Spécification concernant la classification et le traitement des informations de tiers

Introduction

Les valeurs ou niveaux de sensibilité des données étant variables, la classification des informations nous permettra de déterminer la marche à suivre pour les protéger. Elle témoigne également de notre engagement à protéger ces données et nous aide à les gérer efficacement.

Nous avons quatre niveaux de classification :

- Publiques
- Internes
- Confidentielles
- Strictement confidentielles

Le tableau ci-dessous fournit des indications sur les types d'informations qui seront classées dans l'une de ces quatre catégories.

Par défaut, toute information de BT sera classée comme confidentielle, sauf indication contraire.

Si vous n'êtes pas sûr(e) de la catégorie à laquelle appartient une information donnée, veuillez consulter votre contact de sécurité de BT.

Classification des informations	Description générale	Exemples
Public – Cat. 1	Les informations publiques sont les informations qui se trouvent à la disposition de personnes au sein de BT et en dehors de celle-ci.	• Campagnes publicitaires. • Les communications génériques qui se trouvent déjà dans le domaine public (par exemple, déclarations du service de RP, articles publics concernant BT) • Les informations commerciales disponibles au public, comme les prix ou offres publiés.
Internes – Cat. 2	Les informations de BT qui sont à la disposition du personnel de BT et d'autres personnes autorisées à accéder au réseau d'informations de BT. L'accès à ces informations comporte un risque commercial minimal pour BT. Les informations internes peuvent comprendre les informations régies par des obligations générales de confidentialité (par exemple, les courriels de transactions courantes, les rapports ou documents contractuels), à condition que le degré de sensibilité commerciale de ces informations ne requière pas les protections renforcées décrites ci-dessous.	• Les bulletins d'informations internes, comme BT News • Articles FixIt • Les courriels non sensibles à caractère général (par exemple, des informations non commerciales ou des informations nominatives restreintes, comme indiqué en détail dans la colonne à gauche dans le corps du courriel)
Confidentielles – Cat. 3	Les informations confidentielles sont des informations qui doivent être limitées à un public spécifique et dont la divulgation non autorisée pourrait nuire à la réputation de BT ou nuire potentiellement aux personnes concernées par ces informations (par exemple, les informations nominatives à	• Fichiers-journaux du système ; • Données de vente et marketing commercialement sensibles ; • Plans commerciaux locaux ; • Informations nominatives à caractère privé ; et • Données sur les risques.

	caractère privé des employés ou clients). Le principe de « besoin de connaître » doit être appliqué aux informations confidentielles. **Regroupement de nombreux documents confidentiels** Si vous avez un regroupement de documents « confidentiels » dans un même endroit, il pourrait s'avérer nécessaire de moderniser la classification et cela pourrait entraîner la reclassification de chaque document comme « strictement confidentiel » ou bien encore requérir des mesures de sécurité supplémentaires pour sécuriser l'emplacement dans les cas suivants : • Ils pourraient tous ensemble nuire fortement à BT en cas de fuite ; ou • S'ils étaient utilisés avec d'autres données, ils pourraient devenir une cible intéressante.	• Toutes les informations nominatives (selon la définition figurant dans la Condition intitulée « **Protection des informations »**) à moins qu'elles soient classées comme « strictement confidentielles » ci-dessous.
Strictement confidentielles – Cat. 4	Les informations ou données strictement confidentielles sont définies par une circulation en petit nombre ; le principe du besoin de connaître est strictement appliqué (vous devez savoir qui détient les copies et qui peut y accéder). La divulgation non autorisée de ces informations pourrait nuire fortement à BT. Vous devez considérer scrupuleusement si une information est strictement confidentielle car elle requiert les contrôles de sécurité les plus rigoureux.	• Coordonnées bancaires. • Les coordonnées d'authentification doivent être traitées comme des informations strictement confidentielles. • Mots de passe d'ordinateur : les mots de passe doivent être stockés et sécurisés conformément aux directives de cryptage de BT. • Données de comptabilité générale soumises à embargo jusqu'à la publication du rapport annuel. • Plans commerciaux stratégiques, stratégie concurrentielle, nouveaux produits stratégiques et nouvelles politiques en matière de marketing. • Évaluations très sensibles des concurrents, associés ou entrepreneurs. • Informations sensibles de RH qui pourraient provoquer la perte de confiance d'un nombre considérable d'employés. • Détails de plans d'acquisition, d'alliance, de désinvestissement et de fusion de grande envergure. • Détails de vulnérabilités significatives du réseau. • Codes de sécurité de clients, codes de cryptage maîtres, calculs clés, détails de transactions, comptes ou audits. • Rapports d'audit ou résultats contenant des informations sur des défauts/vulnérabilités graves dans les pratiques ou procédés de BT

Comment dois-je traiter les données ?

Les informations doivent être traitées en fonction de leur niveau de classification afin de les protéger convenablement, quel que soit leur emplacement: sur un ordinateur, à travers un réseau, ou leur forme : écrites ou orales.

Nous avons des règles pour traiter les données et les informations.

- **Informations orales et multimédia** : conversations, réseaux sociaux, mini messages, Skype.
- **Documents en papier :** impression, publication, élimination
- **Documents électroniques :** sauvegarder, envoyer des courriels, transférer, supprimer
- **Dans les applications ou systèmes :** centres de données

Nous avons aussi des directives distinctes sur le niveau et le type de cryptage que nous prétendons utiliser pour protéger les informations (notre « norme de cryptage »).

Comment traiter les informations orales et les données multimédia

Réf	Que souhaitez-vous faire ?	Classification des informations	Exigences relatives au traitement	Raison
HSM10	Je souhaite publier des informations sur des sites de réseaux/médias sociaux, par exemple, sur mon compte Twitter personnel.	Publiques	Vous ne devez pas contribuer aux sites ni publier des déclarations en ligne qui pourraient raisonnablement être interprétées comme les opinions de BT ou diffamatoires contre BT et qui pourraient nuire à la marque et à la réputation de BT.	La publication non autorisée d'informations ou les commentaires personnels pourraient nuire à notre marque.
		Internes	Interdit	
		Confidentielles	Interdit	
		Strictement confidentielles	Interdit	
HSM20	Je souhaite discuter ou présenter quelque chose via un entretien ou un message interne	Internes	Vous pouvez utiliser Live Meeting, WebEx, Webjoin, et Lync/Skype for Business	Les informations internes peuvent être vues par les personnes invitées à la réunion
		Confidentielles	Vous pouvez utiliser Live Meeting, WebEx, Webjoin, et Lync/Skype for Business	Les informations confidentielles peuvent être vues par les personnes invitées à la réunion
		Strictement confidentielles	• Vous pouvez utiliser Lync/Skype for Business hébergés sur BT • Vous devez vérifier qui est présent à la conférence • Vous devez verrouiller la réunion de la conférence pour que personne d'autre ne puisse s'y joindre	Lync/Skype for business sont cryptés conformément aux données ci-dessous de la norme de cryptage
HSM30	Je souhaite discuter de quelque chose via un dialogue en ligne externe, par exemple,	Publiques	Les conversations doivent se limiter aux « informations publiques » qui sont gratuitement disponibles sur notre site Web	Éviter la divulgation non autorisée d'informations

	sur un site d'assistance d'un fournisseur comme Cisco	Internes	Interdit	
		Confidentielles	Interdit	
		Strictement confidentielles	Interdit	
HSM40	Je souhaite discuter quelque chose en tête à tête/par téléphone	Internes	Assurez-vous que la conversation ne puisse pas être écoutée par hasard par quelqu'un qui ne travaille pas chez BT ni pour le compte de BT	Éviter la divulgation non autorisée d'informations
		Confidentielles	Comme « internes » et • Vérifiez l'identité de la personne à qui vous parlez et confirmez qu'elle ait un « besoin de connaître » avant de discuter une question confidentielle • Assurez-vous qu'un contrat soit en vigueur avec des tiers pertinents avant d'engager la conversation, s'il y a lieu (N.B. Avant d'assigner ou de confier en sous-traitance la totalité ou une partie du contrat à un tiers, vous devez d'abord obtenir le consentement par écrit de BT) • Assurez-vous que la conversation ne puisse pas être écoutée par hasard • Ne laissez pas d'informations « confidentielles » sur les systèmes de courriel vocal.	Protéger les informations confidentielles et assurer qu'elles soient limitées aux personnes qui ont un besoin de connaître
		Strictement confidentielles	Comme « confidentielles » et • Maintenez les informations « strictement confidentielles » au minimum absolu	
HSM50	Je souhaite envoyer un message/contenu via SMS/MMS à toutes les parties (internes et externes)	Publiques	Le contenu du message doit se limiter aux « informations publiques » qui sont disponibles sur notre site Web	Éviter la divulgation non autorisée d'informations
		Internes	Il n'existe pas d'exigences particulières concernant le traitement	
		Confidentielles	Assurez-vous de n'envoyer le message qu'à ceux qui ont le besoin de connaître et ne divulguez pas les informations suivantes : • Informations de la carte de paiement • Coordonnées bancaires • Mot de passe	Ces 3 éléments sont strictement confidentiels
		Strictement confidentielles	Interdit	

Traitement des documents en papier

Réf	Que souhaitez-vous faire ?	Classification	Exigences relatives au traitement	Raison
HPD10	Je souhaite travailler avec des informations	Internes	Vous devez appliquer la politique « débarrasser le bureau » lorsque vous	Éviter les divulgations par inadvertance

	sur une copie papier dans les installations d'un tiers ou à la maison		ne travaillez pas à votre bureau	
		Confidentielles	Comme « internes » et • Lorsque vous ne travaillez pas sur les documents, mettez les hors de vue et verrouillez-les.	
		Strictement confidentielles	Comme « confidentielles »	
HPD20	Je souhaite faire une impression	Internes	• Assurez-vous d'envoyer les documents à l'imprimante correcte • Ne laissez pas de documents dans le bac à papiers	Éviter les divulgations par inadvertance
		Confidentielles	Comme « internes » et • Utilisez une imprimante contrôlée, une imprimante raccordée à un PC ou une imprimante située dans une salle à accès contrôlé	
		Strictement confidentielles	Comme « confidentielles »	
HPD30	Je souhaite utiliser une imprimante qui ne se trouve pas dans l'établissement d'un fournisseur ni chez moi (elle se trouve par exemple dans les installations d'un tiers, dans un hôtel, etc.)	Internes	En règle générale, cela est interdit car les imprimantes ont des mémoires et les données peuvent être récupérées. Recourez à votre bon sens : voulez-vous vraiment que d'autres personnes puissent voir ces informations ?	Les données et informations peuvent être récupérées de la mémoire d'une imprimante
		Confidentielles	Interdit	
		Strictement confidentielles	Interdit	
HPD40	Je souhaite emporter une information sur une copie papier en dehors de mon lieu de travail	Internes	Emportez-la dans une chemise ou un sac opaque	Éviter les divulgations par inadvertance
		Confidentielles	Comme « internes » et • Vous ne devez pas retirer les coordonnées du client et/ou du paiement des bureaux du fournisseur	
		Strictement confidentielles	Comme « confidentielles »	
HPD50	Je souhaite partager ou envoyer des informations qui se trouvent sur une copie papier à des parties internes	Internes	• Mettez la copie dans une enveloppe et utilisez le service postal interne.	Évite les observations fortuites
		Confidentielles	• N'écrivez pas « strictement confidentiel » sur l'enveloppe extérieure. • Si l'information est couverte par un « privilège juridique », demandez l'avis de votre équipe juridique.	Éviter que les observateurs fortuits sachent que les contenus sont confidentiels. La signature pour livraison est une preuve de postage, de signature à la livraison et de confirmation en ligne de la livraison de l'élément
		Strictement confidentielles	• Utilisez 2 enveloppes et expédiez-les en utilisant une	Éviter que les observateurs fortuits

			livraison « repérable » • N'écrivez pas « Strictement confidentiel » sur l'enveloppe extérieure. • Demandez au propriétaire du document de vous donner la permission de partager la copie papier • De préférence, partagez-la personnellement avec les individus autorisés • Associez des copies aux individus en les filigranant avec un nom ou numéro (si possible) • En cas de perte, signalez un incident de sécurité	sachent que les contenus sont strictement confidentiels. La signature pour livraison est une preuve de postage, de signature à la livraison et de confirmation en ligne de la livraison de l'élément
HPD60	Je souhaite partager ou envoyer une copie papier à des parties externes	Internes Confidentielles Strictement confidentielles	Assurez-vous d'avoir un contrat en vigueur selon HSM40 avec tiers pertinents. Après cela, les contrôles sont les mêmes que pour le partage avec des parties internes.	Voir HPD50
HPD70	Je souhaite envoyer une télécopie	Internes	Vous devez vous assurer d'inclure une page d'en-tête de télécopie avant la/les page(s) du contenu.	Éviter les divulgations par inadvertance
		Confidentielles	• Vous devez envoyer une page d'en-tête avec une page d'essai et prendre ensuite contact avec le destinataire pour confirmer la réception avant de télécopier le contenu • Si l'information est couverte par un « privilège juridique », demandez l'avis de votre équipe juridique	Éviter que les personnes non autorisées reçoivent les informations
		Strictement confidentielles	Interdit	
HPD80	Je souhaite éliminer des informations qui se trouvent sur une copie papier	Internes	Vous devez • la détruire ou • la mettre dans une corbeille à papier qui ne puisse pas être emportée facilement	Les poubelles pour déchets généraux et/ou de recyclage ne sont pas des moyens sûrs d'élimination
		Confidentielles	Vous devez les détruire avec une taille de particules minimum de $\leq$ 160 mm² et avec une largeur de bande pour particules ordinaires de $\leq$ 2 mm, par exemple 2 X 15 mm.	Éviter la divulgation d'informations « confidentielles »
		Strictement confidentielles	Vous devez les détruire avec une taille de particules minimum de $\leq$ 160 mm² et avec une largeur de bande pour particules ordinaires de $\leq$ 2 mm, par exemple, de 2 X 15 mm avec un destructeur de documents avec coupe en travers.	Éviter la divulgation d'informations « strictement confidentielles »

Traitement des documents électroniques

Réf	Que souhaitez-vous faire ?	Classification des informations	Exigences relatives au traitement	Raison
HED10	Je souhaite stocker des informations électroniques sur le portable/PC de l'entreprise	Internes	Cryptage de tout le disque conformément à la norme de cryptage ci-dessous.	Cette norme convertit les informations en un code illisible qui ne peut pas être déchiffré facilement par les personnes non autorisées.
		Confidentielles	Cryptage de tout le disque conformément à la norme de cryptage ci-dessous.	
		Strictement confidentielles	Cryptage de tout le disque conformément à la norme de cryptage ci-dessous.	
HED20	Je souhaite stocker mes documents sur SharePoint ou sur un autre gestionnaire de documents qui n'est PAS hébergé dans le nuage ou avec des services sur Internet	Internes	• Utilisez les niveaux et groupes de permission pour définir un contrôle de l'accès basé sur le rôle. Ceux-ci ne doivent pas être établis au-delà du minimum pour permettre aux individus de faire leur travail. • Réviser les contrôles d'accès tous les ans	Limite l'accès et/ou la modification à ceux qui ont un besoin de connaître.
		Confidentielles	Comme « internes » et • Documentez le procédé pour assigner les rôles aux personnes. • Les rôles et les personnes affectées à ceux-ci doivent être révisés tous les 90 jours. • Les documents doivent être cryptés conformément à la norme de cryptage ci-dessous.	
		Strictement confidentielles	Comme « internes » et • Documentez le procédé pour assigner les rôles aux personnes. • Les rôles et les personnes affectées à ceux-ci doivent être révisés tous les 90 jours. • Les documents doivent être cryptés conformément à la norme de cryptage ci-dessous.	
HED30	Je souhaite stocker des informations électroniques dans le nuage ou à l'aide de services disponibles sur Internet tels que Google Docs, GitHub, btcloud.bt.com, Drobox, Pastebin, Facebook, etc.	Internes	Interdit.	Les services disponibles sur Internet augmentent les risques d'accès non autorisés aux informations
		Confidentielles	Interdit.	
		Strictement confidentielles	Interdit.	
HED40	Je souhaite stocker des informations électroniques sur un support amovible,	Internes	• Les périphériques USB doivent être cryptés conformément à la norme de cryptage ci-	Les supports amovibles sont plus susceptibles d'être égarés ou volés

	comme une clé USB.		dessous. Les informations nominatives ne doivent en aucun cas être stockées sur ces périphériques à moins qu'ils soient cryptés conformément à la norme de cryptage ci-dessous.	qu'un ordinateur et il est plus probable que des personnes non autorisées accèdent aux données. Pour protéger les informations, elles doivent être converties en un code illisible qui ne puisse pas être déchiffré facilement par les personnes non autorisées.
		Confidentielles	Comme « internes »	
		Strictement confidentielles	Comme « internes »	
HED50	Je souhaite stocker des documents électroniques ou des informations de BT sur mon portable/PC personnel	Internes	Interdit	Les personnes non autorisées peuvent accéder aux données de BT, en particulier si le dispositif est perdu, volé, ou mis au rebut en faveur d'un modèle plus récent.
		Confidentielles	Interdit	
		Strictement confidentielles	Interdit	
HED60	Je souhaite envoyer des documents ou informations électroniques à l'adresse de mon courriel personnel.	Internes	Interdit	Éviter la divulgation à des personnes non autorisées
		Confidentielles	Interdit	
		Strictement confidentielles	Interdit	
HED70	Je souhaite réaliser une retransmission automatique vers une adresse de courriel	Internes	Interdit	Des personnes non autorisées pourraient accéder aux données si le compte du courriel, le fournisseur d'accès à Internet ou la connexion à Internet est comprise
		Confidentielles	Interdit	
		Strictement confidentielles	Interdit	
HED80	Je souhaite partager ou envoyer *en interne* des informations électroniques par courriel	Internes	Il n'existe pas d'exigences particulières	
		Confidentielles	• Précisez que le courriel est « strictement confidentiel » • Utilisez les paramètres de sensibilité pour marquer le courriel comme « confidentiel » • Idéalement, réglez les autorisations sur « Ne pas transférer » • Si l'information est couverte par un « privilège juridique », demandez l'avis de votre équipe juridique •	Maintenir le contrôle sur les informations confidentielles
		Strictement confidentielles	Comme « confidentielles » et	Protéger les informations

			• Utilisez un courriel sécurisé pour les envois • S'il n'est pas possible d'utiliser un courriel sécurisé, vous devez crypter le fichier avant de l'envoyer, conformément à la norme de cryptage ci-dessous • Réglez les autorisations sur « Ne pas transférer »	lorsqu'elles parcourent les divers réseaux
HED90	Je souhaite partager ou envoyer *en externe* des informations électroniques par courriel	Internes	Vous ne pouvez les envoyer à un tiers que si un contrat est en vigueur, conformément à HSM40.	Maintenir le contrôle sur les informations confidentielles
		Confidentielles	Comme « internes » et • Cryptez conformément à la norme de cryptage ci-dessous. • Confirmez que vous êtes en train d'envoyer les informations à la bonne adresse de courriel • Si l'information est couverte par un « privilège juridique », demandez l'avis de votre équipe juridique	
		Strictement confidentielles	Comme « confidentielles »	
HED120	Je souhaite faire une sauvegarde des documents électroniques de BT	Internes	• Vous devez stocker vos documents sur les pilotes de périphérique réseau du fournisseur ou le gestionnaire de documents du fournisseur, conformément à HED030. • Le document sauvegardé doit être protégé au même degré que sur le pilote de périphérique réseau, SharePoint. • Si vous utilisez un support amovible, le périphérique doit être crypté conformément à la norme de cryptage ci-dessous.	Les sauvegardes doivent avoir le même niveau de classification et protection que les données originales
		Confidentielles	Comme « internes » et • Cryptez le document conformément à la norme de cryptage ci-dessous avant de réaliser la sauvegarde	
		Strictement confidentielles	Comme « confidentielles »	

Système de traitement et données d'application

Réf	Que souhaitez-vous faire ?	Classification des informations	Exigences relatives au traitement	Raison
HSADE	Je souhaite stocker et traiter des données et informations électroniques qui se trouvent sur un centre de données ou sur un serveur système	Internes	Il n'existe pas d'exigences particulières si les exigences en vigueur susmentionnées pour le stockage de données concernant cette classification sont respectées.	
		Confidentielles	Vous devez observer les exigences d'hébergement de données externes de tiers http://www.selling2bt.com/working/ThirdPartySecurity standards/index.htm	
		Strictement confidentielles	Comme « confidentielles » et Protéger les coordonnées bancaires car elles sont tout particulièrement sensibles. Les contrôles suivants doivent être réalisés. Ils ont la priorité sur toute autre contrôle applicable dans cette spécification de sécurité. 1. Les comptes bancaires doivent être segmentés en unités pour les individus (comptes bancaires personnels de clients et employés de BT). Cela permet d'exclure les coordonnées bancaires de BT et les coordonnées bancaires des divers organismes juridiques de BT). 2. Si une application ne possède que des comptes bancaires de sociétés, le tiers peut présenter des arguments (basés sur le temps, les coûts, les ressources, le nombre de comptes et le nombre d'utilisateurs autorisés à accéder à l'application etc.) afin de déterminer si BT acceptera initialement une solution basée sur un système de cryptage. Si une solution basée sur un système de cryptage est acceptée, BT révisera alors la décision une fois que tous les comptes bancaires sont protégés afin de déterminer s'il convient de continuer de l'utiliser. Cela sera influencé par les niveaux de menace et l'appétit pour les risques de l'entreprise dans son ensemble. 3. Lorsque les coordonnées bancaires réelles sont présentées à un agent dans le cadre d'une transaction commerciale (par exemple, pour vérifier que nous avons le bon compte à facturer, lorsque nous communiquons avec un client via courriel, ou sur une facture), il suffit de montrer les quatre derniers chiffres	

			du compte bancaire (c'est-à-dire que les coordonnées bancaires sont masquées). 4. S'il s'avérait nécessaire d'accéder au compte bancaire complet (par exemple, pour permettre une demande de crédit ou de débit d'une banque), les coordonnées bancaires devront être regroupées ou décryptées, puis transférées à la banque en utilisant un mécanisme de transport crypté conforme à la politique de sécurité de BT. Immédiatement après l'utilisation, les coordonnées bancaires regroupées ou décryptées doivent être supprimées de façon sûre.	

Normes de cryptage

Contrôles généraux de cryptographie.

Réf	Contrôle	Raison
C1.10	Les bibliothèques cryptographiques actuelles doivent être utilisées	Les bibliothèques cryptographiques sont mises à jour régulièrement. En plus de mettre à jour les progiciels en suivant les instructions du fournisseur, les paquets cryptographiques doivent être révisés et mis à jour régulièrement.
C1.20	N'utilisez que des suites cryptographiques approuvées par les normes du secteur d'activité pour le cryptage. Par exemple, pour TLS SSLv2	Les chiffres non approuvés peuvent introduire des vulnérabilités.
C1.30	La version la plus récente de TLS doit être utilisée pour les nouveaux déploiements. SSL V1, 2 et 3 ne doit pas être utilisée	Les versions précédentes, jusqu'à TLS1.0 incluse, ne sont plus considérées sûres
C1.40	La confidentialité de transmission parfaite doit être activée	Les algorithmes de la confidentialité de transmission parfaite permettent d'éviter que les messages capturés soient déchiffrés, même si la clé d'authentification privée est compromise à l'avenir
C1.50	Les certificats auto-signés ne doivent pas être utilisés	Les certificats auto-signés annulent l'avantage de l'authentification à la destination et diminuent considérablement la capacité d'un individu à détecter une attaque de l'intercepteur.
C1.60 **GTS2.370**	Les services d'une autorité de certification du secteur d'activité doivent être utilisés pour la gestion des certificats. Par exemple, verisign	Tenir un inventaire des certificats délivrés pour les vulnérabilités et l'expiration du certificat
C1.70	Les mots de passe doivent être protégés en utilisant une fonction mathématique à sens unique et irréversible (par exemple, l'algorithme de hachage) avec un facteur de transformation aléatoire unique (Salt) par mot de passe. N.B. SALT est une donnée aléatoire utilisée comme entrée supplémentaire à une fonction à sens unique qui réalise le « hachage » d'un mot de passe ou d'une phrase de passe.	Vu que les fichiers stockés contenant le mot de passe peuvent être extraits, toutes les saisies doivent être protégées pour éviter la récupération de mots de passe sous la forme de texte clair
C1.80	Selon C1.70, les mots de passe protégés doivent être stockés en dehors des fichiers de configuration d'un système et le contrôle des accès doit être mis en œuvre afin que seuls les utilisateurs privilégiés appropriés puissent lire ou copier les contenus.	Il ne doit jamais être possible de récupérer des mots de passe protégés par le biais de la traversée de répertoire, la marche SNMP, le vidage de la configuration, ou tout autre mécanisme qui pourrait permettre des tentatives de craquage hors ligne.

Mise en œuvre de la cryptographie technique

Protocoles SSL/TLS	
Utilisable	**Ne pas utiliser**
TLSv1.3 (À confirmer - Disponible sur OpenSSL après le 5 avril).	SSLv3.0
TLSv1.2	SSLv2.0
TLSv1.1	
TLS v1.0*	

***** TLSv1.0 se trouve déjà en fin de vie et son utilisation peut être déconseillée à cause de motifs inconnus. Pour des raisons de conformité (par exemple PCI-DSS), les protocoles tels que TLSv1.0 et TLSv1.1 pourraient être désactivés. Tous les développeurs doivent se tenir prêts à désactiver ces protocoles par le biais de la configuration.

Tailles de clé			
	Symétrique	**Asymétrique**	**Courbe elliptique**
Friche industrielle	≥ 112 bits	≥ 2048 bits	≥ 224 bits
Zone verte	≥ 128 bits	≥ 3072 bits	≥ 384 bits

Échange de clés	
Utilisable	**Ne pas utiliser**
ECDHE (clé temporaire éphémère) échange de clés Diffie-Hellman (les clés ne sont pas basées sur des certificats)	kRSA (échange de clés RSA)
	kDHr (échange de clés Diffie-Hellman avec clé RSA)
	kDHd (échange de clés Diffie-Hellman avec clé DSA)
	kSRP (échange de clés avec mot de passe à distance sécurisé (SRP)) kADH (échange de clés Diffie-Hellman anonyme)
	kPSK (échange de clés avec clé préalablement partagée)

La sécurité de transmission parfaite doit être basée sur des valeurs du groupe Diffie-Hellman configurées ou générées localement et comprenant des nombres premiers « sécurisés ».

Paramètres Diffie Hellman

Paramètres Diffie Hellman	
Utilisable	**Ne pas utiliser**
Groupe Diffie-Hellman de 3072 bits (meilleur groupe – doit être généré localement).	Les valeurs par défaut du serveur (générez vos propres valeurs localement)
Groupe Diffie-Hellman de 2048 bits (s'approche de sa fin de vie – doit être généré localement).	

Authentification	
Utilisable	**Ne pas utiliser**
aRSA (Authentification RSA)	aNULL (pas d'authentification)
aECDSA (Authentification avec algorithme de signature numérique sur courbe elliptique)	aDSS (Authentification DSS)
	aECDH (Diffie-Hellman sur courbe elliptique)
	aDH (Diffie-Hellman)
	aDSA (Algorithme de signature numérique)
	aPSK (Clé préalablement partagée)

	aSRP (Mot de passe à distance sécurisé)

Chiffre/Cryptage	
Utilisable	**Ne pas utiliser**
AES 256 GCM (Rijndael (Norme de cryptage avancé) - Mode Galois/compteur)	eNULL (pas de cryptage)
AES 128 GCM (Rijndael (Norme de cryptage avancé) - Mode Galois/compteur)	DES (cryptage DES)
CHACHA20/POLY1305 (256)	3DES (cryptage 3DES)
AES 256 CCM (Rijndael (Norme de cryptage avancé) - Mode compteur avec CBC-Mac)	RC4 (cryptage RC4)
AES 128 CCM (Rijndael (Norme de cryptage avancé) - Mode compteur avec CBC-Mac)	RC2 (cryptage RC2)
AES 256 CBC (enchaînement des blocs Rijndael) – s'approche de la fin de sa vie.	IDEA (cryptage IDEA)
AES 128 CBC (enchaînement des blocs Rijndael) – s'approche de la fin de sa vie.	Seed (cryptage Seed)
	Camellia (cryptage Camellia)
	ARIA (cryptage ARIA)

Algorithme de hachage MAC	
Utilisable	**Ne pas utiliser**
AEAD (Cryptage authentifié avec données supplémentaires)	MD5 (fonction de hachage MD5)
SHA512 (famille SHA2 - fonction de hachage SHA512)	SHA1 (fonction de hachage SHA1)
SHA384 (famille SHA2 - fonction de hachage SHA384)	SHA (pseudonyme de SHA1)
SHA256 (famille SHA2 - fonction de hachage SHA256)	