Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

X.1362

(03/2017)

SÉRIE X: RÉSEAUX DE DONNÉES, COMMUNICATION ENTRE SYSTÈMES OUVERTS ET SÉCURITÉ

Applications et services sécurisés – Sécurité de l'Internet des objets (IoT)

Procédure de chiffrement simple pour les environnements de l'Internet des objets (IoT)

Recommandation UIT-T X.1362

RECOMMANDATIONS UIT-T DE LA SÉRIE X

RÉSEAUX DE DONNÉES, COMMUNICATION ENTRE SYSTÈMES OUVERTS ET SÉCURITÉ

RÉSEAUX PUBLICS DE DONNÉES	X.1–X.199
INTERCONNEXION DES SYSTÈMES OUVERTS	X.200–X.299
INTERFONCTIONNEMENT DES RÉSEAUX	X.300–X.399
SYSTÈMES DE MESSAGERIE	X.400–X.499
ANNUAIRE	X.500–X.599
RÉSEAUTAGE OSI ET ASPECTS SYSTÈMES	X.600–X.699
GESTION OSI	X.700–X.799
SÉCURITÉ	X.800–X.849
APPLICATIONS OSI	X.850–X.899
TRAITEMENT RÉPARTI OUVERT	X.900–X.999
SÉCURITÉ DE L'INFORMATION ET DES RÉSEAUX	
Aspects généraux de la sécurité	X.1000–X.1029
Sécurité des réseaux	X.1030–X.1049
Gestion de la sécurité	X.1050–X.1069
Télébiométrie	X.1080–X.1099
APPLICATIONS ET SERVICES SÉCURISÉS	
Sécurité en multidiffusion	X.1100–X.1109
Sécurité des réseaux domestiques	X.1110–X.1119
Sécurité des télécommunications mobiles	X.1120–X.1139
Sécurité de la toile	X.1140–X.1149
Protocoles de sécurité	X.1150–X.1159
Sécurité d'homologue à homologue	X.1160–X.1169
Sécurité des identificateurs en réseau	X.1170–X.1179
Sécurité de la télévision par réseau IP	X.1180–X.1199
SÉCURITÉ DU CYBERESPACE	
Cybersécurité	X.1200–X.1229
Lutte contre le spam	X.1230–X.1249
Gestion des identités	X.1250–X.1279
APPLICATIONS ET SERVICES SÉCURISÉS	
Communications d'urgence	X.1300–X.1309
Sécurité des réseaux de capteurs ubiquitaires	X.1310–X.1339
Recommandations relatives aux infrastructures de clé publique	X.1340–X.1349
Sécurité de l'Internet des objets (IoT)	**X.1360–X.1369**
Sécurité des systèmes de transport intelligents	X.1370–X.1379
ECHANGE D'INFORMATIONS SUR LA CYBERSÉCURITÉ	
Aperçu général de la cybersécurité	X.1500–X.1519
Echange concernant les vulnérabilités/les états	X.1520–X.1539
Echange concernant les événements/les incidents/l'heuristique	X.1540–X.1549
Echange de politiques	X.1550–X.1559
Heuristique et demande d'informations	X.1560–X.1569
Identification et découverte	X.1570–X.1579
Echange garanti	X.1580–X.1589
SÉCURITÉ DE L'INFORMATIQUE EN NUAGE	
Aperçu de la sécurité de l'informatique en nuage	X.1600–X.1601
Conception de la sécurité de l'informatique en nuage	X.1602–X.1639
Bonnes pratiques et lignes directrices concernant la sécurité de l'informatique en nuage	X.1640–X.1659
Mise en oeuvre de la sécurité de l'informatique en nuage	X.1660–X.1679
Sécurité de l'informatique en nuage (autres)	X.1680–X.1699

Pour plus de détails, voir la Liste des Recommandations de l'UIT-T.

Recommandation UIT-T X.1362

Procédure de chiffrement simple pour les environnements de l'Internet des objets (IoT)

Résumé

L'Internet des objets (IoT) est considéré comme l'un des domaines les plus importants pour les futurs travaux de normalisation. A l'UIT-T, l'IoT est défini comme étant une infrastructure mondiale pour la société de l'information, qui permet de disposer de services évolués en interconnectant des objets (physiques ou virtuels).

Dans certains environnements de l'IoT, en particulier pour les dispositifs de l'IoT, l'exigence de traitement en temps réel veut que les tâches soient traitées dans un laps de temps déterminé. Afin d'assurer la confidentialité des données et la protection de l'intégrité, l'une des mesures fondamentales est l'application d'algorithmes de chiffrement des données/d'authentification. L'application habituelle d'algorithmes de chiffrement des données/d'authentification est problématique en ce sens qu'elle ne satisfait pas l'exigence de traitement en temps réel.

La Recommandation UIT-T X.1362 définit la procédure de chiffrement avec données de gabarit associées (EAMD) pour les dispositifs de l'IoT. Elle décrit la procédure EAMD et la façon dont elle assure un ensemble de services de sécurité pour le trafic qui utilise cette procédure.

Historique

Edition	Recommandation	Approbation	Commission d'études	Identifiant unique*
1.0	UIT-T X.1362	30-03-2017	17	11.1002/1000/13196

Mots clés

Application d'algorithmes de chiffrement des données/d'authentification, chiffrement avec données de gabarit associées (EAMD), dispositifs de l'IoT, exigence de traitement en temps réel.

* Pour accéder à la Recommandation, reporter cet URL http://handle.itu.int/ dans votre navigateur Web, suivi de l'identifiant unique, par exemple http://handle.itu.int/11.1002/1000/11830-en.

AVANT-PROPOS

L'Union internationale des télécommunications (UIT) est une institution spécialisée des Nations Unies dans le domaine des télécommunications et des technologies de l'information et de la communication (ICT). Le Secteur de la normalisation des télécommunications (UIT-T) est un organe permanent de l'UIT. Il est chargé de l'étude des questions techniques, d'exploitation et de tarification, et émet à ce sujet des Recommandations en vue de la normalisation des télécommunications à l'échelle mondiale.

L'Assemblée mondiale de normalisation des télécommunications (AMNT), qui se réunit tous les quatre ans, détermine les thèmes d'étude à traiter par les Commissions d'études de l'UIT-T, lesquelles élaborent en retour des Recommandations sur ces thèmes.

L'approbation des Recommandations par les Membres de l'UIT-T s'effectue selon la procédure définie dans la Résolution 1 de l'AMNT.

Dans certains secteurs des technologies de l'information qui correspondent à la sphère de compétence de l'UIT-T, les normes nécessaires se préparent en collaboration avec l'ISO et la CEI.

NOTE

Dans la présente Recommandation, l'expression "Administration" est utilisée pour désigner de façon abrégée aussi bien une administration de télécommunications qu'une exploitation reconnue.

Le respect de cette Recommandation se fait à titre volontaire. Cependant, il se peut que la Recommandation contienne certaines dispositions obligatoires (pour assurer, par exemple, l'interopérabilité et l'applicabilité) et considère que la Recommandation est respectée lorsque toutes ces dispositions sont observées. Le futur d'obligation et les autres moyens d'expression de l'obligation comme le verbe "devoir" ainsi que leurs formes négatives servent à énoncer des prescriptions. L'utilisation de ces formes ne signifie pas qu'il est obligatoire de respecter la Recommandation.

DROITS DE PROPRIÉTÉ INTELLECTUELLE

L'UIT attire l'attention sur la possibilité que l'application ou la mise en œuvre de la présente Recommandation puisse donner lieu à l'utilisation d'un droit de propriété intellectuelle. L'UIT ne prend pas position en ce qui concerne l'existence, la validité ou l'applicabilité des droits de propriété intellectuelle, qu'ils soient revendiqués par un membre de l'UIT ou par une tierce partie étrangère à la procédure d'élaboration des Recommandations.

A la date d'approbation de la présente Recommandation, l'UIT n'avait pas été avisée de l'existence d'une propriété intellectuelle protégée par des brevets à acquérir pour mettre en œuvre la présente Recommandation. Toutefois, comme il ne s'agit peut-être pas de renseignements les plus récents, il est vivement recommandé aux développeurs de consulter la base de données des brevets du TSB sous http://www.itu.int/ITU-T/ipr/.

TABLE DES MATIÈRES

Introduction

Il est admis que l'Internet des objets (IoT) est l'un des domaines les plus importants pour les futurs travaux de normalisation. A l'UIT-T, l'IoT est défini dans la Recommandation [b-UIT-T Y.2060] comme étant une infrastructure mondiale pour la société de l'information, qui permet de disposer de services évolués en interconnectant des objets (physiques ou virtuels) grâce aux technologies de l'information et de la communication interopérables existantes ou en évolution.

Les réseaux de capteurs ubiquitaires (USN) semblent être l'un des domaines les plus pertinents de l'IoT. Les réseaux USN sont des réseaux de noeuds de capteurs intelligents qui pourraient être déployés "partout, tout le temps, par quiconque ou quoi que ce soit". On estime que les techniques de sécurité pour les réseaux USN sont efficaces dans le contexte de l'IoT, car ces réseaux ont de nombreux points de convergence avec l'IoT, dans la mesure où ils sont au contact de certains dispositifs tels que des dispositifs de détection et d'actionnement. En ce qui concerne la sécurité des réseaux USN, des Recommandations ont déjà été publiées, par exemple la Recommandation [b-UIT-T X.1311], qui porte sur le cadre de sécurité, la Recommandation [b-UIT-T X.1312], qui contient des lignes directrices sur la sécurité des intergiciels, et la Recommandation [b-UIT-T X.1313], qui porte sur les exigences de sécurité pour le routage dans les réseaux de capteurs sans fil. Cependant, aucune étude n'a été faite en vue de l'élaboration de Recommandations sur les techniques de confidentialité des données et de protection de l'intégrité assurant la sécurité de la couche dispositif des réseaux USN. Par conséquent, la sécurité de la couche dispositif est un élément qui fait défaut dans les réseaux USN ainsi que dans l'IoT; il convient donc de procéder à une étude et un examen de cet élément en vue de sa future normalisation.

En revanche, dans certains environnements de l'IoT, en particulier pour les dispositifs de l'IoT tels que les dispositifs de détection et d'actionnement, qui peuvent être utilisés dans des systèmes de contrôle industriel (ICS), il existe une exigence de traitement en temps réel selon laquelle les tâches sont traitées dans un laps de temps déterminé. Afin d'assurer la protection de la confidentialité et de l'intégrité des données, l'une des contre-mesures fondamentales est l'application d'algorithmes de chiffrement des données/d'authentification. Le problème posé par l'application habituelle d'algorithmes de chiffrement des données/d'authentification est qu'elle ne satisfait pas l'exigence de traitement en temps réel. L'autre problème rencontré est celui de l'intégration de niveaux de sécurité différents. Plus précisément, à l'intérieur d'un paquet de communication, des données occupant des emplacements différents nécessitent des niveaux différents de sécurité importante. En conséquence, le chiffrement de données situées dans un emplacement correspondant à un niveau de sécurité faible est considéré comme une opération inutile.

Comme indiqué précédemment, pour garantir la sécurité des environnements IoT, en particulier des dispositifs de l'IoT, il est nécessaire d'appliquer de nouveaux algorithmes de chiffrement des données/d'authentification qui satisfont l'exigence de traitement en temps réel et qui intègrent des niveaux de sécurité différents.

Par conséquent, le chiffrement avec données de gabarit associées qui, au sein d'un paquet de communication, chiffre uniquement les données dont le niveau de sécurité est élevé se révèle nécessaire. Les données de gabarit associées servent à indiquer le niveau de sécurité des données pour chaque emplacement au sein d'un paquet.

Recommandation UIT-T X.1362

Procédure de chiffrement simple pour les environnements de l'Internet des objets (IoT)

1 Domaine d'application

La présente Recommandation fournit une procédure de chiffrement pour la sécurité des dispositifs de l'Internet des objets. Cette procédure est destinée à être appliquée aux environnements de l'IoT, en particulier aux dispositifs de l'IoT dotés obligatoirement de capacités de communication et éventuellement de capacités de détection, d'actionnement, de stockage de données et de traitement de données. La présente Recommandation détaille la méthode de chiffrement avec données de gabarit associées (EAMD) pour les environnements de l'IoT. Elle décrit le fonctionnement du chiffrement EAMD et la façon dont il fournit un ensemble de services de sécurité pour le trafic qui utilise cette méthode. Des exemples d'application sont également fournis dans l'Annexe A.

2 Références

La présente Recommandation se réfère à certaines dispositions des Recommandations UIT-T et textes suivants qui, de ce fait, en sont partie intégrante. Les versions indiquées étaient en vigueur au moment de la publication de la présente Recommandation. Toute Recommandation ou tout texte étant sujet à révision, les utilisateurs de la présente Recommandation sont invités à se reporter, si possible, aux versions les plus récentes des références normatives suivantes. La liste des Recommandations de l'UIT-T en vigueur est régulièrement publiée. La référence à un document figurant dans la présente Recommandation ne donne pas à ce document, en tant que tel, le statut d'une Recommandation.

[IETF RFC 4303] IETF RFC 4303 (2005), *IP Encapsulating Security Payload (ESP).*

[IETF RFC 7296] IETF RFC 7296 (2014), *Internet Key Exchange Protocol Version 2 (IKEv2).*

[IETF RFC 7321] IETF RFC 7321 (2014), *Cryptographic Algorithm Implementation Requirements and Usage Guidance for Encapsulating Security Payload (ESP) and Authentication Header (AH).*

[ISO/CEI 10116] ISO/CEI 10116:2006, *Technologies de l'information – Techniques de sécurité – Modes opératoires d'un chiffrement par blocs de n-bits.*

3 Définitions

3.1 Termes définis ailleurs

La présente Recommandation utilise les termes suivants définis ailleurs:

3.1.1 actionneur [b-UIT-T Y.4109]: dispositif qui accomplit des actions physiques en réaction à un signal d'entrée.

NOTE – Un actionneur pourrait, par exemple, agir sur l'écoulement d'un gaz ou d'un liquide, sur la distribution de l'électricité, ou par une opération mécanique. Les variateurs et les relais sont des exemples d'actionneurs. La décision d'activer l'actionneur peut provenir d'une application MOC, d'un être humain ou de dispositifs et de passerelles MOC.

3.1.2 données utiles de sécurité par encapsulage IP (ESP) [IETF RFC 4303]: protocole IPsec utilisé pour fournir la confidentialité, l'authentification de l'origine des données, l'intégrité sans connexion, un service anti-répétition (forme d'intégrité de séquence partielle), et une confidentialité (limitée) de flux de trafic. L'ensemble des services fournis dépend des options choisies au moment de la configuration de l'association de sécurité (SA) et de l'emplacement sur lequel elle est mise en oeuvre dans une topologie de réseau.

3.1.3 indice du paramètre de sécurité (SPI) [b-IETF RFC 4301]: valeur arbitraire de 32 bits utilisée par un receveur pour identifier l'association SA à laquelle un paquet entrant devrait être destiné.

3.1.4 données détectées [b-UIT-T F.4104]: données détectées par un capteur lié à un noeud capteur particulier.

3.1.5 capteur [b-UIT-T Y.4105]: dispositif électronique qui détecte une condition physique ou un composé chimique et fournit un signal électronique proportionnel à la caractéristique observée.

3.1.6 numéro de séquence [IETF RFC 4303]: champ de 32 bits non signé contenant un compteur qui augmente d'une unité pour chaque paquet envoyé, soit un numéro de séquence propre à l'association SA de chaque paquet.

3.2 Termes définis dans la présente Recommandation

La présente Recommandation définit les termes suivants:

3.2.1 contrôleur programmable: dispositif électronique qui contrôle les actionneurs en se fondant sur les données détectées par les capteurs.

3.2.2 association de sécurité avec gabarit (SAM): ensemble de paramètres propres à un protocole de sécurité. L'association SAM définit les services et les mécanismes nécessaires pour protéger le trafic en appliquant la méthode de chiffrement avec données de gabarit associées (EAMD). C'est le protocole associé à une association SAM qui redirige vers elle, en fonction des couches du protocole telles que la couche transport ou la couche du protocole Internet (IP). Il est possible d'inclure, dans ces paramètres, des identificateurs d'algorithmes, des modes, des identificateurs de couche à laquelle est appliqué le chiffrement EAMD ainsi que des clés de chiffrement.

4 Abréviations et acronymes

La présente Recommandation utilise les abréviations et les acronymes suivants:

AES	norme de chiffrement perfectionné (*advanced encryption standard*)
CBC	enchaînement de blocs de chiffrement (*cipher block chaining*)
CMAC	code d'authentification de message basé sur un chiffrement (*cipher-based message authentication code*)
EAMD	chiffrement avec données de gabarit associées (*encryption with associated mask data*)
EAMDSP	données utiles pour la sécurité de chiffrement EAMD (EAMD *security payload*)
ESP	données utiles de sécurité par encapsulage IP (*encapsulating security payload*)
ICS	système de contrôle industriel (*industrial control system*)
IoT	Internet des objets (*Internet of things*)
IP	protocole Internet (*Internet protocol*)
IPSec	sécurité IP (*IP security*)
IV	vecteur d'initialisation (*initialization vector*)
MAC	code d'authentification de message (*message authentication code*)
SA	association de sécurité (*security association*)
SAM	association de sécurité avec gabarit (*security association with mask*)
SAMD	base de données SAM (SAM *database*)
SPI	indice des paramètres de sécurité (*security parameters index*)
TCP	protocole de commande de transmission (*transmission control protocol*)
UDP	protocole de datagramme d'utilisateur (*user datagram protocol*)

USN réseaux de capteurs ubiquitaires (*ubiquitious sensor networks*)

XOR OU exclusif (*exclusive* OR)

5 Conventions

Aucune.

6 Présentation du chiffrement avec données de gabarit associées (EAMD)

6.1 Spécification de la procédure EAMD

On dénombre un ensemble varié de menaces de sécurité pour les environnements de l'IoT [b-ZT]. La présente Recommandation se concentre sur les menaces suivantes:

1) Les attaques par usurpation d'identité (*impersonation attacks*) qui interceptent des données légitimes ou de fausses données légitimes et conduisent à une divulgation ou une altération des informations.
2) Les écoutes illicites qui consistent à capturer des paquets appartenant au réseau et transmis par les ordinateurs d'autres personnes et à lire le contenu des données à la recherche d'informations confidentielles de toute sorte.
3) Les attaques par mystification (*spoofing attacks*) qui prennent l'apparence d'un composant légitime afin d'obtenir des données ou altérer des informations.

Afin de réduire ces menaces pour les environnements de l'IoT, en particulier pour les dispositifs de l'IoT, la présente Recommandation détaille la méthode de chiffrement avec données de gabarit associées (EAMD), qui consiste à réaliser des opérations cryptographiques ciblées sur certaines parties des paquets de communication simples transmis entre plusieurs dispositifs. Les opérations cryptographiques comprennent le chiffrement et le déchiffrement, la production/vérification du code d'identification de message (MAC) et le chiffrement authentifié. Les algorithmes de chiffrement utilisés pour le chiffrement EAMD ne seront pas traités dans la présente Recommandation; toutefois, les normes [b-ISO/CEI 9797], [b-ISO/CEI 18033] et [b-ISO/CEI 19772] sont de bonnes références, respectivement, en matière d'algorithmes de chiffrement, d'algorithmes de code MAC et d'algorithmes de chiffrement authentifié.

Il est à noter que la construction décrite dans ce paragraphe peut être envisagée comme un protocole utilisant le modèle "chiffrement suivi du code MAC" de type [b-ASIACRYPT] et [b-EUROCRYPT].

Dans le paquet de communication, les blocs de données sur lesquels des opérations de chiffrement sont effectuées sont indiqués à l'aide d'un gabarit.

On partira du principe que l'expéditeur connaît l'algorithme de chiffrement, la clé, le vecteur initial et le gabarit pour une communication sécurisée par chiffrement EAMD, et que l'expéditeur et le receveur connaissent l'identificateur de l'algorithme et la clé de l'autre. Avec ce postulat, la communication sécurisée par chiffrement EAMD est réalisée grâce à l'obtention par l'expéditeur des informations pour le chiffrement EAMD, qui les partage avec le receveur. La Figure 1 est une présentation générale du chiffrement avec données de gabarit associées (EAMD).

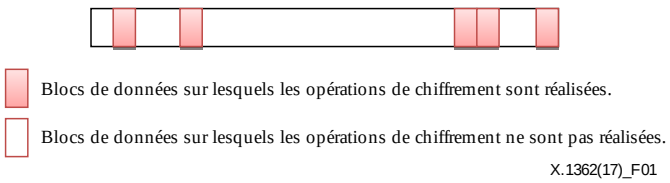

Figure 1 – Paquet de communication transmis en utilisant le chiffrement avec données de gabarit associées

Dans une communication sécurisée par chiffrement EAMD, le traitement des paquets sortants s'effectue de la manière suivante:

1) Ajout d'un bourrage indispensable pour le chiffrement.
2) Extraction des données pour procéder au chiffrement à l'aide du gabarit pour le chiffrement et copie dans la mémoire tampon, utilisée pour les calculs temporaires.
3) Chiffrement du résultat dans la mémoire tampon au moyen de la clé, de l'algorithme de chiffrement et de toute autre donnée nécessaire.
4) Substitution du résultat dans le paquet à l'aide du gabarit.
5) Encapsulation du résultat dans le champ des données utiles.

Si l'option intégrité est sélectionnée, le traitement s'effectue comme suit[1]:

6) Extraction des données pour la production d'un code MAC à l'aide du gabarit pour la production de code MAC et copie dans la mémoire tampon.
7) Ajout d'un bourrage indispensable pour la production du code MAC.
8) Production du code MAC à partir du résultat dans la mémoire tampon.
9) Ajout du code MAC dans le paquet.

La Figure 2 illustre le traitement d'un paquet sortant.

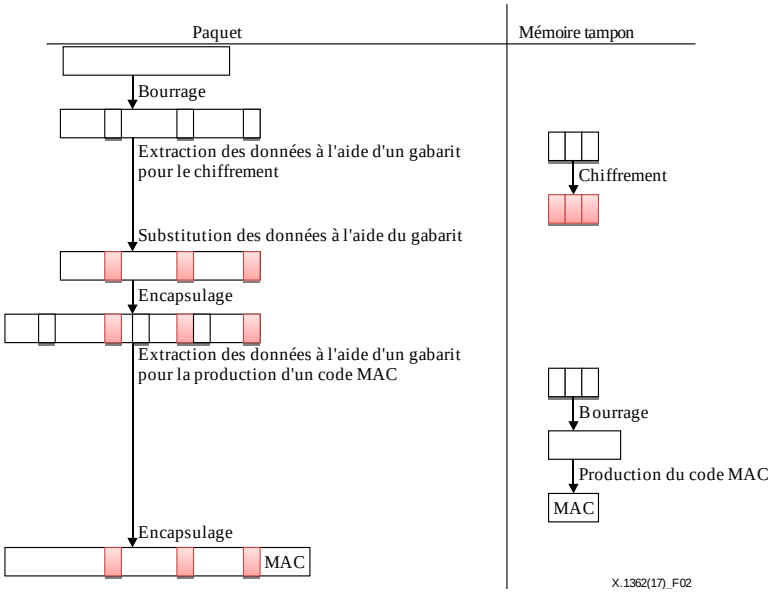

Figure 2 – Production d'un paquet en utilisant la méthode de chiffrement avec données de gabarit associées pendant le traitement d'un paquet sortant

Dans une communication sécurisée par chiffrement EAMD, le traitement des paquets entrants s'effectue de la manière suivante:

Si l'option intégrité est sélectionnée, les étapes 1 à 3 ci-après doivent être respectées[1]:

1) Extraction des données du paquet, à l'exception du code MAC, et copie dans la mémoire tampon selon le gabarit pour la production de code MAC.
2) Ajout d'un bourrage indispensable pour la production du code MAC.

[1] Lors de l'utilisation du chiffrement avec données de gabarit associé pour établir un lien avec le protocole ESP pour la sécurité IP (IPsec), il convient d'assurer la confidentialité par le biais de l'authentification.

3) Calcul du code MAC à partir des données de bourrage à l'aide de l'algorithme d'intégrité spécifié et vérification de son identité avec le code MAC contenu dans le paquet. Si le code MAC calculé est identique au code MAC reçu, alors le paquet est considéré comme valable et est accepté. Si les codes MAC sont différents, alors le receveur doit considérer le paquet reçu comme non valable.

4) Suppression de l'en-tête du paquet.

5) Extraction des données du résultat et copie dans la mémoire tampon selon le gabarit en vue du déchiffrement.

6) Déchiffrement dans la mémoire tampon du résultat ayant été extrait.

7) Substitution du résultat contenu dans la mémoire tampon dans le paquet à l'aide du gabarit pour le déchiffrement.

8) Suppression du bourrage pour le chiffrement du paquet.

La Figure 3 illustre le traitement d'un paquet entrant.

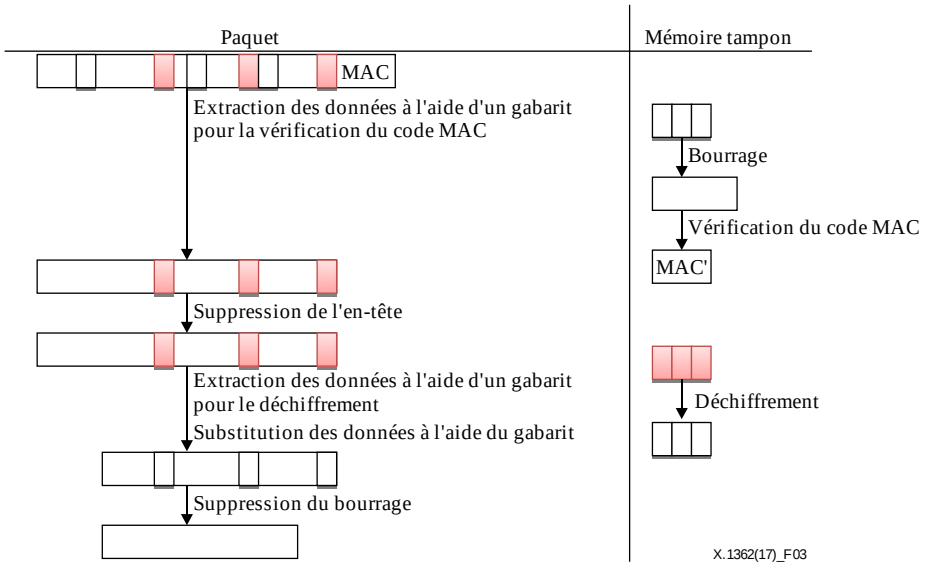

Figure 3 – Production d'un paquet en utilisant le chiffrement avec données de gabarit associées pendant le traitement d'un paquet entrant

6.2 Gabarit d'extraction des données cibles en vue du chiffrement avec données de gabarit associées

Pour les opérations de chiffrement avec données de gabarit associées, la cible du bloc de données entrant pour l'algorithme correspondant est extraite en divisant le paquet en blocs dont la taille correspond à celle utilisée par l'algorithme de chiffrement, en se basant sur le paramètre du gabarit.

7 Chiffrement avec données de gabarit associées

Ce paragraphe indique la façon dont il est possible de fournir un ensemble de services de sécurité pour le trafic dans chaque couche. La présente Recommandation décrit une méthode de communication sécurisée grâce au chiffrement avec données de gabarit associées, lui-même fondé sur les données utiles pour la sécurité de chiffrement EAMD (EAMDSP). La Figure 4 est une description générale de cette méthode de communication. Le flux détaillé de la communication sécurisée par chiffrement EAMD est décrit de la manière suivante:

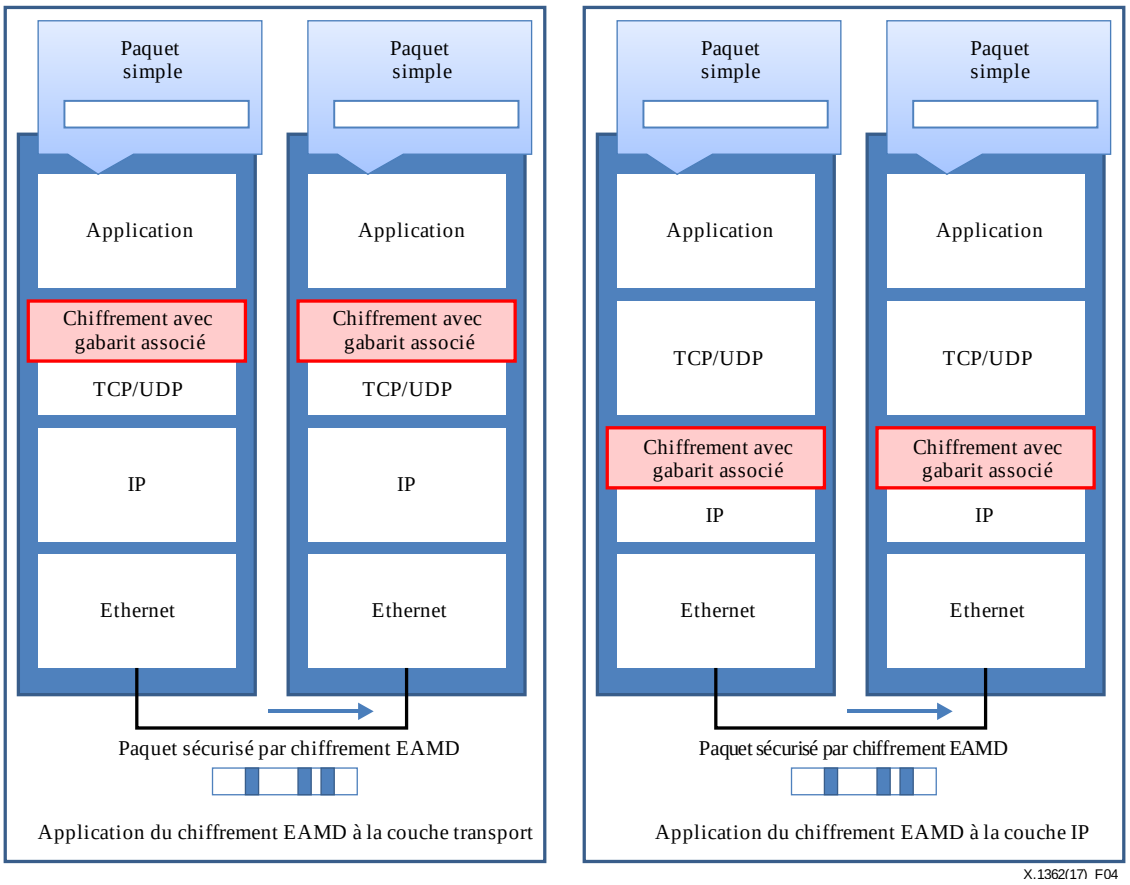

Figure 4 – Description générale de la communication sécurisée par chiffrement avec données de gabarit associées

7.1 Association de sécurité avec gabarit (SAM)

L'association de sécurité avec gabarit (SAM) est définie comme un ensemble de paramètres propres à un protocole de sécurité. L'association SAM définit les services et les mécanismes nécessaires pour protéger le trafic en appliquant la méthode de chiffrement EAMD. C'est le protocole associé à une association SAM qui redirige vers elle, en fonction des couches du protocole telles que la couche transport ou la couche du protocole Internet (IP). Il est possible d'inclure, dans ces paramètres, des identificateurs d'algorithmes, des modes, un identificateur de couche à laquelle est appliqué le chiffrement EAMD, des paramètres propres à une couche tels que l'adresse et le port IP, ainsi que des clés de chiffrement. L'association SAM contient un CryptCtx, qui est défini comme étant un ensemble de paramètres de chiffrement. La base de données relative à l'association SAM (SAMD) contient des données sur l'état associées à l'association SAM.

Le Tableau 1 contient l'ensemble des paramètres obligatoires de ce format.

Tableau 1 – Paramètres obligatoires du CryptCtx de l'association de sécurité (SA)

N°	Paramètre	Signification
1	encAlg	Identificateur de l'algorithme pour le chiffrement
2	encKey	Clé pour le chiffrement
3	encMask	Zone où a lieu le chiffrement

Le Tableau 2 contient l'ensemble des paramètres optionnels.

Tableau 2 – Paramètres optionnels du CryptCtx de l'association de sécurité (SA)

N°	Paramètre	Signification
1	encRoundKey	Clé de séquence pour le chiffrement
2	decRoundKey	Clé de séquence pour le déchiffrement
3	encIV	Vecteur initial (IV) pour le chiffrement
4	macRoundKey	Clé de séquence pour le code MAC
5	macK1	Sous-clé pour le code CMAC K1
6	macK2	Sous-clé pour le code CMAC K2
7	KeyStream	Nombres aléatoires générés à l'avance
8	KeyStreamHead	Pointeur de l'en-tête des nombres aléatoires non utilisés
9	KeyStreamTail	Pointeur de la partie terminale des nombres aléatoires non utilisés
10	EncIVTail	Vecteur initial pour la génération de nombres aléatoires
11	macAlg	Identificateur d'algorithme pour le code MAC
12	macKey	Clé pour le code MAC
13	macMask	Zone utilisée pour générer un code MAC par un algorithme choisi

7.2 Format du paquet de données utiles pour la sécurité de chiffrement EAMD (EAMDSP)

La Figure 5 est une illustration du format d'un paquet de données utiles pour la sécurité de chiffrement EAMD (EAMDSP). Le paquet commence avec l'en-tête des données utiles EAMDSP de longueur variable. Après ce champ vient celui des données utiles, dont la structure dépend du choix qui a été fait concernant l'algorithme et le mode de chiffrement. Après le champ des données utiles viennent les champs du bourrage, de la longueur de bourrage et de l'en-tête suivant. Le champ du code d'authentification du message (MAC), optionnel, se trouve en fin de paquet. La partie terminale du paquet EAMDSP comprend les champs du bourrage, de la longueur de bourrage et de l'en-tête suivant.

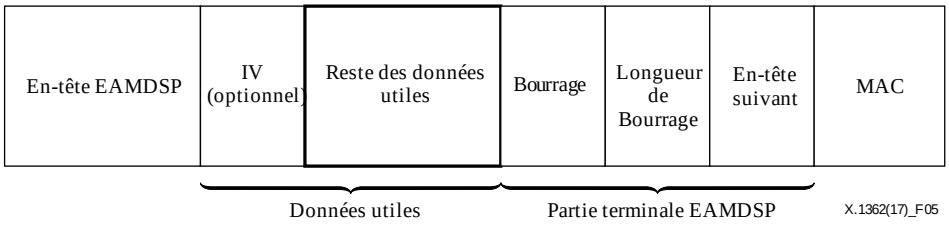

Figure 5 – Format d'un paquet EAMDSP

La partie terminale EAMDSP (transmise) comprend les champs du bourrage, de la longueur de bourrage et de l'en-tête suivant. Les données additionnelles et cachées de la partie terminale du paquet EAMDSP (qui ne sont pas transmises) sont comprises dans le calcul de l'intégrité.

Si le service d'intégrité est sélectionné, le calcul de l'intégrité englobe l'en-tête EAMDSP, les données utiles et la partie terminale du paquet EAMDSP. Si le service de confidentialité est sélectionné, le cryptogramme comprend les données utiles (à l'exception des données de synchronisation du chiffrement qui peuvent figurer parmi les données utiles) et la partie terminale du paquet EAMDSP.

Les paragraphes suivants décrivent les champs du format de l'en-tête. La mention "optionnel" signifie que le champ est omis si l'option n'a pas été sélectionnée, c'est-à-dire qu'il n'est présent ni dans le paquet qui est transmis ni dans le paquet formaté pour le calcul du code MAC. La sélection d'une option se fait lors de la configuration de l'association SAM. Ainsi, le format des paquets EAMDSP correspondant à une association SAM est valable pour la durée de cette association. A l'inverse, la

mention "obligatoire" signifie que le champ est toujours présent dans le format du paquet EAMDSP, quelle que soit l'association SAM.

7.2.1 Données utiles

Les données utiles sont un champ de longueur variable qui contient des données (du paquet d'origine) décrites dans le champ de l'en-tête suivant. Le champ des données utiles est obligatoire et a une longueur égale à un nombre entier d'octets. Si l'algorithme utilisé pour le chiffrement des données utiles nécessite des données de synchronisation cryptographique, par exemple un vecteur d'initialisation (IV), alors ces données apparaissent explicitement dans le champ des données utiles, mais elles ne figurent pas dans un champ à part dans le paquet EAMDSP, ce qui veut dire que la transmission d'un IV explicite n'est pas visible au niveau du paquet EAMDSP.

7.2.2 Bourrage (pour le chiffrement)

Si on utilise un algorithme de chiffrement qui nécessite que le texte en clair soit un multiple d'un certain nombre d'octets, par exemple un multiple de la taille de bloc d'un chiffrement par blocs, le champ du bourrage est utilisé pour donner au texte en clair (qui comprend les champs des données utiles, du bourrage, de la longueur de bourrage et de l'en-tête suivant) la taille requise par l'algorithme.

7.2.3 Longueur de bourrage

Le champ de la longueur de bourrage indique le nombre d'octets de bourrage situés immédiatement avant dans le champ du bourrage. Le champ de la longueur de bourrage est obligatoire.

7.2.4 En-tête suivant

Le champ de l'en-tête suivant est obligatoire. Il permet d'identifier le type de données contenues dans le champ des données utiles, par exemple l'en-tête et les données d'une couche suivante.

7.2.5 Code d'authentification de message (MAC)

Le code d'authentification de message est un champ de longueur variable calculé à partir des données indiquées par le gabarit pour assurer la protection de l'intégrité. Les champs implicites de la partie terminale du paquet EAMDSP tels que le bourrage pour la production d'un code MAC sont compris dans le calcul d'un code MAC. Le champ MAC est optionnel. Il est inclus uniquement si le service d'intégrité a été sélectionné et il est fourni soit par un algorithme d'intégrité distinct, soit par un algorithme au mode combiné qui utilise un code MAC. La longueur de ce champ est spécifiée par l'algorithme d'intégrité choisi et l'association SAM correspondante. La spécification de l'algorithme d'intégrité doit préciser la longueur du code MAC ainsi que les règles de comparaison et les étapes du processus pour sa vérification.

7.3 Traitement des paquets

7.3.1 Traitement des paquets sortants

Le traitement des paquets sortants à l'aide du chiffrement avec données de gabarit associées s'effectue comme suit:

1) Recherche de l'association SAM:

   Les données utiles EAMDSP sont appliquées à un paquet sortant uniquement une fois qu'il a été établi que l'association SAM correspondante nécessite un traitement EAMDSP, sur la base d'informations telles que l'identificateur de couche et les paramètres propres à la couche comme l'adresse IP ou le numéro de port dans le paquet. L'association SAM indique la clé et les gabarits nécessaires pour le chiffrement et pour la production d'un code MAC.

2) La transformation des données au moyen du chiffrement EAMD est décrite au § 6.1.

3) Envoi du paquet:

L'en-tête d'origine est ajouté au paquet chiffré selon le processus EAMD, puis le paquet obtenu est envoyé dans le réseau.

7.3.2 Traitement des paquets entrants

Le traitement des paquets entrants à l'aide du chiffrement avec données de gabarit associées s'effectue comme suit:

1) Recherche de l'association SAM:

A la réception d'un paquet contenant un en-tête EAMDSP, le receveur détermine l'association SAM qu'il convient d'utiliser en faisant une recherche dans la base de données SAMD. L'entrée d'une association SAM dans la base de données SAMD indique également à quelle couche le chiffrement EAMD est appliqué lors du traitement des paquets sortants ainsi que les paramètres propres à la couche tels que l'adresse IP ou le numéro de port du paquet, et s'il devrait y avoir un champ de code MAC. De plus, l'entrée dans la base de données SAMD spécifie les algorithmes et les clés à utiliser pour le déchiffrement et la vérification du code MAC (s'il y a lieu).

2) Vérification des données de l'en-tête EAMDSP:

La vérification des données de l'en-tête EAMDSP peut se faire en utilisant certaines valeurs dans l'en-tête EADMSP et doit être effectuée avant la vérification de l'intégrité et le déchiffrement. Si cette vérification échoue, le paquet est considéré comme non valable.

La transformation des données au moyen du chiffrement EAMD est décrite au § 6.1.

8 Chiffrement EAMD avec algorithme de chiffrement authentifié

8.1 Association de sécurité avec gabarit (SAM)

Dans le cas d'un chiffrement EAMD avec algorithme de chiffrement authentifié, l'association SAM est également définie conformément au § 7.1.

Le Tableau 3 contient l'ensemble des paramètres obligatoires de ce format.

Tableau 3 – Paramètres obligatoires du CryptCtx de l'association SA

N°	Paramètre	Signification
1	auencAlg	Identificateur de l'algorithme pour le chiffrement authentifié
2	auencKey	Clé pour le chiffrement authentifié
3	encMask	Zone où a lieu le chiffrement

Le Tableau 4 contient l'ensemble des paramètres optionnels.

Tableau 4 – Paramètres optionnels du CryptCtx de l'association SA

N°	Paramètre	Signification
1	auencRoundKey	Clé de séquence pour le chiffrement authentifié
2	audecRoundKey	Clé de séquence pour le déchiffrement
3	IV	Vecteur initial (IV) pour le chiffrement authentifié
4	Nonce	Clé de séquence pour le chiffrement authentifié

8.2 Format du paquet des données utiles pour la sécurité de chiffrement EAMD (EAMDSP)

La Figure 6 est une illustration du format d'un paquet de données utiles pour la sécurité de chiffrement EAMD (EAMDSP). Le paquet commence avec l'en-tête de données utiles EAMDSP, de longueur variable. Après ce champ vient celui des données utiles, dont la structure dépend du choix qui a été fait concernant l'algorithme et le mode de chiffrement. Après le champ des données utiles viennent les champs du bourrage, de la longueur de bourrage et de l'en-tête suivant. La partie terminale du paquet EAMDSP comprend les champs du bourrage, de la longueur de bourrage et de l'en-tête suivant.

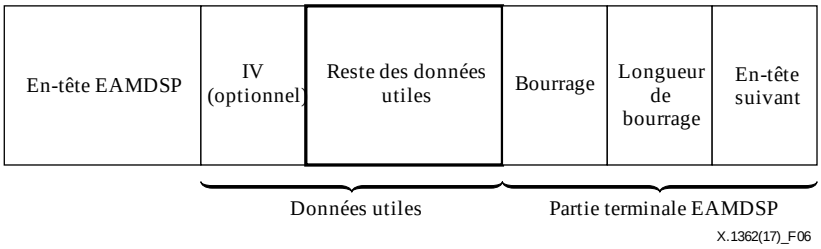

Figure 6 – Format d'un paquet EAMDSP (pour un chiffrement authentifié) sans code MAC

La partie terminale du paquet EAMDSP (transmise) comprend les champs du bourrage, de la longueur de bourrage et de l'en-tête suivant. Les données additionnelles et cachées de la partie terminale du paquet EAMDSP (qui ne sont pas transmises) sont comprises dans le calcul de l'intégrité.

Si le service d'intégrité est sélectionné, le calcul de l'intégrité englobe l'en-tête EAMDSP, les données utiles et la partie terminale du paquet EAMDSP. Si le service de confidentialité est sélectionné, le cryptogramme comprend les données utiles (à l'exception des données de synchronisation du chiffrement qui peuvent figurer parmi les données utiles) et la partie terminale du paquet EAMDSP.

Les paragraphes suivants décrivent les champs du format de l'en-tête. La mention "optionnel" signifie que le champ est omis si l'option n'a pas été sélectionnée, c'est-à-dire qu'il n'est présent ni dans le paquet qui est transmis ni dans le paquet formaté pour le calcul du code MAC. La sélection d'une option se fait lors de la configuration de l'association de sécurité SAM. Ainsi, le format des paquets EAMDSP correspondant à une association SAM est valable pour la durée de cette association. A l'inverse, la mention "obligatoire" signifie que le champ est toujours présent dans le format du paquet EAMDSP, quelle que soit l'association SAM.

8.2.1 Données utiles

Les données utiles sont un champ de longueur variable qui contient des données (du paquet d'origine) décrites dans le champ de l'en-tête suivant. Le champ de données utiles est obligatoire et a une longueur égale à un nombre entier d'octets.

Le format du paquet de données utiles de sécurité par encapsulage IP (ESP) peut être formulé de la manière suivante: ESP = SPI || Numéro de séquence || IV || C où C est le cryptogramme produit par l'algorithme de chiffrement authentifié. Dans ce cas, C porte l'étiquette d'authentification.

8.2.2 Bourrage (pour le chiffrement authentifié)

Si on utilise un algorithme de chiffrement authentifié qui nécessite que le texte en clair soit un multiple d'un certain nombre d'octets, par exemple un multiple de la taille de bloc d'un chiffrement par blocs, le champ de bourrage est utilisé pour donner au texte en clair (qui comprend les champs de données utiles, de bourrage, de la longueur de bourrage et de l'en-tête suivant) la taille requise par l'algorithme.

8.2.3 Longueur de bourrage

Le champ de la longueur de bourrage indique le nombre d'octets de bourrage situés immédiatement avant dans le champ du bourrage. Le champ de la longueur de bourrage est obligatoire.

8.2.4 En-tête suivant

Le champ de l'en-tête suivant est obligatoire. Il permet d'identifier le type de données contenues dans le champ de données utiles, par exemple l'en-tête et les données d'une couche suivante.

8.3 Traitement des paquets

8.3.1 Traitement des paquets sortants

Le traitement des paquets sortants à l'aide du chiffrement avec données de gabarit associées s'effectue comme suit:

1) Recherche de l'association SAM:

   Les données utiles EAMDSP sont appliquées à un paquet sortant uniquement une fois qu'il a été établi que l'association SAM correspondante nécessite un traitement EAMDSP, sur la base d'informations telles que l'identificateur de couche et les paramètres propres à la couche comme l'adresse IP ou le numéro de port dans le paquet. L'association SAM indique la clé et les gabarits nécessaires pour le chiffrement authentifié.

2) Transformation des données au moyen du mode de chiffrement authentifié EAMD:

   1) Ajout d'un bourrage indispensable pour le chiffrement.
   2) Extraction des données pour procéder au chiffrement à l'aide d'un gabarit de chiffrement et copie dans la mémoire tampon, utilisée pour les calculs temporaires.
   3) Chiffrement du résultat dans la mémoire tampon au moyen de la clé, de l'algorithme de chiffrement et toute autre donnée nécessaire.
   4) Substitution du texte chiffré dans le paquet à l'aide du gabarit.
   5) Ajout de l'étiquette d'authentification dans le paquet au niveau de l'emplacement du code MAC.

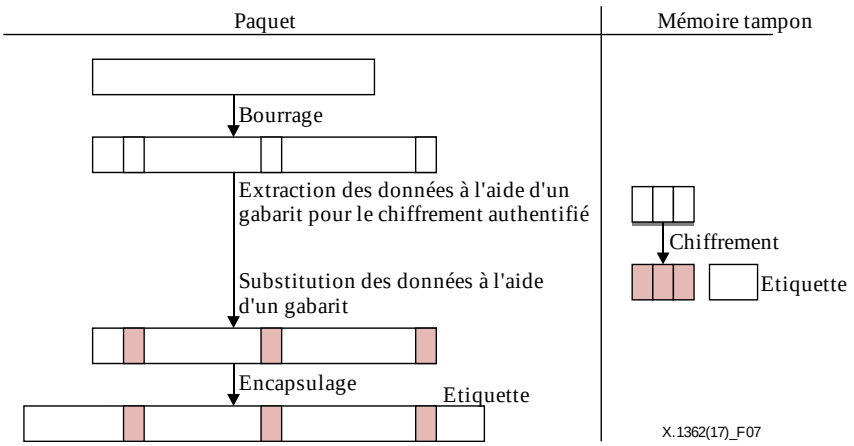

Figure 7 – Traitement des paquets sortants pour le mode de chiffrement authentifié

3) Envoi du paquet:

   L'en-tête d'origine est ajouté au paquet chiffré selon le processus EAMD, puis le paquet obtenu est envoyé dans le réseau.

8.3.2 Traitement des paquets entrants

Le traitement des paquets entrants à l'aide du chiffrement avec données de gabarit associées s'effectue comme suit:

1) Recherche de l'association SAM:

   A la réception d'un paquet contenant un en-tête EAMDSP, le receveur détermine l'association SAM qu'il convient d'utiliser en faisant une recherche dans la base de données SAMD. L'entrée d'une association SAM dans la base de données SAMD indique également à quelle couche le chiffrement EAMD a été appliqué lors du traitement des paquets sortants ainsi que les paramètres propres à la couche tels que l'adresse IP ou le numéro de port du paquet. De plus, l'entrée dans la base de données SAMD spécifie les algorithmes et les clés à utiliser pour le déchiffrement et la vérification de l'étiquette d'authentification.

2) Vérification des données de l'en-tête EAMDSP:

   La vérification des données de l'en-tête EAMDSP peut se faire en utilisant certaines valeurs dans l'en-tête EADMSP et doit être effectuée avant la vérification de l'intégrité et le déchiffrement. Si cette vérification échoue, le paquet est considéré comme non valable.

3) Transformation des données au moyen du mode de déchiffrement authentifié EAMD

   1) Suppression de l'en-tête du paquet.
   2) Extraction des données pour procéder au déchiffrement à l'aide du gabarit de déchiffrement et copie dans la mémoire tampon, utilisée pour les calculs temporaires.
   3) Séparation de l'étiquette d'authentification du reste du paquet et copie dans la mémoire tampon.
   4) Déchiffrement du résultat dans la mémoire tampon au moyen de la clé, de l'algorithme de déchiffrement et de toute autre donnée nécessaire.
   5) Substitution du résultat obtenu après déchiffrement dans le paquet à l'aide du gabarit, à condition que le déchiffrement n'ait pas échoué.

4) Suppression du bourrage pour le chiffrement du paquet.

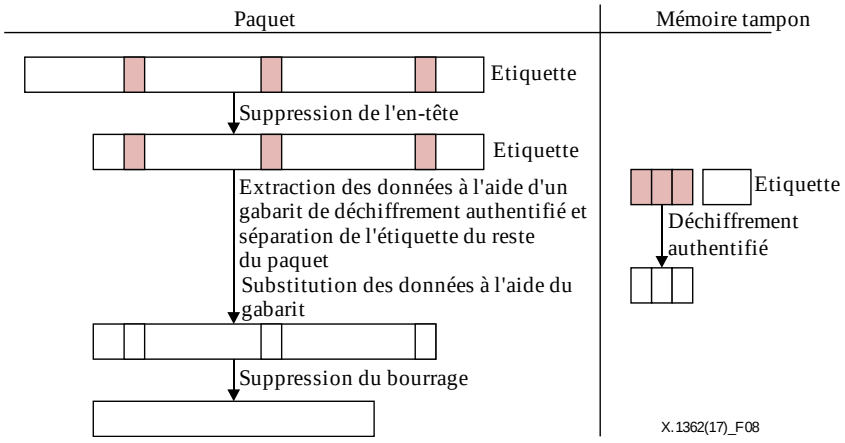

Figure 8 – Traitement des paquets entrants pour le mode de chiffrement authentifié

9 Conseils et limites

9.1 Conseils pour la configuration de l'association SAM

Pour ce qui est de la méthode de chiffrement EAMD, il convient de noter que si une entité malveillante était en mesure de modifier le gabarit, elle pourrait choisir une valeur pour le gabarit telle qu'aucune donnée ne serait chiffrée. Si un gabarit est altéré de cette façon, toutes les données du

dispositif seraient alors communiquées "en clair" (en d'autres termes, non chiffrées). Il s'agirait d'une vulnérabilité majeure sur le plan de la sécurité.

Pour que ce problème ne se pose pas, il faut tenir compte des questions suivantes:

1) Sécurité des communications avec un gabarit

   Pour l'initialisation et la mise à jour des données de calcul de clé comme les clés de chiffrement, les vecteurs initiaux et d'autres paramètres de sécurité, il existe un certain nombre de protocoles de configuration de clés, parmi lesquels la version 2 du Protocole d'échange de clés par Internet (IKEv2) [IETF RFC 7296], le protocole de concordance des clés et le protocole de transport des clés.

   Pour une communication entre entités associées, il convient de s'assurer que l'initialisation et la mise à jour du gabarit et des informations de calcul de clé concordent en utilisant ces protocoles. Par exemple, pendant le processus de communication pour la configuration de la clé, les informations de calcul de clé devraient contenir également les informations relatives au gabarit pour que l'intégrité et la confidentialité liées au gabarit puissent être garanties à l'aide d'algorithmes de chiffrement et d'algorithmes de codage MAC utilisés dans ces protocoles.

2) Sécurité pour le stockage des gabarits

   Il convient de s'assurer qu'une fois que le gabarit est appliqué au dispositif, il n'existe pas de protocole permettant à l'autre dispositif de le lire.

   A cette fin, les méthodes suivantes peuvent être envisagées.

   La première est un système sécurisé qui attribue les composants du système de telle sorte que les dispositifs qui se voient appliquer un chiffrement EAMD ne sont pas communiqués directement à une entité en dehors du système; à la place, un composant passerelle à la capacité de calcul élevée est communiqué à cette entité.

   La seconde méthode est une protection des dispositifs qui repose sur un matériel inviolable ou sur le principe d'offuscation du logiciel, lequel consiste à créer un code ayant fait l'objet d'une offuscation et difficilement compréhensible par les humains.

9.2 Conseils pour une utilisation appropriée des vecteurs d'initialisation et des nonces

Ce paragraphe fournit des conseils pour une utilisation appropriée des vecteurs d'initialisation (ainsi que des modes de chiffrement par bloc et du bourrage). La mauvaise utilisation des vecteurs d'initialisation ou du bourrage est une erreur fréquente dans les attaques contre les protocoles. Un vecteur IV ou un nonce (nombre arbitraire à usage unique) jouera vraisemblablement un rôle essentiel dans la sécurité du protocole.

Pour utiliser le mode d'enchaînement de blocs chiffrés (CBC) [ISO/CEI 10116] pour un chiffrement qui comprend une combinaison de blocs de texte en clair et de blocs de texte chiffré, il faut procéder de la manière décrite ci-dessous.

Lorsque le mode CBC est utilisé comme mode de traitement des blocs de texte chiffré, il convient d'envisager une sécurité contre les attaques par oracle de bourrage (*padding oracle attacks*) dont il est question dans [b-CBCPADD]. Le mode CBC nécessite qu'un vecteur IV soit combiné avec le premier bloc de texte en clair. Il n'est pas nécessaire que le vecteur IV soit secret, mais il doit être imprévisible.

Pour utiliser un algorithme de chiffrement authentifié de façon sûre, il faut procéder de la manière décrite ci-dessous.

Si une application n'est pas capable d'assurer l'exigence d'unicité relative au nonce lors de sa production, alors elle devrait utiliser un nonce de longueur nulle. Pour de telles applications,

l'utilisation d'algorithmes aléatoires ou d'algorithmes à états [b-IETF RFC 5116] est appropriée. Dans les autres cas, une application devrait utiliser des nonces d'une longueur de 12 octets.

Lorsque des nonces ou des vecteurs IV sont répétés, de nombreux systèmes doivent faire face à des attaques pratiques qui peuvent révéler, par exemple, l'OU exclusif (XOR) de deux paquets. En conséquence, il est vivement recommandé que le vecteur IV ou le mot de circonstance soit unique.

9.3 Limites quant à l'utilisation du chiffrement EAMD

L'utilisation du chiffrement EAMD est limitée par les exigences de traitement en temps réel du système.

L'intérêt du chiffrement EAMD est optimal pour les systèmes dans lesquels l'expéditeur et le destinataire ont tous les deux un certain niveau de capacité de calcul, par exemple lorsque l'architecture de l'unité centrale de traitement (CPU) est de 16 ou 32 bits et que le système est doté de capacités raisonnables en matière de fréquence (des centaines de MHz) et de mémoire.

Il convient de noter qu'il est peu probable que le chiffrement EAMD soit une solution adaptée pour les systèmes ayant des exigences de puissance limitées étant donné que la puissance requise pour la mise en mémoire tampon pour le chiffrement EAMD peut donner lieu à des opérations de traitement importantes.

Il convient également de noter que le gabarit est très sensible, tout comme la clé de chiffrement dont il a été question ci-dessus. On en conclut donc que le chiffrement EAMD ne devra être appliqué que lorsqu'il peut être estimé que le gabarit fera l'objet d'une gestion et d'une protection sûre.

Annexe A

Liens avec les protocoles en vigueur

(La présente Annexe fait partie intégrante de la présente Recommandation.)

Pour avoir une communication sécurisée en utilisant la méthode de chiffrement avec données de gabarit associées, il est nécessaire de déterminer la couche à laquelle le chiffrement s'applique. Différentes couches sont possibles, comme la couche transport, la couche IP, etc. La présente Annexe indique comment il est possible d'établir un lien entre le chiffrement avec données de gabarit associées et les protocoles existants. Dans le cas de l'établissement d'un lien entre le chiffrement avec données de gabarit associé et le protocole IPsec, il est nécessaire d'assurer la confidentialité et l'authentification. Il convient d'assurer la confidentialité par le biais de l'authentification [IETF RFC 7321].

A.1 Lien avec le protocole ESP pour la sécurité IP (IPsec) [IETF RFC 4303]

A.1.1 Format de l'association SAM

L'association SAM définit les services et les mécanismes nécessaires pour protéger le trafic en appliquant la méthode de chiffrement EAMD. La Figure A.1 illustre le format d'une association de sécurité avec gabarit (SAM) pour les cas où le chiffrement EAMD est appliqué à la couche réseau.

```
SecurityAssertion ::= SEQUENCE {
  layerIdentifier OCTET STRING (SIZE(1)),
  SPI             OCTET STRING (SIZE (4)),
  ipAddr          OCTET STRING (SIZE (4)),
  cryptCtx        CryptCtx
}
CryptCtx ::= SEQUENCE {
  encAlg    OCTET STRING (SIZE (4))
  encKey    OCTET STRING (SIZE (keySizeMax)),
  encMask   OCTET STRING (SIZE (maskLength))
}
keySizeMax INTEGER ::= 64
maskLength INTEGER ::= 16
```

Figure A.1 – Format de l'association SAM pour la couche réseau

A.1.2 Format du paquet

La Figure A.2 est une illustration du format d'un paquet de données utiles pour la sécurité de chiffrement EAMD (EAMDSP). Le paquet commence avec l'en-tête de données utiles EAMSDP, de longueur variable. Après ce champ vient celui des données utiles, dont la structure dépend du choix qui a été fait concernant l'algorithme et le mode de chiffrement. Après le champ de données utiles viennent les champs du bourrage, de la longueur de bourrage et de l'en-tête suivant. Le champ du code d'authentification du message (MAC), optionnel, se trouve à la fin du paquet. La partie terminale du paquet EAMDSP comprend les champs du bourrage, de la longueur de bourrage et de l'en-tête suivant. Compte tenu du volume de trafic causé par le chiffrement EAMD et les calculs pour le code MAC dans le cadre du chiffrement EAMD, le format peut suivre un autre modèle, dans lequel la longueur du numéro de séquence est 8B et le champ de l'en-tête suivant est positionné dans l'en-tête EAMDSP.

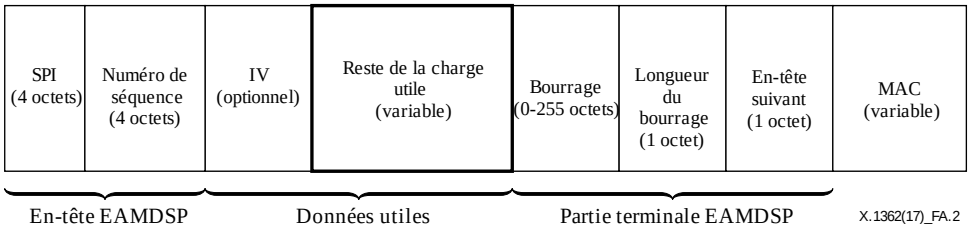

Figure A.2 – Exemple de format d'un paquet EAMDSP pour établir un lien avec le protocole ESP pour la sécurité IP

1) Indice des paramètres de sécurité (SPI):

L'indice des paramètres de sécurité est une valeur arbitraire de 32 bits utilisée par un receveur pour identifier l'association SAM à laquelle un paquet entrant devrait être destiné. Le champ de l'indice SPI est obligatoire. L'indice SPI est présent dans le protocole afin de permettre au système receveur de choisir l'association SAM qui permettra de traiter un paquet reçu.

2) Numéro de séquence:

Ce champ de 32 ou 64 bits non signé contient un compteur qui augmente d'une unité pour chaque paquet envoyé, soit un numéro de séquence propre à l'association SAM de chaque paquet ou, à défaut, une valeur générée selon une règle univoque.

3) Données utiles:

Les données utiles sont un champ de longueur variable qui contient des données (du paquet d'origine) décrites dans le champ de l'en-tête suivant. Le champ de données utiles est obligatoire et a une longueur égale à un nombre entier d'octets. Si l'algorithme utilisé pour le chiffrement des données utiles nécessite des données de synchronisation cryptographique, par exemple un vecteur d'initialisation (IV), alors ces données apparaissent explicitement dans le champ des données utiles, mais elles ne figurent pas comme un champ à part dans le paquet EAMDSP, ce qui veut dire que la transmission d'un vecteur IV explicite n'est pas visible au niveau du paquet EAMDSP.

4) Bourrage (pour le chiffrement):

Il se peut également qu'il soit nécessaire de procéder au bourrage, indépendamment des exigences de l'algorithme de chiffrement, afin de s'assurer que le texte chiffré obtenu se termine par une limite de 4 octets. Plus précisément, les champs de la longueur de bourrage et de l'en-tête suivant doivent être exactement alignés à l'intérieur d'un mot de 4 octets, comme indiqué dans les figures illustrant le format d'un paquet EAMDSP ci-dessus, afin de garantir que le champ du code MAC (s'il y a lieu) soit aligné sur une limite de 4 octets.

5) Longueur de bourrage:

Le champ de la longueur de bourrage indique le nombre d'octets de bourrage situés immédiatement avant dans le champ du bourrage. La fourchette de valeurs valables va de 0 à 225, avec une valeur de zéro signifiant qu'il n'y a aucun octet de bourrage. Le champ de la longueur de bourrage est obligatoire.

6) En-tête suivant:

Le champ de l'en-tête suivant est un champ obligatoire, de 8 bits, qui permet d'identifier le type de données contenues dans le champ de données utiles, par exemple l'en-tête et les données d'une couche suivante.

7) Code d'authentification de message (MAC)

Le code d'authentification de message est un champ de longueur variable calculé à partir des données indiquées par le gabarit pour assurer la protection de l'intégrité. Les champs implicites de la partie terminale d'un paquet EAMDSP, tels que le bourrage pour la production d'un code MAC, sont compris dans le calcul d'un code MAC. Le champ de code MAC est optionnel.

A.1.3 Traitement des paquets

Le traitement des paquets sortants à l'aide du chiffrement avec données de gabarit associées s'effectue comme suit:

1) Recherche de l'association SAM:

L'association SAM correspondante nécessitant un traitement EAMDSP est établie en fonction d'informations telles que l'identificateur de la couche et les paramètres propres à la couche comme l'adresse IP ou le numéro de port dans le paquet.

2) Transformation des données au moyen du chiffrement EAMD:

Le chiffrement et la production d'un code MAC sont réalisés en utilisant la méthode de chiffrement EAMD selon le processus décrit au § 6.1.

3) Envoi du paquet:

L'en-tête d'origine est ajouté au paquet chiffré selon le processus EAMD, puis le paquet obtenu est envoyé dans le réseau.

Le traitement des paquets entrants à l'aide du chiffrement avec données de gabarit associées s'effectue comme suit:

1) Recherche de l'association SAM:

L'association SAM correspondante nécessitant un traitement EAMDSP est établie en fonction d'informations telles que l'identificateur de couche, qui identifie la couche de transport, et l'adresse IP ou le numéro de port dans le paquet.

2) Vérification du numéro de séquence:

La vérification du numéro de séquence s'effectue en utilisant la valeur du numéro de séquence dans l'en-tête EAMDSP et doit être réalisée avant la vérification de l'intégrité et le déchiffrement. Si cette vérification échoue, le paquet est considéré comme non valable.

3) Transformation des données au moyen du chiffrement EAMD:

La vérification du code MAC et le déchiffrement sont réalisés en utilisant le processus de chiffrement EAMD décrit au § 6.1.

A.1.4 Gabarit d'extraction des données cibles pour le chiffrement avec données de gabarit associées

Pour les opérations de chiffrement avec données de gabarit associées, la cible du bloc de données entrant pour l'algorithme correspondant est extraite en divisant le paquet en blocs dont la taille correspond à celle de l'algorithme de chiffrement utilisé, en se basant sur le paramètre du gabarit. Par exemple, dans le cas d'un chiffrement avec données de gabarit associées au moyen d'une norme de chiffrement perfectionné (AES), les données utiles sont divisées en blocs de 128 bits car la longueur de bloc de la norme AES est de 128 bits. La cible du bloc de déchiffrement est extraite en trouvant le bloc à l'aide du gabarit. Ensuite, les données cibles pour cette opération sont obtenues par concaténation de la cible du bloc de déchiffrement. Le format du gabarit est décrit dans les Figures A.3 et A.4. Ce paramètre montre les blocs qui devraient être chiffrés ou déchiffrés dans le cas où les données utiles sont divisées en blocs dont la taille correspond à celle de l'algorithme de chiffrement utilisé.

```
MaskFormat ::= SEQUENCE {
  encryptionArea OCTET STRING (SIZE (12))
  reserved OCTET STRING (SIZE (4))
}
```

Figure A.3 – Format du gabarit

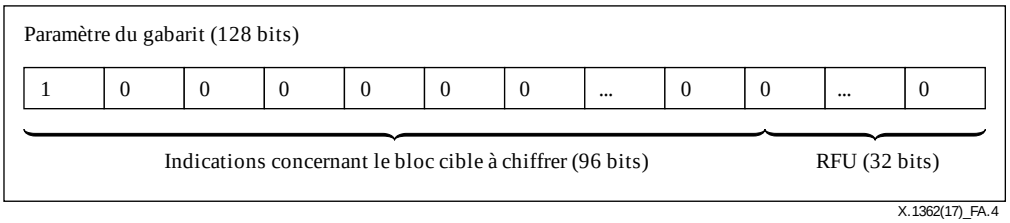

Figure A.4 – Format détaillé du paramètre du gabarit

Dans le cas présent, le paramètre du gabarit indique que seul le premier bloc est chiffré puisque le premier bit du paramètre du gabarit est vrai. Le chiffrement de certaines zones nécessite de changer certains bits du paramètre du gabarit de faux à vrai.

A.1.5 Algorithme de bourrage

Un algorithme de bourrage peut être décrit de la manière suivante:

– Ajouter '0x80' à la fin des données utiles.

– Si la longueur des données utiles est un multiple de la longueur de bloc de l'algorithme de chiffrement, le bourrage est terminé.

Si la longueur des données utiles n'est PAS un multiple de la longueur de bloc de l'algorithme de chiffrement, ajouter '0x00' à la fin des données utiles jusqu'à ce que la longueur des données utiles soit un multiple de cette valeur.

Bibliographie

[b-UIT-T F.4104] Recommandation UIT-T F.4104/F.744 (2009), *Description et spécifications de service concernant les intergiciels des réseaux de capteurs ubiquitaires*.

[b-UIT-T X.1311] Recommandation UIT-T X.1331 (2011) ISO/CEI 29180:2012, *Technologies de l'information – Cadre de sécurité des réseaux de capteurs ubiquitaires*.

[b-UIT-T X.1312] Recommandation UIT-T X.1312 (2011), *Lignes directrices sur la sécurité des intergiciels des réseaux de capteurs ubiquitaires*.

[b-UIT-T X.1313] Recommandation UIT-T X.1313 (2012), *Prescriptions de sécurité pour le routage dans les réseaux de capteurs sans fil*.

[b-UIT-T Y.4000] Recommandation UIT-T Y.4000/Y.2060 (2012), *Présentation générale de l'Internet des objets*.

[b-UIT-T Y.4105] Recommandation UIT-T Y.4105/Y.2221 (2010), *Prescriptions de prise en charge pour les applications et services de réseaux de capteurs ubiquitaires dans l'environnement des réseaux de prochaine génération*.

[b-UIT-T Y.4109] Recommandation UIT-T Y.4109/Y.2061 (2012), *Spécifications relatives à la prise en charge d'applications de communication orientées machine dans l'environnement des réseaux de prochaine génération*.

[b-IETF RFC 4301] IETF RFC 4301 (2005), *Security Architecture for the Internet Protocol.*

[b-IETF RFC 5116] IETF RFC 5116 (2008), *An Interface and Algorithms for Authenticated Encryption.*

[b-ISO/CEI 9797] ISO/CEI 9797-1:2011, *Technologies de l'information – Techniques de sécurité – Codes d'authentification de message (MAC) – Partie 1: Mécanismes utilisant un cryptogramme bloc.*

[b-ISO/CEI 18033] ISO/CEI 18033-3:2010, *Technologies de l'information – Techniques de sécurité – Algorithmes de chiffrement – Partie 3: Chiffrement par blocs*.

[b-ISO/CEI 19772] ISO/CEI 19772:2009, *Technologies de l'information – Techniques de sécurité – Algorithmes de chiffrement – Partie 3: Chiffrage authentifié.*

[b-ASIACRYPT] Bellare, M., and Namprempre, C. (2000), *Authenticated encryption:* Relations *among notions and analysis of the generic composition paradigm*, in Tatsuaki Okamoto, editor, ASIACRYPT 2000, Vol. 1976 of LNCS, Springer, décembre, p. 531-545.

[b-CBCPADD] Vaudenay, S. (2002), *Security Flaws Induced by CBC Padding Applications to SSL, IPSEC, WTLS*, EUROCRYPT 2002.

[b-EUROCRYPT] Namprempre, C., Rogaway, P., and Shrimpton, T. (2014), *Reconsidering generic composition*, in Phong Q. Nguyen and Elisabeth Oswald, editors, EUROCRYPT 2014, Vol. 8441 of LNCS, Springer, mai, p. 257-274.

[b-ZT] Li, Zhang, and Xin, Tong (2013), *Threat Modeling and Countermeasures Study for the Internet of Things*, Journal of Convergence Information Technology (JCIT), Vol. 8, N° 5, mars.

SÉRIES DES RECOMMANDATIONS UIT-T

Série A	Organisation du travail de l'UIT-T
Série D	Principes de tarification et de comptabilité et questions de politique générale et d'économie relatives aux télécommunications internationales/TIC
Série E	Exploitation générale du réseau, service téléphonique, exploitation des services et facteurs humains
Série F	Services de télécommunication non téléphoniques
Série G	Systèmes et supports de transmission, systèmes et réseaux numériques
Série H	Systèmes audiovisuels et multimédias
Série I	Réseau numérique à intégration de services
Série J	Réseaux câblés et transmission des signaux radiophoniques, télévisuels et autres signaux multimédias
Série K	Protection contre les perturbations
Série L	Environnement et TIC, changement climatique, déchets d'équipements électriques et électroniques, efficacité énergétique; construction, installation et protection des câbles et autres éléments des installations extérieures
Série M	Gestion des télécommunications y compris le RGT et maintenance des réseaux
Série N	Maintenance: circuits internationaux de transmission radiophonique et télévisuelle
Série O	Spécifications des appareils de mesure
Série P	Qualité de transmission téléphonique, installations téléphoniques et réseaux locaux
Série Q	Commutation et signalisation et mesures et tests associés
Série R	Transmission télégraphique
Série S	Equipements terminaux de télégraphie
Série T	Terminaux des services télématiques
Série U	Commutation télégraphique
Série V	Communications de données sur le réseau téléphonique
Série X	**Réseaux de données, communication entre systèmes ouverts et sécurité**
Série Y	Infrastructure mondiale de l'information, protocole Internet, réseaux de prochaine génération, Internet des objets et villes intelligentes
Série Z	Langages et aspects généraux logiciels des systèmes de télécommunication

Imprimé en Suisse
Genève, 2017