clé prépartagée (TLS 1.3 seulement);
- Indication de renégociation (TLS 1.2 seulement);
- Indication du nom de serveur (SNI);
- Algorithmes de signature;
- Liste des certifications des signatures électroniques des horodateurs;
- Groupes pris en charge;
- Formats des points EC pris en charge (TLS 1.2 seulement);
- Versions prises en charge (TLS 1.3 seulement);
- Indication d'autorité de certification fiable (TLS 1.2 seulement).

Remarque : N'activez pas les extensions dans vos configurations qui ne font pas partie des listes présentées plus haut.

3.3 AUTHENTIFICATION CLIENT ET SERVEUR

Selon les documents RFC 5280 [5] et RFC 8446 [6], le client doit valider le certificat du serveur. 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). Le client doit vérifier qu'il y a bel et bien dans le certificat une valeur dans l'extension « Nom Alternatif du Sujet » ou dans le champ « Nom Distinct du Sujet » qui correspond au DNS ou à l'adresse IP demandée.

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

Finalement, le client doit 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 d'accès du certificat de validation 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 de liste de révocation de certificats ou du protocole OCSP. Le serveur doit 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 client doit vérifier que la longueur de la clé publique dans le certificat respecte les exigences de longueur précisées dans l'ITSP.40.11 [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* [10]) 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 dans le but d'établir une nouvelle connexion TLS.

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

4 SÉCURITÉ DU PROTOCOLE INTERNET (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 matériel de clé sécuritaire qui peut être utilisé dans le protocole IPsec pour sécuriser les données qui sont échangées.

4.1 PROTOCOLE IKEv2

Le protocole IKEv2 est détaillé dans le document *RFC 7296 Internet Key Exchange Protocol Version 2 (IKEv2)* [11].

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 doivent être utilisées pour l'authentification et non pas les clés prépartagées.

Vous trouverez au tableau 6, la liste des schèmes d'authentification qui sont conformes à ITSP.40.111 [1].

Tableau 6 : Schèmes 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 RSASSA-PSS avec une longueur en bits de 3072 et SHA-384 RSASSA-PSS avec une longueur en bits de 4096 et SHA-384	RSASSA-PKCS1-v1.5 avec une longueur en bits de 3072 et SHA-384 RSASSA-PKCS1-v1.5 avec une longueur en bits de 4096 et SHA-384	RSASSA-PSS avec une longueur en bits de 2048 et SHA-256 RSASSA-PKCS1-v1.5 avec une longueur en bits de 2048 et SHA-256

4.1.2 CHIFFREMENT DU MESSAGE

Le tableau 7 présente les algorithmes de chiffrement du message du protocole IKEv2 qui sont conformes à l'ITSP.40.111 [1].

Tableau 7 : 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 4.1.6 (voir plus bas).

4.1.3 ÉCHANGE DE CLÉS

Le tableau 8 présente la liste des groupes d'échange de clés du protocole IKEv2 qui sont conforme à l'ITSP.40.111 [1].

Tableau 8 : 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 des courbes elliptiques.

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

4.1.4 FONCTIONS PSEUDO-ALÉATOIRES POUR LA GÉNÉRATION DE CLÉS

Le protocole IKEv2 utilise une fonction pseudo-aléatoire pour générer des éléments de mise en clé de chiffrement. Le tableau 9 présente la liste des fonctions pseudo-aléatoires qui sont conformes à ITSP.40.111 [1].

Tableau 9 : Fonctions pseudo-aléatoires adéquates de 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 DU PROTOCOLE IKEv2

Si vous n'utilisez pas un algorithme de chiffrement authentifié (AEAD), comme le Galois/Counter Mode, pour le chiffrement du message, un mécanisme de protection de l'intégrité supplémentaire est nécessaire. Le tableau 10 présente la liste des mécanismes de protection de l'intégrité qui sont conformes à l'ITSP.40.111 [1].

Tableau 10 : Mécanismes de protection de l'intégrité adéquats et abandonnés

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 EXTENSIBLE AUTHENTICATION PROTOCOL (EAP)

Le document *RFC 7396 JSON Merge Patch* [13] précise que l'EAP (*Extensible Authentication Protocol*) du protocole IKEv2 peut être utilisé avec l'authentification basée sur la clé publique du répondeur du IKEv2. Le document *RFC 5998 An Extension for EAP-Only Authentication in IKEv2* [14] 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* [14], nous recommandons que vous utilisiez des méthodes qui prennent en charge la liaison de canaux. Nous recommandons également que vous continuiez d'utiliser l'authentification basée sur la clé publique du répondeur.

4.1.7 PROTECTION CONTRE LE DÉNI DE SERVICE DISTRIBUÉ (DDOS)

L'IKEv2 est sujette aux attaques par Déni de service distribué (DDoS). Dans le cadre d'une attaque DDoS, un auteur malveillant submerge un répondeur avec un très grand nombre de requêtes qui sont envoyées à partir d'une adresse IP faussée laissant ainsi des négociations incomplètes.

Pour vous protéger des attaques DDoS, vous devez configurer le protocole IKEv2 pour que la durée de vie des négociations IKE SA (association de sécurité) incomplètes ou le nombre maximal d'échanges de négociation soient permis jusqu'à un certain niveau pour une adresse IP précise avant que des mesures de protection soient prises. Vous devez mettre en place les mesures de protection décrites au document *RFC 8019 Protecting IKEv2 Implementations from DDoS Attacks* [15].

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.

Dans le document *RFC 7383 Internet Key Exchange Protocol Version 2 (IKEv2) Message Fragmentation* [16], la taille maximale recommandée 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 DE LA CLÉ ET DE L'AUTHENTIFICATION

Dans le contexte de l'IKEv2, la remise à la clé crée de nouveaux éléments de mise en clé de chiffrement pour l'association de sécurité IKE ou une association de sécurité enfant (CHILD SA) par l'échange CREATE_CHILD_SA. La ré-authentification requiert un échange complet et crée une nouvelle IKE SA. Dans ce cas, les anciens échanges d'association de sécurité sont supprimés.

Nous recommandons que vous vous assuriez que la période de remise en clé ou que la durée de vie de la clé de la CHILD SA (y compris les associations de sécurité du protocole de charge utile de sécurité d'encapsulation – ESP pour *Encapsulated Security Payload*) ne dépasse pas 8 heures. La période de ré-authentification ou la durée de vie de l'authentification IKE SA ne doit pas dépasser 24 heures.

4.1.9 REPRISE DE SESSION

Le document *RFC 5723 Internet Key Exchange Protocol Version 2 (IKEv2) Session Resumption* [17] 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 le temps nécessaire pour la remise à la 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 l'authenticité des communications Internet entre les hôtes réseau, les passerelles et les dispositifs. L'IPsec procure également un contrôle d'accès, une protection contre les tentatives de rejeu et la protection contre l'analyse du trafic.

Les hôtes, les passerelles et les dispositifs IPsec doivent être configurés de manière à utiliser le protocole IPsec conformément aux directives stipulées dans les documents *RFC 4301 Security Architecture for the Internet Protocol* [18], *RFC 4303 IP Encapsulating Security Payload (ESP)* [19] et *RFC 7321 Cryptographic Algorithm Implementation Requirements and Usage Guidance for Encapsulating Security Payload (ESP) and Authentication Header (AH)* [20].

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]. Le Centre pour la cybersécurité recommande de suivre les conseils sur l'installation et l'administration de l'IPsec fournis à la section 3 de ce dernier document.

4.2.1 GÉNÉRATION DE CLÉS

Une association de sécurité IPsec précise les éléments de mise en clé utilisés pour chiffrer les échanges protégés dans une session IPsec précise et pour 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 DE L'INTÉGRITÉ DES DONNÉES

L'authentification doit être effectuée à partir 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.

L'IPsec doit utiliser le protocole ESP en mode tunnel pour protéger la confidentialité, l'intégrité et l'authenticité des paquets et des en-têtes de paquets. Il faut éviter d'utiliser l'en-tête d'authentification (AH pour *Authentication Header*) puisqu'il ne permet pas de protéger la confidentialité.

Le tableau 11 présente la liste des algorithmes de chiffrement des paquets ESP qui sont conformes à ITSP.40.111 [1].

Tableau 11 : 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* [18]. Si les modes GCM ou CCM ne sont pas pris en charge, un mécanisme de protection de

l'intégrité doit être configuré. Le tableau 12 présente la liste des mécanismes de protection de l'intégrité qui sont conformes à l'ITSP.40.111 [1].

Tableau 12 : Mécanismes de protection de l'intégrité adéquats et abandonnés

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 doit être utilisée. Si la performance le permet, utilisez la taille de fenêtre anti-rejeu recommandée de 128 paquets.

5 PROTOCOLE SECURE SHELL (SSH)

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

Les serveurs et clients SSH doivent être configurés de manière à utiliser la version 2.0 du protocole SSH conformément aux documents *RFC 4251 The Secure Shell (SSH) Protocol Architecture* [21], *RFC 4252 The Secure Shell (SSH) Authentication Protocol* [22], *RFC 4253 The Secure Shell (SSH) Transport Layer Protocol* [23] et *RFC 4254 The Secure Shell (SSH) Connection Protocol* [24].

La version 1.0 du protocole SSH présente de sérieuses vulnérabilités. Les administrateurs doivent vérifier qu'elle ne tourne pas 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]. Le Centre pour la cybersécurité recommande de suivre les conseils sur l'installation et l'administration du protocole SSH fournis à la section 10 de ce document.

5.1 AUTHENTIFICATION DU PROTOCOLE SSH

Le protocole SSH offre à la fois l'authentification serveur seulement et l'authentification mutuelle serveur-client.

Vous devez utiliser l'authentification mutuelle serveur-client. Dans ce cas, le serveur est d'abord authentifié par le protocole de couche de transport et suivi de l'authentification du client par le protocole d'authentification SSH.

L'authentification du serveur est effectuée avec une cryptographie à clé publique. L'authentification du client auprès du serveur peut quant à elle être effectuée avec divers mécanismes. L'authentification du client qui est basé sur des clés publiques ou l'authentification Kerberos sont préférées à plusieurs autres formes d'authentification à l'aide de mots de passe. Il faut éviter d'utiliser l'authentification non interactive par clé publique du protocole SSH puisque celle-ci est vulnérable aux adresses IP faussées.

Si vous utilisez l'authentification par clé publique, vous devez 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. Ce cadre propose également des fonctions de gestion de clé comme des listes des certificats révoqués (CRL), des contrôles de la durée de vie de la clé et des restrictions d'usage de la clé. Le document *RFC 6187 x509.v3 certificates for Secure Shell Authentication* [25] recommande l'utilisation de certificats x509.v3 dans le cadre du protocole SSH.

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

5.2 REDIRECTION DE PORT DU PROTOCOLE SSH

Avec la redirection de port du protocole SSH, un hôte peut 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 du protocole SSH. La redirection de port doit être désactivée dans le cadre d'utilisateurs de comptes interactifs. Pour les dispositifs qui nécessitent la tunnellisation SSH, l'activité réseautique devrait être sécurisée dans un autre tunnel (p. ex., IPsec).

5.3 ACCÈS RACINE DU PROTOCOLE SSH

Vous devez désactiver les connexions à distance des comptes d'utilisateurs racines.

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 chiffrement de l'ITSP.40.111 [1] et qui respectent les recommandations du document *NIST SP 800-57 Part 3 Rev 1* [4]. Le Centre pour la cybersécurité recommande de suivre les conseils en matière de chiffrement du protocole de couche de transport SSH fournis à la section 10.2.1 de ce document.

5.4.1 SÉLECTION DE L'ALGORITHME DE CHIFFREMENT

Le mode d'enchaînement de blocs de chiffrement (CBC) ne doit pas être utilisé avec le protocole SSH puisque ce dernier est vulnérable aux attaques par récupération du texte en clair. Dans le document *RFC 4344 The Secure Shell (SSH) Transport Layer Encryption Modes* [26], on recommande d'utiliser le mode de chiffrement basé sur un compteur (CTR) du protocole SSH au lieu du mode CBC. Il vaut encore mieux d'utiliser des algorithmes de chiffrement authentifié (AEAD), comme l'AES GCM, qui protège l'authenticité et la confidentialité. D'autant plus qu'en utilisant un algorithme AEAS, vous n'avez pas besoin d'utiliser un algorithme MAC séparé.

Le tableau 13 présente la liste des algorithmes de chiffrement du protocole SSH qui satisfont aux conseils en matière de chiffrement fournis dans l'ITSP.40.111 [1].

Tableau 13 : 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 devez vous assurer de l'unicité de la paire (clé, nonce) pour chaque message chiffré.

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 14, la liste des algorithmes MAC pour le protocole SSH qui correspondent aux conseils en matière de chiffrement fournis dans l'ITSP.40.11 [1].

Tableau 14 : 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 15 présente la liste des algorithmes d'échange de clé du protocole SSH qui sont conformes aux conseils en matière de chiffrement de l'ITSP.40.111 [1].

Tableau 15 : 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* [26], l'horaire de remise à la clé est basé sur un délai ou sur un volume de données.

Pour éviter les collisions MAC, au document *RFC 4344* [26] on recommande une remise à la clé après avoir reçu 2^{32} paquets lorsqu'on utilise une séquence de nombre de 32 bits.

5.4.4 ALGORITHMES DE CLÉ PUBLIQUE

Le protocole SSH permet facultativement d'assurer l'authentification au moyen de clés publiques. Le tableau 16 présente la liste des algorithmes de clé publique du protocole SSH qui sont conformes aux conseils en matière de chiffrement de l'ITSP.40.111 [1].

Tableau 16 : Algorithmes de clé publique recommandés du protocole SSH

Recommandés	Adéquats	Abandonnés
ecdsa-sha2-nistp256 ecdsa-sha2-nistp384 ecdsa-sha2-nistp521 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 SECURE/MULTI-PURPOSE 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.

Comme indiqué aux documents *RFC 8551 Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 4.0 Message Specification* [27] et *RFC 8550 Secure/Multipurpose Internet Mail Extensions (S/MIME)* [28], *vous devez utiliser la version 4.0 de* S/MIME qui comprend d'ailleurs une prise en charge de l'AES-GCM.

Des conseils sur l'utilisation de la cryptographie à courbe elliptique (CCE) dans la spécification CMS aux fins de génération de signatures numériques et d'échange de clés pour le chiffrement ou l'authentification des messages sont fournis dans le document *RFC 5753 Use of Elliptic Curve Cryptography (ECC) Algorithms in Cryptographic Message Syntax (CMS)* [29].

Les fournisseurs de logiciels doivent mettre en place des mécanismes d'isolation multiparties avec des considérations de sécurité pour traiter le contenu HTML et les messages multiparties ou mixtes (multi-part/mixed), comme discuté au document *RFC 8551* [27]. Jusqu'à ce que ces isolations à parties multiples soient prises en charge, les clients S/MIME doivent être configurés de manière à désactiver l'affichage de contenu à distance ou pour n'afficher que les messages en texte en clair.

6.1 ALGORITHMES D'EMPREINTE NUMÉRIQUE (*DIGEST*)

Les algorithmes d'empreinte numérique sont utilisés en S/MIME pour créer un condensé du message ou en tant que partie d'un algorithme de signature. Le tableau 15 présente la liste des algorithmes de condensé de message qui sont conformes aux conseils en matière de chiffrement de l'ITSP.40.111 [1].

Tableau 17 : Algorithmes de condensé de message 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 chiffrement de l'ITSP.40.111 [1]. Dans le cas de S/MIME 3.2 et des versions précédentes, SHA-1 ne doit pas être utilisé en tant qu'algorithme Digest pour signer des messages.

6.2 ALGORITHMES DE SIGNATURE

Des algorithmes de signature doivent être utilisés en parallèle d'un algorithme d'empreinte numérique. Le tableau 18 présente la liste des algorithmes de signature, qui sont pairés à un algorithme d'empreinte numérique de la section 6.1. Ces algorithmes de signature sont conformes aux conseils en matière de chiffrement de l'ITSP.40.111 [1].

Tableau 18 : Paires d'algorithmes de signature et d'empreinte numérique recommandées

Recommandées	Adéquates	Abandonnées
ECDSA avec la courbe NIST P-256 ECDSA avec la courbe NIST P-384 ECDSA avec la courbe NIST P-521 RSASSA PSS avec un modulo de 3072 bits ou plus grand	RSASSA PKCS1v1.5 avec un modulo de 3072 bits ou plus DSA avec un modulo de 3072 bits ou un plus grand groupe	ECDSA avec la courbe NIST P-224 RSASSA PSS avec un modulo de 2048 bits RSASSA PKCS1v1.5 avec un modulo de 2048 bits DSA avec un groupe de 2048 bits

Nous recommandons d'utiliser un schéma de signature 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 le précise le document *RFC 5756 Updates for RSAES-OAEP and RSASSA-PSS Algorithm Parameters* [30], qu'aux types de contenu de données signées, comme indiqué dans le document *RFC 4056 Use of the RSASSA-PSS Signature Algorithm in Cryptographic Message Syntax (CMS)* [31]. Si vous effectuez des signatures à partir de plusieurs algorithmes de signature, vous devez utiliser l'attribut de syntaxe de message chiffré (CMS) « MultipleSignatures » comme précisé au document *RFC 5752 Multiple Signatures in Cryptographic Message Syntax (CMS)* [32].

Les applications RSASSA-PSS doivent protéger contre les attaques de substitution d'algorithmes de hachage. Elles doivent vérifier que l'algorithme de hachage utilisé pour calculer l'empreinte numérique du contenu du message est le même algorithme de hachage utilisé pour calculer l'empreinte numérique des attributs signés.

6.3 ALGORITHMES DE CHIFFREMENT DE CLÉ

La majorité des algorithmes de chiffrement du protocole S/MIME exige de paramétrer un algorithme d'emballage de clé précis. Vous trouverez les algorithmes d'emballage de clé acceptés à la section 6.3.1 du présent document. Le tableau 19 présente la liste des algorithmes de chiffrement de clé qui sont conformes aux conseils en matière de chiffrement de l'ITSP.40.111 [1].

Tableau 19 : Algorithmes de chiffrement de clé 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 de 3072 bits ou plus 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 de 2048 bits ou plus RSAES OAEP avec un modulo de 2048 bits RSAES PKCS1v1.5 avec un modulo de 2048 bits ou plus

Nous recommandons l'utilisation d'une courbe elliptique normale Diffie-Hellman, comme précisé dans le document *RFC 5753 Use of Elliptic Curve Cryptography (ECC) Algorithms in Cryptographic Message Syntax (CMS)* [33].

Si vous utilisez un chiffrement RSA, vous devez mettre en place le schéma RSAES-OAEP comme précisé aux documents *RFC 3560 Use of the RSAES-OAEP Key Transport Algorithm in Cryptographic Message Syntax (CMS)* [34] et *RFC 5756 Updates for RSAES-OAEP and RSASSA-PSS Algorithm Parameters* [30], afin d'être conforme aux conseils en matière de chiffrement de l'ITSP.40.111 [1].

Si vous utilisez un protocole S/MIME qui permet le déchiffrement de PKCS #1 v1.5, vous devez mettre en place une vérification de la clé de chiffrement du contenu (CEK) et un remplissage aléatoire en tant que mesures d'atténuation, comme décrit au document *RFC 3218 Preventing the Million Message Attack on Cryptographic Message Syntax* [36].

6.3.1 ALGORITHMES D'EMBALLAGE DE CLÉ

Le tableau 20 présente la liste des algorithmes d'emballage de clé qui peuvent être utilisés avec un algorithme de chiffrement approprié conformément aux conseils en matière de chiffrement de l'ITSP.40.111 [1].

Tableau 20 : Algorithmes d'emballage de clé 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

6.4 ALGORITHMES DE CHIFFREMENT DE CONTENU

Les algorithmes de chiffrement ci-dessous sont appropriés pour le chiffrement de contenu S/MIME et sont conformes aux conseils en matière de chiffrement de l'ITSP.40.111 [1].

Tableau 21 : Algorithmes de chiffrement de contenu

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

7 PROGRAMMES D'ASSURANCE DES TECHNOLOGIES COMMERCIALES

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

8 RÉSUMÉ

Les protocoles de sécurité cryptographique fournissent des mécanismes de sécurité servant à protéger l'authenticité, la confidentialité et l'intégrité l'information. Avant de choisir les protocoles à mettre en place, les organismes doivent d'abord déterminer quelles sont leurs exigences en matière de sécurité. Les exigences de chacun varient et plusieurs protocoles sont à leur disposition. La sélection et la mise en place de chaque protocole doivent être effectuées de manière à soutenir l'organisme et à satisfaire à ses exigences.

8.1 COORDONNÉES DU CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

Pour obtenir de plus amples renseignements sur la configuration sécurisée des protocoles réseau, veuillez communiquer avec nous par courriel ou par téléphone :

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

9 CONTENU COMPLÉMENTAIRE

9.1 LISTE D'ABRÉVIATIONS

Terme	Définition
AC	Autorité de certification
AEAD	Chiffrement AEAD (*Authenticated Encryption with Associated Data*)
AES	Norme avancée de chiffrement (*Advanced Encryption Standard*)
AH	En-tête d'authentification (*Authentification Header*)
AS	Association de sécurité
ATM	Agent de transfert de message
CAVP	Programme de validation des algorithmes cryptographiques (*Cryptographic Algorithm Validation Program*)
CBC	Enchaînement de blocs de chiffrement (*Cipher Block Chaining*)
CCE	Cryptographie à courbe elliptique
CMS	Spécification CMS (*Cryptographic Message Syntax*)
DANE	Protocole DANE (*DNS-Based Authentication of Named Entities*)
DH	Diffie-Hellman
DTLS	Protocole DTLS (*Datagram Transport Layer Security*)
ECDH	Diffie-Hellman à courbe elliptique (*Elliptic Curve Diffie-Hellman*)
ECDHE	Courbe elliptique Diffie-Hellman éphémère (*Ephemeral Elliptic Curve Diffie-Hellman*)
ECDSA	Algorithme de signature numérique réalisé à l'aide d'une courbe elliptique (*Elliptic Curve Digital Signature Algorithm*)
ECP	Nombre premier modulo a des groupes de courbes elliptiques (*Elliptic Curve Groups modulo a Prime*)
ESP	Charge utile de sécurité d'encapsulation (*Encapsulated Security Payload*)
FIPS	Federal Information Processing Standard
GC	Gouvernement du Canada
GCM	Galois/Counter Mode
HMAC	Code d'authentification de message à base de fonction de hachage (*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*)
ITSG	Conseils en matière de sécurité des technologies de l'information (*Information Technology Security Guidance*)
ITSP	Conseils en matière de sécurité des technologies de l'information pour les praticiens (*Information Technology Security Guidance for Practitioners*)

LCR	Liste des certificats révoqués
MAC	Code d'authentification de message (*Message Authentication Code*)
NIST	National Institute of Standards and Technology
PFS	Confidentialité persistante (*Perfect Forward Secrecy*)
PRF	Fonction pseudo-aléatoire (*Pseudo-Random Function*)
PVMC	Programme de validation des modules cryptographiques
RFC	Appel de commentaires; document RFC (*Requests for Comments*)
RSA	Rivest-Shamir-Adleman
S/MIME	Protocole S-MIME (*Secure Multipurpose Internet Mail Extensions*)
SCT	Secrétariat du Conseil du Trésor du Canada
SHA	Algorithme SHA (*Secure Hash Algorithm*)
SMTP	Protocole de transfert de courrier simple; protocole SMTP (*Simple Mail Transfer Protocol*)
SP	Publication spéciale (*Special Publication*)
SSH	Protocole SSH (*Secure Shell*)
SSL	Protocole SSL (*Secure Socket Layer*)
STI	Sécurité des technologies de l'information
TI	Technologies de l'information
TLS	Sécurité de la couche de transport (*Transport Layer Security*)

9.2 GLOSSAIRE

Terme	Définition
Authentification	Processus ou mesure utilisée pour vérifier l'identité 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.
Disponibilité	Fait pour un système ou pour de l'information d'être accessible et utilisable intégralement et en temps opportun par les bonnes personnes. La disponibilité s'applique à des actifs d'information, des logiciels et à du matériel (infrastructure et ses composantes).
Information classifiée	Toute information liée à l'intérêt national et qui pourrait faire l'objet d'une exception ou d'une exclusion en vertu de la *Loi sur l'accès à l'information* ou de la *Loi sur la protection des renseignements personnels*, mais dont la compromission, selon toute vraisemblance, porterait atteinte à l'intérêt national.
Confidentialité	Fait d'être divulgué uniquement aux mandants autorisés.
Cryptographie	Discipline qui traite des principes, des moyens et des méthodes permettant de rendre des renseignements inintelligibles et de reconvertir des renseignements inintelligibles en renseignements cohérents.
Attaque par déni de service distribuée (Attaque DDoS)	Une attaque à l'intérieur de laquelle plusieurs systèmes compromis sont utilisés pour attaquer une cible en particulier. L'inondation de messages entrants au système ciblé force l'arrêt de ce dernier et rend le service indisponible aux utilisateurs légitimes.
Déchiffrement	Conversion en clair de l'information (voix ou données) chiffrée par l'opération inverse du chiffrement.
Signature numérique	Transformation cryptographique des données qui fournit les services d'authentification de l'origine, d'intégrité des données et de non-répudiation du signataire.
Chiffrement	Transformation de données lisibles en une séquence de caractères illisibles à l'aide d'un processus de codage réversible.
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.
Intégrité	La capacité de protéger l'information contre sa modification et sa suppression par inadvertance. L'intégrité permet de déterminer ce que l'information prétend être. L'intégrité s'applique également aux processus, à la logique d'une application logicielle, à du matériel et à du personnel.
Gestion des clés	Procédures et mécanismes de génération, de distribution, de remplacement, de stockage, d'archivage et de destruction des clés qui commandent les processus de chiffrement ou d'authentification.
Attaque par rejeu	Forme d'attaque réseau dans laquelle une transmission de données valide est malicieusement répétée ou repoussée par un attaquant qui l'a interceptée.

9.3 RÉFÉRENCES

Numéro	Référence
1	Centre de la sécurité des télécommunications. ITSP.40.111 *Algorithmes cryptographiques pour l'information NON CLASSIFIÉ, PROTÉGÉ A et PROTÉGÉ B*, août 2016.
2	Secrétariat du Conseil du Trésor du Canada. *Ligne directrice sur la définition des exigences en matière d'authentification*, novembre 2008.
3	Centre de la sécurité des télécommunications. ITSG-33 – *La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie*, décembre 2014.
4	National Institute of Standards and Technology. *Special Publication 800-57 Part 3 Rev 1 Recommendation for Key Management Part 3: Application-Specific Key Management Guidance,* janvier 2015.
5	Cooper, D. et autres. *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*. Documents RFC [en ligne], ISSN 2070-1721, RFC 5280, mai 2008.
6	Rescola, E. *The Transport Layer Security (TLS) Protocol Version 1.3.* Documents RFC [en ligne], ISSN 2070-1721, RFC 8446, août 2018.
7	Hodges, J., C. Jackson et A. Barth. *HTTP Strict Transport Security (HSTS)*. Documents RFC [en ligne], ISSN 2070-1721, RFC 6797, novembre 2012.
8	Hoffman, P., *SMTP Service Extension for Secure SMTP over Transport Layer Security*, Documents RFC [en ligne], ISSN 2070-1721, RFC 3207, février 2002.
9	Dukhovni, V. et autres. *SMTP Security via Opportunistic DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS)*, Documents RFC [en ligne], ISSN 2070-1721, RFC 7672, octobre 2015.
10	Ray, M. et S. Dispensa. *Transport Layer Security (TLS) Renegotiation Indication Extension,* Documents RFC [en ligne], ISSN 2070-1721, RFC 5746, février 2010.
11	Kaufman, C. et autres. *Internet Key Exchange Protocol Version 2 (IKEv2)*. Documents RFC [en ligne], ISSN 2070-1721, RFC 7296, octobre 2014.
12	Kivinen, T. et J. Snyder. *Signature Authentication in the Internet Key Exchange Version 2 (IKEv2)*. Documents RFC [en ligne], ISSN 2070-1721, RFC 7427, janvier 2015.
13	Hoffman, P. et J. Snell. *JSON Merge Patch*. Documents RFC [en ligne], ISSN 2070-1721, RFC 7396, octobre 2014.
14	Eronen, P. et H. Tschofeniq. *An Extension of EAP-Only Authentication in IKEv2.* Documents RFC [en ligne], ISSN 2070-1721, RFC 5998, septembre 2010.
15	Nir, Y. et V. Smyslov. *Protecting IKEv2 Implementations from Distributed Denial-of-Service Attacks.* Documents RFC [en ligne], ISSN 2070-1721, RFC 8019, novembre 2016.
16	Smyslov, V. *Internet Key Exchange Protocol Version 2 (IKEv2) Message Fragmentation*. Documents RFC [en ligne], ISSN 2070-1721, RFC 7383, novembre 2014
17	Sheffer, Y et H. Tschofenig. *Internet Key Exchange Protocol Version 2 (IKEv2) Session Resumption*. Documents RFC [en ligne], ISSN 2070-1721, RFC 5723, janvier 2010
18	Kent, S. et K. Seo. *Security Architecture for the Internet Protocol.* Documents RFC [en ligne], ISSN 2070-1721, RFC 4301, décembre 2005.
19	Kent, S. *IP Encapsulating Security Payload (ESP)*. Documents RFC [en ligne], ISSN 2070-1721, RFC 4303, décembre 2005.

Numéro	Référence
20	McGrew, D. et P. Hoffman. *Cryptographic Algorithm Implementation Requirements and Usage Guidance for Encapsulating Security Payload (ESP) and Authentication Header (AH)*. Documents RFC [en ligne], ISSN 2070-1721, RFC 7321, août 2014.
21	Ylonen, T. et C. Lonvick, Ed. *The Secure Shell (SSH) Protocol Architecture*. Documents RFC [en ligne], ISSN 2070-1721, RFC 4251, janvier 2006.
22	Ylonen, T. et C. Lonvick, Ed. *The Secure Shell (SSH) Authentication Protocol*. Documents RFC [en ligne], ISSN 2070-1721, RFC 4252, janvier 2006.
23	Ylonen, T. et C. Lonvick, Ed. *The Secure Shell (SSH) Transport Layer Protocol*. Documents RFC [en ligne], ISSN 2070-1721, RFC 4253, janvier 2006.
24	Ylonen, T. et C. Lonvick, Ed. *The Secure Shell (SSH) Connection Protocol*. Documents RFC [en ligne], ISSN 2070-1721, RFC 4254, janvier 2006.
25	Igoe, K. et D. Stebila. *X.509v3 Certificates for Secure Shell Authentication*. Documents RFC [en ligne], ISSN 2070-1721, RFC 6187, mars 2011.
26	Bellare, M., T. Kohno et C. Namprempre. *The Secure Shell (SSH) Transport Layer Encryption Modes.* Documents RFC [en ligne], ISSN 2072-1721, RFC 4344, janvier 2006.
27	Schaad, J., B. Ramsdell, et S. Turner. *Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 4.0 Message Specification.* Documents RFC [en ligne], ISSN 2070-1721, RFC 8551, avril 2019.
28	Schaad, J., B. Ramsdell, et S. Turner. *Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 4.0 Certificate Handling.* Documents RFC [en ligne], ISSN 2070-1721. RFC 8550, avril 2019.
29	Turner, S. et D. Brown. *Use of Elliptic Curve Cryptography (ECC) Algorithms in Cryptographic Message Syntax (CMS)*. Documents RFC [en ligne], ISSN 2070-1721, RFC 5753, janvier 2010.
30	Turner, S. et autres. *Updates for RSAES-OAEP and RSASSA-PSS Algorithm Parameters*. Documents RFC [en ligne], ISSN 2070-1721, RFC 5756, janvier 2010.
31	Schaad, J. *Use of the RSASSA-PSS Signature Algorithm in Cryptographic Message Syntax (CMS)*. Documents RFC [en ligne], ISSN 2070-1721, RFC 4056, juin 2005.
32	Turner, S. et J. Schaad. *Multiple Signatures in Cryptographic Message Syntax (CMS)*. Documents RFC [en ligne], ISSN 2070-1721, RFC 5752, janvier 2010.
33	Turner, S. et D. Brown. *Use of Elliptic Curve Cryptography (ECC) Algorithms in Cryptographic Message Syntax (CMS)*. Documents RFC [en ligne], ISSN 2070-1721, RFC 5753, janvier 2010.
34	Housley, R. *Use of the RSAES-OAEP Key Transport Algorithm in Cryptographic Message Syntax (CMS)*. Documents RFC [en ligne], ISSN 2070-1721, RFC 3560, juillet 2003.
35	Margolis, D. Risher, M., Ramakrishnan, B., Brothman, A. et Jones, J. *SMTP MTA Strict Transport Security (MTA-STS).* Documents RFC [en ligne], ISSN 2070-1721, RFC 8461, septembre 2018.
36	Rescorla, E. *Preventing the Million Message Attack on Cryptographic Message Syntax.* Documents RFC [en ligne], RFC 3218, janvier 2002