

IPv6 et la sécurité: IPsec

Objectif:
Sécuriser ...

IPsec

- Toutes les implémentations conformes IPv6 doivent intégrer IPsec
- Services
 - Confidentialité des données
 - Confidentialité du flux des données
 - Authentification de l'origine des données
 - Authentification mutuelle
 - Intégrité des données
 - Prévention contre le rejeu des données
 - Non-répudiation
- Attaques
 - IP sniffing, spoofing, flooding
 - Écoute, usurpation de l'identité, inondation de messages

Orientations IETF

- Deux extensions IP de sécurité
 - Authentification: AH Authentication Header
 - Services d'authentification, intégrité des données
 - Optionellement détection de rejeu et non-répudiation
 - Confidentialité: ESP Encapsulating Security Payload
 - Services de confidentialité, intégrité, authentification et détection de rejeu
 - Confidentialité du flux (au moins de façon limitée)
- Deux modes de protection
 - Transport
 - Tunnel

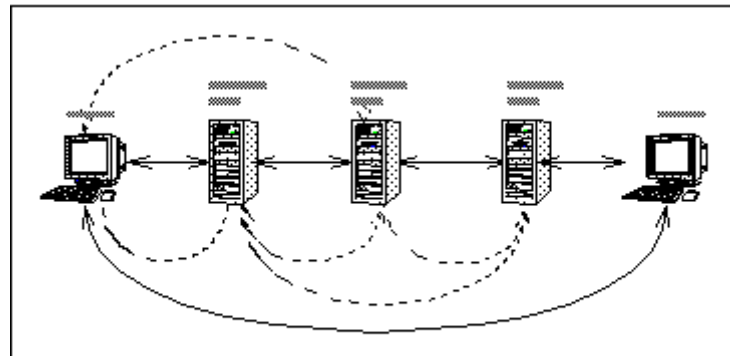


Figure 12-1. Différents modes de protection

Association de sécurité

- L'ensemble des services et mécanismes de sécurité choisis par les deux entités du réseau forme l'association de sécurité de la communication
- Unidirectionnelle
 - $A \rightarrow B$ et, éventuellement, $B \rightarrow A$
- identifiée par le triplet:
 - SPI Security Parameters Index
 - (SAID: Security Association Identifier)
 - Adresse du destinataire du paquet IP
 - Protocole de sécurité AH ou ESP

Contenu d'une association de sécurité

- AH:
 - Algorithme d'authentification, clés de chiffrement, ...
- ESP
 - Algorithme de chiffrement, clés de chiffrement,...
 - Algorithme d'authentification, clés de chiffrement
 - Si le service d'authentification est choisi
- Durée de vie
 - Pour éviter que les clés de chiffrement soient utilisées trop longtemps
- Mode du protocole IPsec
 - Transport
 - Tunnel
 - (Wildcard, c-à-d choisi par l'application)

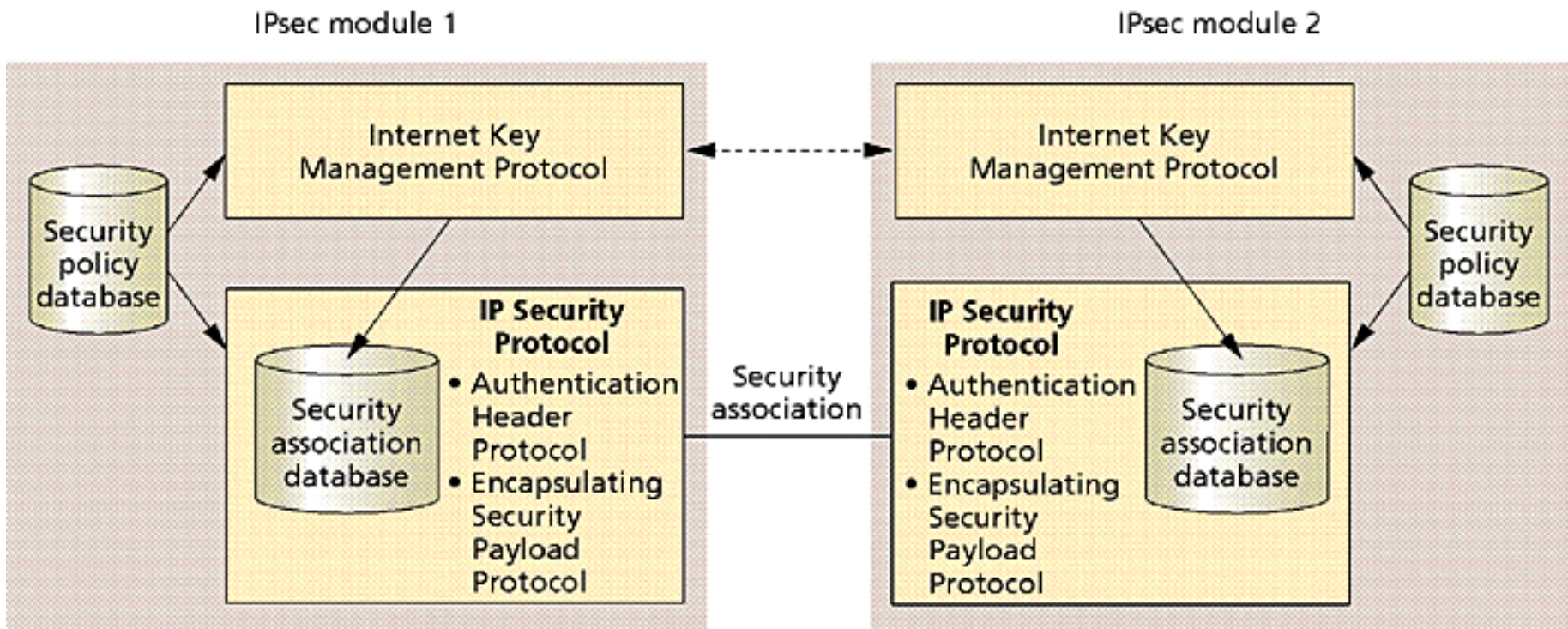
Choix d'une association de sécurité

- Choix, au niveau station émettrice ou passerelle de sécurité, dépend des paramètres suivants (sélecteurs):
 - Adresse IP de la source
 - Identité de l'utilisateur
 - Identité de l'équipement
 - Numéros de ports source et destination
 - Protocole de niveau transport
 - Adresse IP de l'équipement distant
 - Niveau de sensibilité des données
 - RFC 1108 <http://www.ietf.org/rfc/rfc1108.txt>
- En général on utilise
 - Adresse IP de destination
 - Numéro de protocole
 - Numéros de port

Bases de données

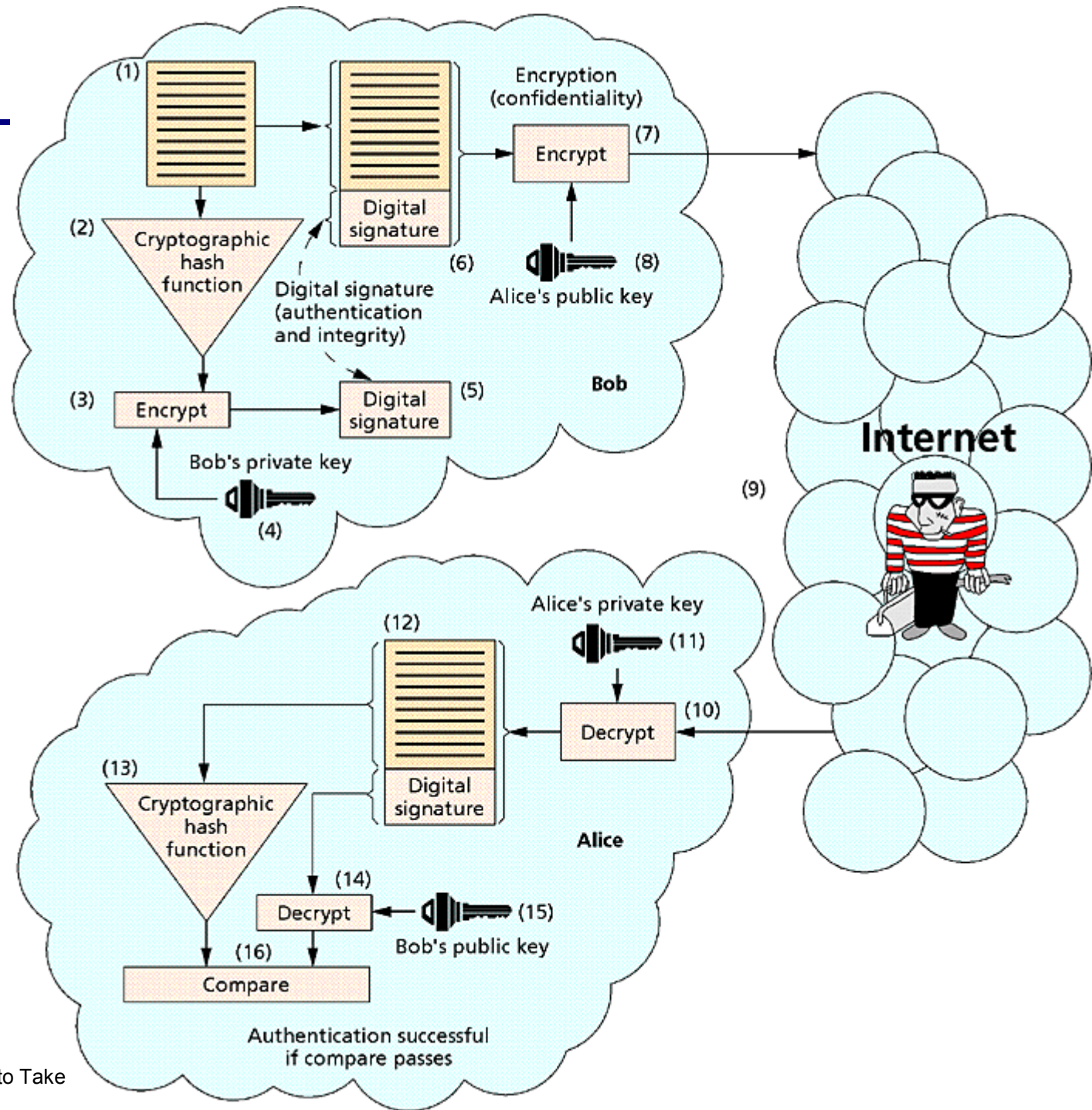
- IETF conseille deux BD
 - Security Policy DB (SPD)
 - En fonction du sélecteur
 - Discard
 - Bypass IPsec
 - Apply IPsec

- Security Association DB (SAD)
 - Services et mécanismes à appliquer
 - RFC 2401 → 2401bis
 - <http://www.ietf.org/rfc/rfc2401.txt>



PGP

- Pretty Good Privacy
 - Zimmerman, MIT



Source: P. Dowd et al., "Network Security: It's Time to Take It Seriously", IEEE Computer, Sep. 1998, pp. 24-28

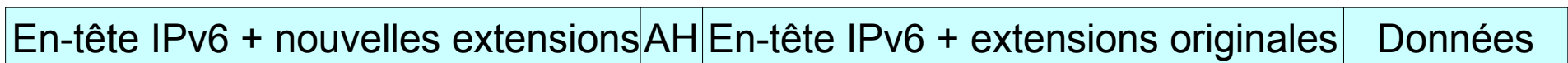
Digests et Signatures numériques

- Digest
 - Condensé d'un document obtenu avec une fonction mathématique de hachage (Hash function)
 - ex. "message" \longrightarrow "msg"
- Digital Signature
 - Le fait d'encrypter un condensé avec la clef privée d'un utilisateur produit une signature numérique
 - elle garantit à la fois:
 - l'identité de l'auteur (authentification)
 - l'intégrité du message
 - l'impossibilité pour l'auteur de "répudier" son message
- Applications typiques
 - Echange de documents, téléchargement de programmes
 - Courrier Electronique

Positionnement de l'extension d'authentification



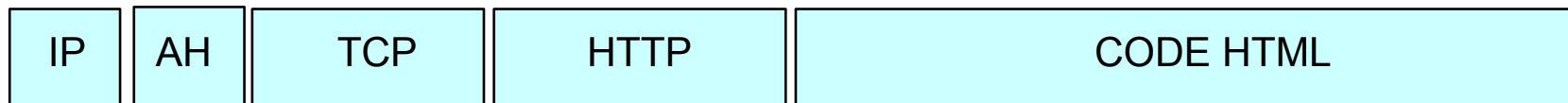
Mode transport



Mode tunnel

Authentication Header Protocol

- Authentification et intégrité
- Trois niveaux de clefs
 - host-oriented keying
 - user-oriented keying
 - session-unique keying





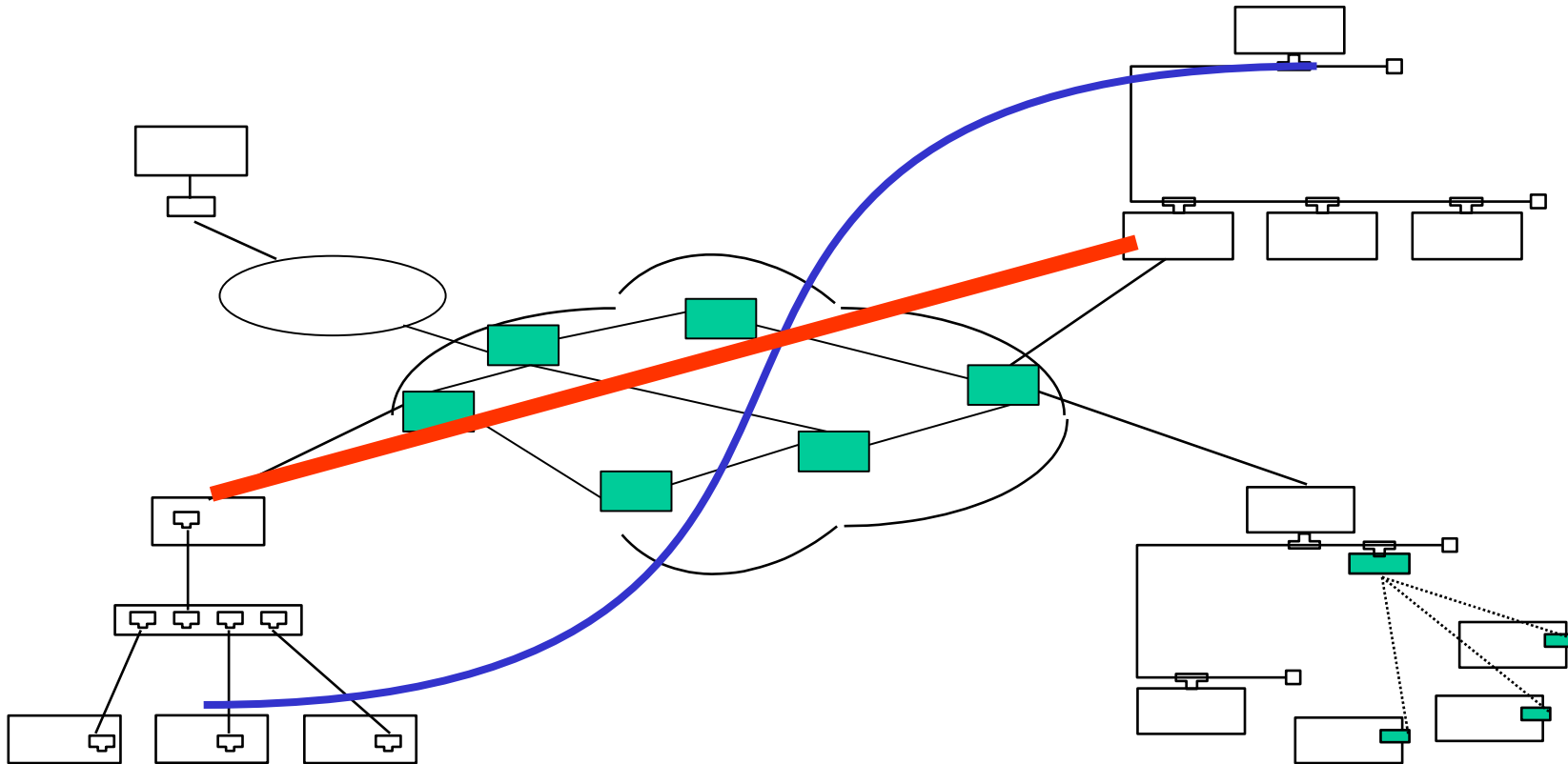
Encapsulating Security Payload Protocol

- Confidentialité
- Deux niveaux
 - Transport Layer Payload (le contenu du paquet)
 - entire IP packet (tout le paquet y compris l'en-tête)



Modes d'opération

- Deux modes d'opération
 - transport mode 
 - adresses source et destination en clair
 - tunnel mode 
 - adresses source et destination cachées



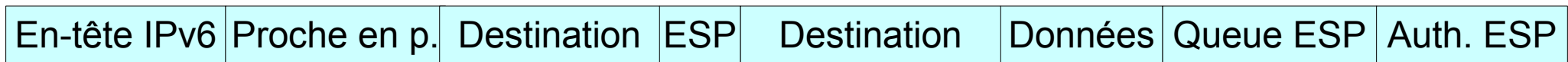
Contenu de l'extension d'authentification

32

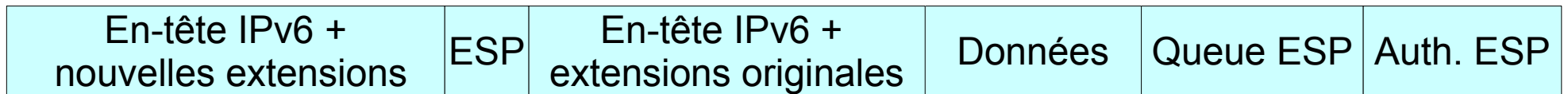
En-tête suiv.	Lg. extension	Réservé
Indice des paramètres de sécurité (SPI)		
Numéro de séquence		
Authentificateur (nombre variable de mots de 32 bits)		

Confidentialite

Les deux modes de protection



Mode transport



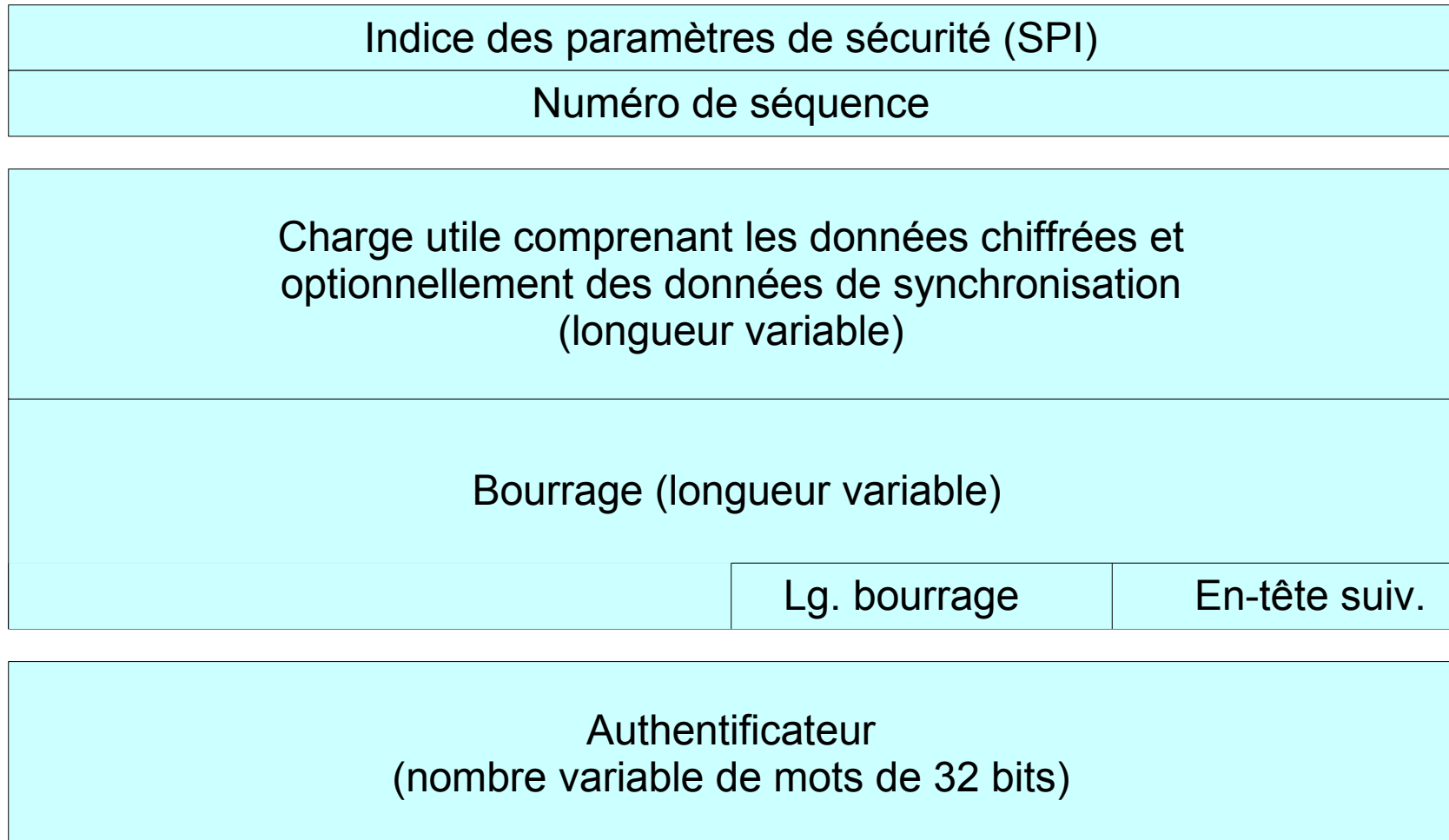
Mode tunnel



Contenu de l'extension de confidentialite

1

32



Questions

- 1 -
- 2 -
- 3 -
-
- Vos questions
-
-
-

Références

- IPv6 Théorie et Pratique, Chapitre Sécurité
 - <http://livre.point6.net/index.php/S%C3%A9curit%C3%A9>