RÉPUBLIQUE
FRANÇAISE
*Liberté*
*Égalité*
*Fraternité*

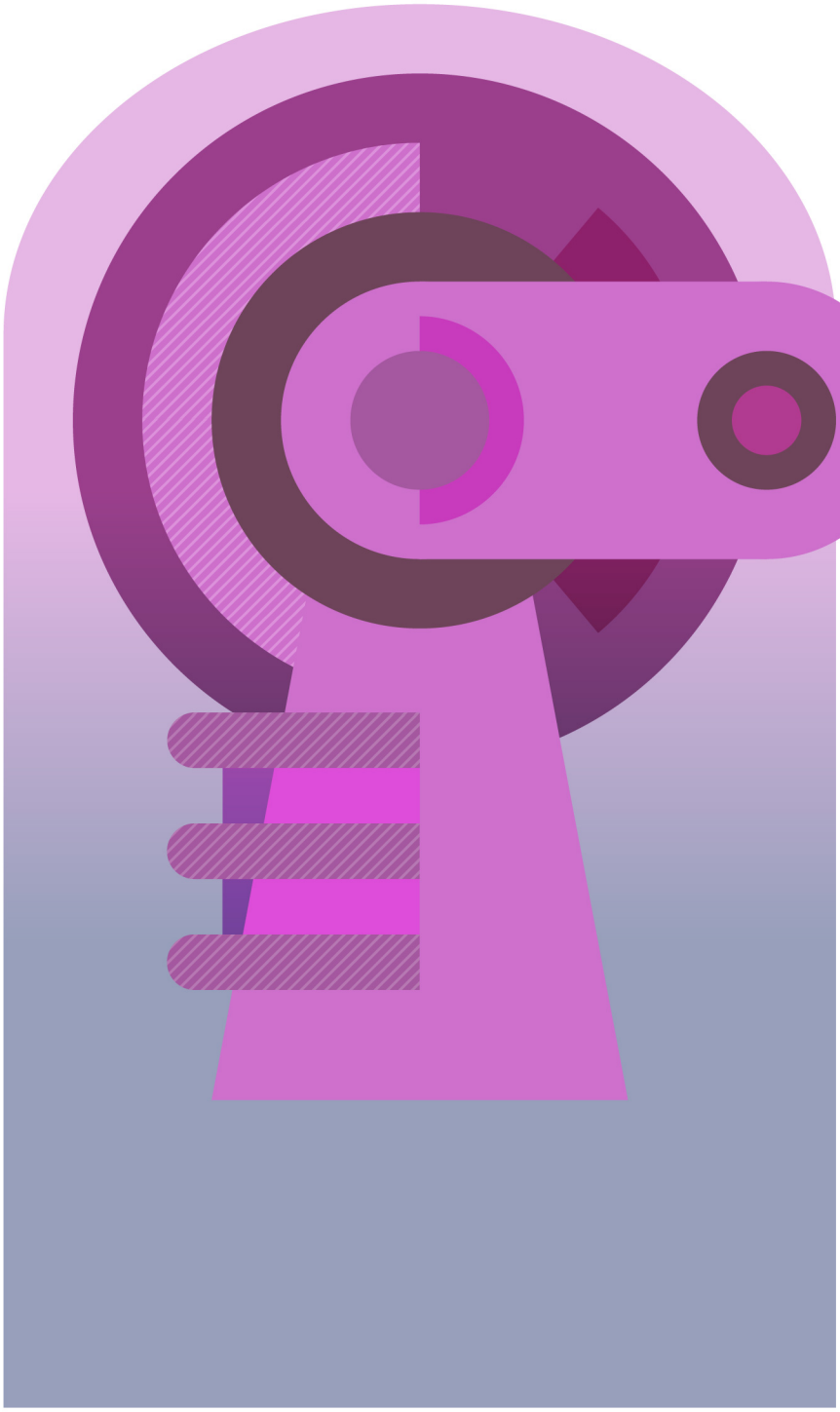
# TRANSITION POST-QUANTIQUE D'IPSEC

## FICHE TECHNIQUE ANSSI

ANSSI-FT-117
02/02/2026

**PUBLIC VISÉ :**

Développeur Administrateur RSSI DSI Utilisateur



# Informations

## Attention

Ce document rédigé par l'ANSSI s'intitule **« Transition Post-Quantique d'IPsec »**. Il est téléchargeable sur le site `cyber.gouv.fr`.



## Évolutions du document :

| VERSION | DATE | NATURE DES MODIFICATIONS |
|---|---|---|
| 1.0 | 02/02/2026 | Version initiale |

# Table des matières

# 1
# Introduction

Ce document vise à présenter un état des lieux de la transition post-quantique du protocole IPsec (Internet Protocol Security). Le protocole est composé de plusieurs protocoles définis dans une série de RFC [9, 10, 11, 12]. Le document présente d'abord le fonctionnement général du protocole. Ensuite, il identifie les parties du protocole concernées par la menace quantique et des solutions de transition associées. Il présente également les travaux existants sur le sujet. Ce document vient en complément de l'avis de l'ANSSI sur la transition post-quantique [1, 2].

Les mécanismes de cryptographie asymétrique utilisés aujourd'hui sont vulnérables à la menace quantique. Ainsi, le but de la transition post-quantique est de les remplacer par des mécanismes de cryptographie asymétrique dite post-quantique, supposée résistante à des attaques qui seraient réalisées sur un ordinateur classique et sur un ordinateur quantique. En particulier, les signatures de cryptographie classique sont remplacées par des signatures de cryptographie post-quantique, et les échanges de clés, souvent basés sur le schéma Diffie-Hellman (DH), sont remplacés par des échanges de clés basés sur des mécanismes d'encapsulation de clés (ou *Key Encapsulation Mechanism* (KEM)) post-quantiques. Pendant la transition post-quantique, l'hybridation est recommandée par l'ANSSI [1, 2]. Cela signifie l'utilisation d'un mécanisme de cryptographie asymétrique classique éprouvé, mais vulnérable à des attaques quantiques, combiné avec un mécanisme de cryptographie asymétrique supposé résistant aux attaques quantiques, mais pour lequel l'assurance de robustesse vis-à-vis des attaques réalisées à l'aide d'ordinateurs classique et quantique est moindre. Une conséquence de l'utilisation des mécanismes de cryptographie post-quantique dans les protocoles est une augmentation importante de la taille des messages échangés pendant les phases d'échange de clés et d'authentification. En effet, les mécanismes de cryptographie post-quantique existants possèdent des tailles de clés, de chiffrés et de signatures très grandes par rapport aux mécanismes de cryptographie classique. Quant aux mécanismes de cryptographie symétrique, la robustessse de ces derniers n'est pas menacée par l'ordinateur quantique. Toutefois, l'ANSSI recommande [1, 2] d'augmenter les tailles des clés du chiffrement symétrique et des sorties des fonctions de hachage.

# 2
# Présentation d'IPsec

IPsec est un protocole de communication sécurisé, souvent utilisé pour mettre en place un réseau virtuel privé (VPN) entre un initiateur et un répondeur. Un tunnel IPsec assure principalement la confidentialité et l'intégrité des paquets IP [1] qui y transitent, ainsi que l'authentification de l'initiateur et du répondeur. Il est composé de trois protocoles comme présenté dans la Figure 1 : IKEv2 [9] (*Internet Key Exchange*), AH [10] (*Authentication Header*) et ESP [11] (*Encapsulating Security Payload*). La partie impactée par la transition post-quantique est indiquée en rouge, il s'agit du protocole IKEv2.

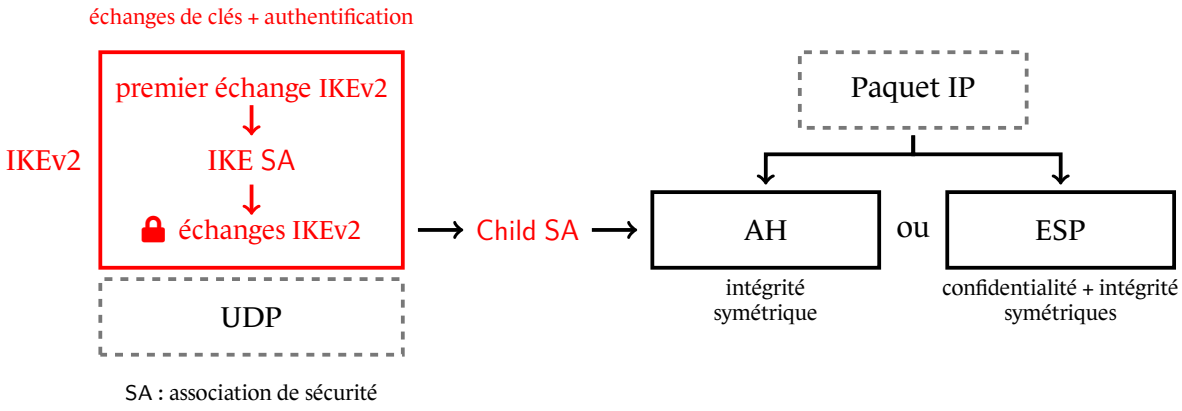



FIGURE 1 – Protocole IPsec

- Le protocole IKEv2 (*Internet Key Exchange*) permet à l'initiateur et au répondeur de s'authentifier mutuellement, de négocier les suites cryptographiques et d'établir des secrets partagés. Les suites cryptographiques négociées et les secrets partagés sont regroupés dans une structure appelée association de sécurité (SA), fournie au protocole qui protège les paquets IP (AH ou ESP). IKEv2 fonctionne au-dessus du protocole de transport UDP, et représente la partie *handshake* du protocole IPsec.

**Attention**

Le protocole IKEv2 est impacté par la menace quantique. En effet, des mécanismes asymétriques sont utilisés pour l'échange de clés (DH) et l'authentification mutuelle par signature de l'initiateur et du répondeur [1, 2].

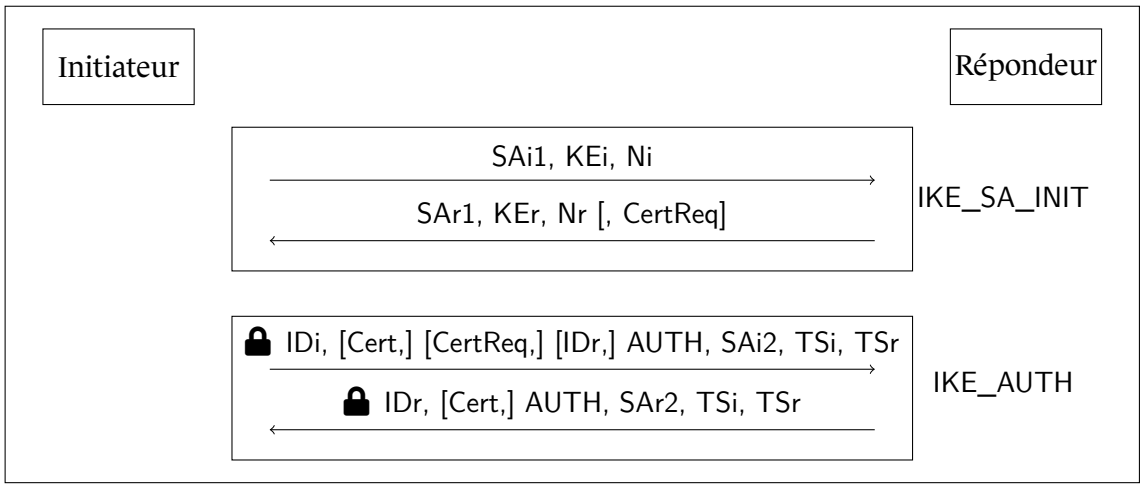
- Le protocole AH (*Authentication Header*) permet de protéger les paquets IP en intégrité, et assure une protection contre le rejeu de messages. Les données nécessaires à la protection (méca-

1. En fonction du type de protection choisi, l'intégralité du paquet IP peut être protégé (y inclut l'en-tête), ou uniquement les données contenues dans le paquet IP.

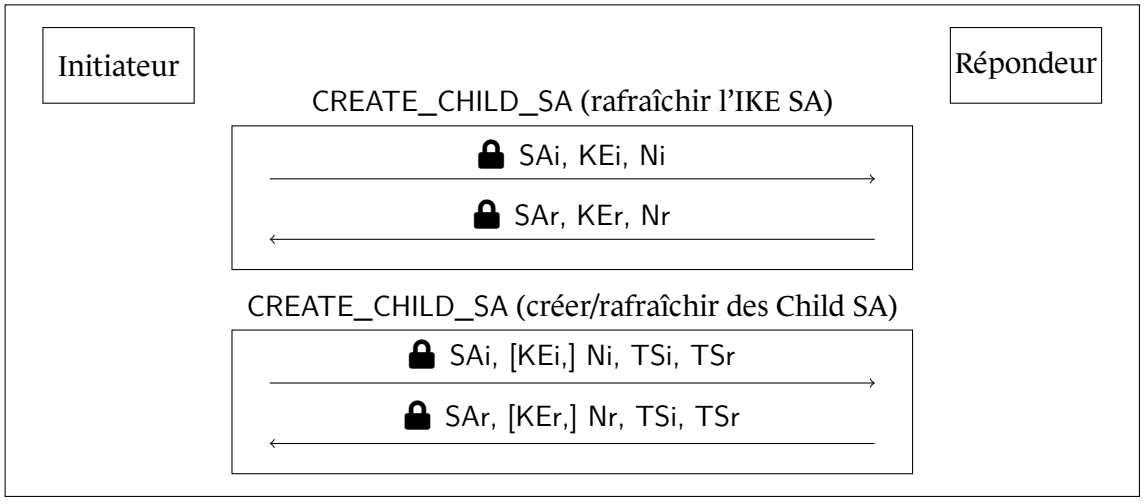
nismes, clés, fenêtre anti-rejeu, etc) sont consultées dans les associations de sécurité correspondantes (Child SA). Le fonctionnement de ce protocole n'est pas impacté par la menace quantique, puisqu'il n'utilise pas de mécanismes asymétriques. Ainsi, le protocole AH ne sera pas traité dans la suite de ce document. Toutefois, la sécurité des clés utilisées dans ce protocole repose sur le protocole IKEv2, pendant lequel la dérivation de clés est calculée.

- Le protocole ESP (*Encapsulating Security Payload*) permet de protéger les paquets IP en intégrité et confidentialité, et assure une protection contre le rejeu de messages. Les données nécessaires à la protection (mécanismes, clés, fenêtre anti-rejeu, etc) sont consultées dans les associations de sécurité correspondantes (Child SA). Le fonctionnement de ce protocole n'est pas impacté par la menace quantique, puisqu'il n'utilise pas de mécanismes asymétriques. Ainsi, le protocole ESP ne sera pas traité dans la suite de ce document. Toutefois, la sécurité des clés utilisées dans ce protocole repose sur le protocole IKEv2, pendant lequel la dérivation de clés est calculée.

## 2.1 Le protocole IKEv2




(a) Échange initial à l'établissement de la session




(b) Échange pour créer ou rafraîchir une paire de Child SA, ou rafraîchir l'IKE SA

FIGURE 2 – Échanges IKEv2 simplifiés

Les échanges du protocole IKEv2 sont rappelés dans la Figure 2. Les messages munis d'un cadenas sont protégés en confidentialité et intégrité. Les champs entre crochets sont optionnels en fonction du contexte. Tous les échanges IKEv2 se passent par paire : une requête et sa réponse.

### 2.1.1 Associations de sécurité

IKEv2 permet d'établir des associations de sécurité. Une association de sécurité (SA) est une structure de données contenant les paramètres de sécurité nécessaires pour protéger un flux de données. Une association de sécurité spécifie notamment les suites cryptographiques et les clés symétriques de chiffrement et d'intégrité, la fenêtre anti-rejeu et la durée de validité. Il existe deux types d'associations de sécurité établies avec IKEv2 :

- l'association de sécurité IKE SA est créée pendant les échanges IKE_SA_INIT, et finalisée après l'authentification mutuelle dans les échanges IKE_AUTH. Cette association est bidirectionnelle et sert à protéger en confidentialité et intégrité tous les échanges du protocole IKEv2 qui ont lieu après les échanges IKE_SA_INIT (notamment IKE_AUTH, CREATE_CHILD_SA et INFORMATIONAL, ces derniers étant utilisés pour des messages de fonctionnement). En d'autres termes, les échanges du protocole IKEv2 peuvent être vus comme des messages d'un tunnel de service IKEv2, et l'association de sécurité IKE SA spécifie les paramètres de sécurité pour protéger les messages de ce tunnel. Cette association de sécurité est différente des associations de sécurité utilisées pour protéger les paquets IP du tunnel IPsec.
- Les associations de sécurité Child SA servent à protéger les paquets IP, soit en intégrité avec AH, soit en intégrité et confidentialité avec ESP. Une association de sécurité Child SA est unidirectionnelle. Les échanges pour créer des associations de sécurité Child SA résultent en une paire d'associations de sécurité, où les clés symétriques sont notamment différentes dans les deux sens des échanges. La première paire d'associations de sécurité Child SA est établie pendant les échanges IKE_AUTH, et d'autres paires peuvent être établies pendant des échanges CREATE_CHILD_SA. IPsec permet de contrôler le niveau de granularité pour la protection des différents paquets IP transitant sur le tunnel IPsec. Par exemple, une seule paire d'associations de sécurité Child SA peut être établie entre l'initiateur et le répondeur pour protéger tous les paquets IP du tunnel IPsec, ou une paire d'associations de sécurité par connexion TCP, etc.

### 2.1.2 Les échanges IKE_SA_INIT et IKE_AUTH

Les deux premiers échanges IKE_SA_INIT et IKE_AUTH (Figure 2a) ont lieu à l'initialisation du canal de communication. Ils servent à effectuer le premier échange de clés entre l'initiateur et le répondeur, ainsi que leur authentification mutuelle. Après ces échanges, l'association de sécurité IKE SA et la première paire d'associations de sécurité Child SA sont établies. Il existe deux moyens d'authentification mutuelle :

- par signature et certificat,
- par clé pré-partagée (symétrique).

Les échanges IKE_SA_INIT se déroulent de la manière suivante :

- dans la requête IKE_SA_INIT, l'initiateur envoie dans le champ SAi1 ses propositions de suites cryptographiques. Il envoie également sa clé publique DH dans KEi et une valeur aléatoire à usage unique dans Ni. Le champ SAi1 contient notamment des propositions pour :

- des mécanismes symétriques de chiffrement, d'intégrité, ou de chiffrement avec de l'intégrité,
- des groupes DH pour l'échange de clés,
- des fonctions pseudo-aléatoires, notamment utilisées pour la dérivation de clés.

- Dans la réponse IKE_SA_INIT, le répondeur envoie sa sélection de suite cryptographique dans SAr1, sa clé publique DH dans KEr et une valeur aléatoire à usage unique dans Nr. Le répondeur peut également demander le certificat de l'initiateur avec le champ CertReq dans le cas d'une authentification par signature.

Après ces échanges, les clés symétriques de chiffrement et d'intégrité pour protéger les échanges IKEv2 sont dérivées à partir du secret partagé DH et des valeurs aléatoires dans les champs Ni et Nr. Néanmoins, les associations de sécurité IKE SA ne sont finalisées qu'à la fin des échanges IKE_AUTH :

- dans la requête IKE_AUTH, l'initiateur envoie sa chaîne d'identification dans IDi et son certificat dans Cert si le répondeur l'avait demandé dans sa réponse IKE_SA_INIT. Il envoie optionnellement une chaîne d'identification dans IDr, indiquant avec quelle identité du répondeur il souhaite communiquer [2]. De plus, l'initiateur envoie le champ CertReq pour demander le certificat du répondeur dans le cas d'une authentification par signature. L'initiateur s'authentifie avec le champ AUTH contenant :
  - une signature si l'initiateur s'authentifie par signature,
  - ou un code d'authentification si l'initiateur s'authentifie par clé pré-partagée. Ce code est calculé à partir de la fonction pseudo-aléatoire (symétrique) de l'association de sécurité IKE SA et d'une clé pré-partagée entre l'initiateur et le répondeur. Ce code d'authentification prouve la possession de la clé pré-partagée par l'initiateur.

  Enfin, l'initiateur peut déclencher l'établissement de la première paire de Child SA à ce niveau, en envoyant des nouvelles propositions de suites cryptographiques dans le champ SAi2. Les champs TSi et TSr permettent de spécifier le trafic à protéger avec les associations Child SA à établir (*e.g.*, adresses IP, ports).

- Dans la réponse IKE_AUTH, le répondeur envoie sa chaîne d'identification dans IDr et son certificat dans Cert si l'initiateur l'avait demandé. Il s'authentifie avec le champ AUTH similairement à l'initiateur. Enfin, il envoie ses sélections pour les champs SAr2, TSi et TSr, pour finaliser l'établissement de la première paire de Child SA.

### Information

Les clés des associations de sécurité Child SA créées pendant les échanges IKE_AUTH sont dérivées à partir des mêmes valeurs que pour l'association de sécurité IKE SA. En d'autres termes, le même secret DH, ainsi que les mêmes valeurs aléatoires dans Ni et Nr sont utilisés. Dans des échanges CREATE_CHILD_SA, les associations de sécurité sont créées avec des nouveaux champs Ni et Nr, et optionnellement un nouveau secret DH. Il existe un autre moyen d'exécuter les échanges IKE_SA_INIT et IKE_AUTH sans générer une paire d'associations de sécurité Child SA, définie dans la RFC 6023 [7].

2. Cette chaîne est utile par exemple lorsque le répondeur est une machine hôte avec plusieurs identités partageant la même adresse IP.

Après ces échanges initiaux, l'association de sécurité IKE SA est établie, ainsi que la première paire d'associations de sécurité Child SA. Tous les échanges ultérieurs IKEv2 (notamment IKE_AUTH, CREATE_CHILD_SA et INFORMATIONAL, ces derniers utilisés pour des messages de fonctionnement) sont ainsi protégés en utilisant l'association de sécurité IKE SA.

### 2.1.3 Les échanges CREATE_CHILD_SA

Les échanges CREATE_CHILD_SA (Figure 2b) servent à rafraîchir l'association de sécurité IKE SA, ou à créer ou rafraîchir une paire d'associations de sécurité Child SA. Ces échanges se déroulent de la manière suivante :

- dans la requête CREATE_CHILD_SA, l'initiateur envoie ses propositions de suites cryptographiques dans le champ SAi. Il envoie également sa nouvelle clé publique DH dans KEi, ainsi qu'une valeur aléatoire à usage unique dans Ni. Dans le cas d'un échange pour créer ou rafraîchir une paire de Child SA, le champ KEi est optionnel, et l'initiateur envoie les champs TSi et TSr.
- Dans la réponse CREATE_CHILD_SA, le répondeur envoie son choix de suite cryptographique dans SAr. Il envoie également sa nouvelle clé publique DH dans KEr, ainsi qu'une valeur aléatoire à usage unique dans Nr. Dans le cas d'un échange pour créer ou rafraîchir une paire de Child SA, le champ KEr est optionnel, et le répondeur envoie ses sélections pour les champs TSi et TSr.

Après ces échanges, les clés symétriques de chiffrement et d'intégrité sont dérivées à partir du secret partagé DH (s'il existe), des valeurs aléatoires dans les champs Ni et Nr et d'une clé symétrique dérivée dans l'association de sécurité IKE SA. Ces clés sont stockées dans les associations de sécurité Child SA correspondantes, et servent à protéger le trafic utile de paquets IP en confidentialité et en intégrité, en fonction du protocole choisi (AH ou ESP).

# 3
# Transition post-quantique d'IPsec

Comme mentionné précédemment, le protocole IKEv2 met en œuvre des mécanismes asymétriques pour les échanges de clés et l'authentification par signature. Ces derniers sont vulnérables à la menace quantique. La transition post-quantique d'IKEv2 peut être réalisée en utilisant des clés pré-partagées (*c.f.*, Section 3.1), ou en utilisant une méthode d'hybridation (*c.f.*, Section 3.2) qui est la solution privilégiée par l'ANSSI [1, 2]. Notons que la transition post-quantique pour la confidentialité des échanges est plus urgente que celle pour l'authentification, notamment à cause des attaques *"store-now decrypt-later"*.

## 3.1 Sécurité post-quantique par clé pré-partagée

Comme précisé dans l'avis sur la transition post-quantique de l'ANSSI [1, 2], une clé pré-partagée peut être utilisée dans le cadre de la transition post-quantique, notamment si la confidentialité et l'intégrité (classiques et post-quantiques) de la clé pré-partagée sont assurées. De plus, une attention particulière doit être portée à la gestion et la distribution de clés pré-partagées. Enfin, la mise en œuvre de clé pré-partagée peut être une mesure temporaire dans la transition post-quantique. La mise en œuvre de l'hybridation et l'utilisation de mécanismes post-quantiques pour assurer une sécurité post-quantique devront être effectuées à terme.

**Authentification post-quantique par clé pré-partagée.** Comme présenté dans la Section 2.1, le protocole IKEv2 propose l'authentification par clé pré-partagée en calculant les champs AUTH (Figure 2) comme des codes d'authentification symétriques. Ainsi, l'utilisation de cette solution est possible dans IKEv2 pour assurer une authentification post-quantique de l'initiateur et du répondeur.

**Confidentialité post-quantique par clé pré-partagée.** Le protocole IKEv2 ne propose pas par défaut l'utilisation d'une clé pré-partagée dans la dérivation des clés symétriques. En 2020, une extension du protocole a été publiée dans la RFC 8784 [5]. Cette extension permet d'utiliser une clé pré-partagée dans la dérivation des clés symétriques, en combinaison avec l'échange de clés basé sur le schéma DH. Cette clé est différente de la clé pré-partagée utilisée pour l'authentification. Néanmoins, cette solution présente une limitation de sécurité.

### Attention

La solution proposée dans la RFC 8784 [5] présente une limitation. En effet, la clé pré-partagée n'est utilisée que dans la dérivation des clés permettant de protéger le trafic des paquets IP avec les futures associations de sécurité (Child SA). En d'autres termes, le trafic des échanges IKEv2 n'est pas protégé avec des clés dérivées en utilisant cette clé pré-partagée, mais uniquement avec la clé partagée issue de l'échange basé sur le

schéma DH.

En 2025, la RFC 9867 [16] a été publiée. Ce document propose une solution qui étend l'utilisation de la clé pré-partagée pour dériver aussi les clés qui protègent les échanges IKEv2. Cette solution négocie des clés pré-partagées en utilisant des échanges intermédiaires [15] entre IKE_SA_INIT et IKE_AUTH. La RFC 9867 propose également une manière de négocier d'autres clés pré-partagées dans les échanges CREATE_CHILD_SA.

### Attention

La compromission de la clé pré-partagée est rétroactive, elle implique la compromission de toutes les sessions IKEv2 où elle a été utilisée. Ceci a des conséquences sur la propriété de la confidentialié persistante des échanges IKEv2 chiffrés (ou *Perfert Forward Secrecy* (PFS)). La propriété PFS signifie que la compromission des clés d'une session ne doit pas compromettre des clés de sessions passées. Par exemple, si la dérivation des clés de chaque session utilise une même clé pré-partagée et un nouveau secret DH, la compromission de la clé pré-partagée signifie qu'un attaquant quantique pourra réaliser l'attaque *"store-now decrypt-later"* sur toutes les sessions établies utilisant cette clé, puisque les secrets DH peuvent être compromis avec un ordinateur quantique. Dans ce cas, la propriété PFS est assurée en classique avec le secret DH, mais pas en post-quantique.

**Implémentations.** StrongSwan implémente l'authentification par clé pré-partagée dans IKEv2. De plus, StrongSwan implémente depuis la version 5.7.0, la solution proposée dans la RFC 8784 [5].

## 3.2 Sécurité post-quantique par hybridation

L'hybridation du protocole IKEv2 implique la modification des messages échangés. D'une part, les échanges de clés basés sur le schéma DH sont effectués dans les échanges IKE_SA_INIT et CREATE_CHILD_SA. D'autre part, l'authentification par signature de l'initiateur et du répondeur est effectuée dans les échanges IKE_AUTH.

### 3.2.1 Hybridation des échanges de clés

Les échanges de clés ont lieu dans les échanges IKE_SA_INIT et CREATE_CHILD_SA. L'hybridation consiste à exécuter deux échanges de clés : un échange de clés avec un mécanisme classique (par exemple le schéma DH) et un échange de clés avec un mécanisme post-quantique (par exemple ML-KEM [13]). Ensuite, les deux secrets partagés sont combinés pour dériver le secret final ayant une sécurité classique et post-quantique.

### Attention

Le mécanisme de combinaison des secrets partagés issus des deux échanges de clés (classique et post-quantique) pour dériver le secret partagé final doit assurer une sécurité classique et post-quantique. Des manières de combiner les deux secrets sont citées dans l'avis sur la transition post-quantique de l'ANSSI [1, 2].

L'hybridation des échanges de clés dans IKEv2 implique les champs suivants :

- SAi1 et SAr1 dans IKE_SA_INIT, dédiés notamment à la négociation du groupe DH pour l'association de sécurité IKE SA,
- KEi et KEr dans IKE_SA_INIT, dédiés à l'échange de clés basé sur le schéma DH pour l'association de sécurité IKE SA,
- SAi et SAr dans CREATE_CHILD_SA, dédiés notamment à la négociation du groupe DH, optionnel dans le cas des associations de sécurité Child SA.
- KEi et KEr dans CREATE_CHILD_SA, dédiés à l'échange de clés basé sur le schéma DH, optionnel dans le cas des associations de sécurité Child SA.

Dans le cas d'un échange de clés hybride, les champs SAi1, SAr1, SAi et SAr présentent des noms de mécanismes pour des échanges de clés hybrides (groupe Diffie-Hellman et KEM post-quantique). Néanmoins, les champs KEi et KEr ne peuvent pas être utilisés pour effectuer l'échange de clés hybride sans modification du protocole. En effet, l'initiateur doit envoyer sa clé publique DH et sa clé publique du KEM post-quantique, suivi du répondeur qui doit envoyer sa clé publique DH et le chiffré résultant de l'encapsulation sur la clé publique du KEM post-quantique de l'initiateur. Ces données ne peuvent pas être envoyées dans les champs KEi et KEr à cause de la gestion de la fragmentation dans le protocole IKEv2, et des tailles importantes des clés publiques et des chiffrés des KEM post-quantiques existants.

**Fragmentation des données dans IKEv2.** Une conséquence inévitable de la transition post-quantique est l'augmentation de la taille des messages échangés pour l'échange de clés et l'authentification par signature, à cause des tailles des clés, des signatures et des chiffrés plus grandes des mécanismes post-quantiques. Les messages seront ainsi fragmentés par le protocole IP, si le protocole de communication ne gère pas la fragmentation des messages. Une description détaillée de ce problème est donnée en Annexe A. Le protocole IKEv2 fonctionne au-dessus du protocole de transport UDP, qui n'assure pas la fiabilité et la réception des paquets comme TCP. De plus, IKEv2 ne supporte pas nativement la fragmentation de ses messages. Ceci pose un problème pour l'utilisation des mécanismes post-quantiques avec des tailles de clés et de chiffrés conséquentes. En 2014, la RFC 7383 [14] a été publiée, proposant un mécanisme de gestion de la fragmentation, pour que la bonne réception des fragments soit contrôlée au niveau protocolaire d'IKEv2. Ce mécanisme permet de fragmenter tous les messages IKEv2 chiffrés. Ceci inclut tous les messages, à l'exception des premiers échanges IKE_SA_INIT (*c.f.*, Figure 2). Le mécanisme proposé a été motivé par les échanges de certificats et chaînes de certification, pouvant avoir des tailles conséquentes.

Pour permettre des échanges de clés hybrides dès les premiers échanges IKE_SA_INIT, la RFC 9370 [17] a été publiée en 2023, permettant d'effectuer plusieurs échanges de clés successifs dans IKEv2 (par exemple, un échange de clés basé sur le schéma DH puis un échange de clés avec un KEM post-quantique). Une description de la proposition dans le cas des échanges initiaux IKEv2 est présentée dans la Figure 3.

Dans la solution proposée, les premiers messages IKE_SA_INIT servent toujours à négocier les suites cryptographiques (incluant les différents mécanismes d'échanges de clés), et échanger des clés publiques DH. Ensuite, des messages intermédiaires IKE_INTERMEDIATE [15] sont utilisés pour effectuer le reste des échanges de clés négociés. Ces messages IKE_INTERMEDIATE sont donc chiffrés et le traitement de leur fragmentation est automatiquement pris en compte grâce au mécanisme dans [14]. Notons que cette technique permet d'effectuer plusieurs échanges de

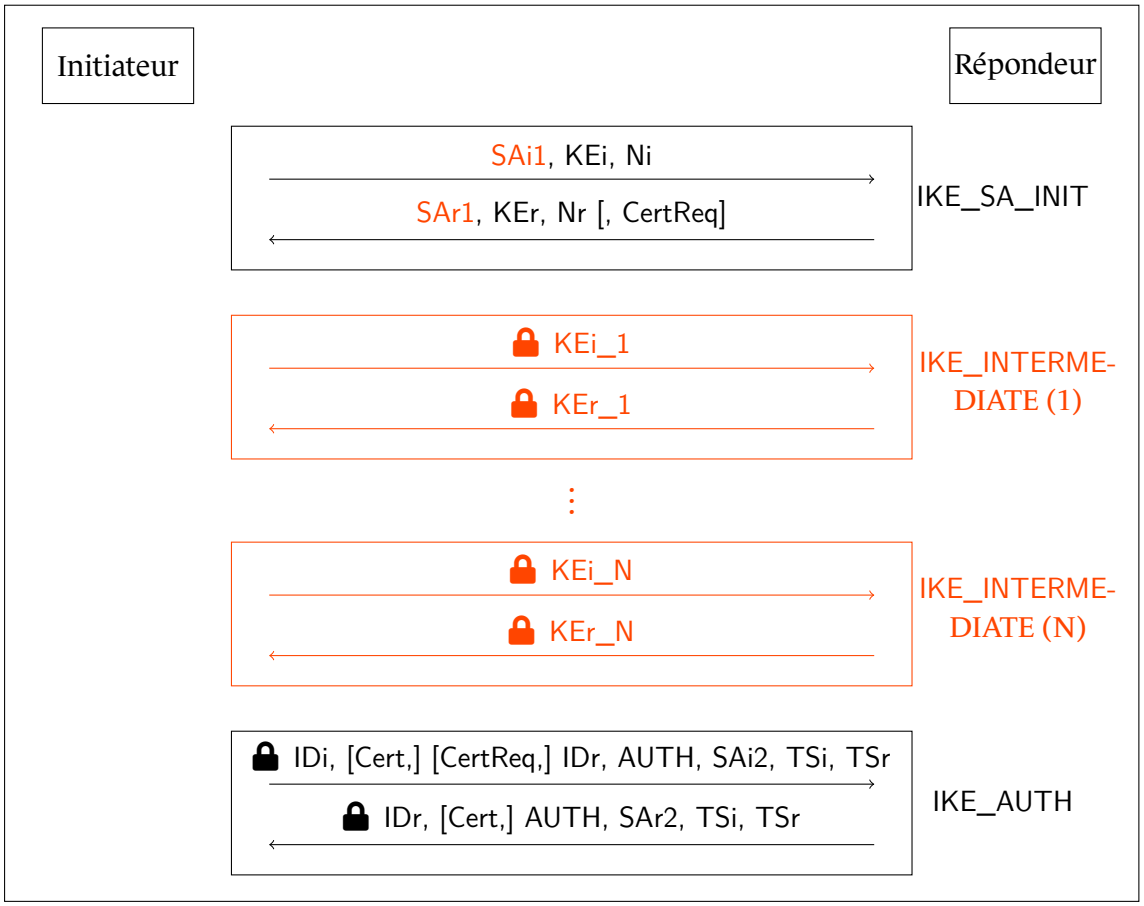



FIGURE 3 – Échanges initiaux IKEv2 avec $N + 1$ échanges de clés tel que proposé dans [17]

clés différents, classiques et post-quantiques. Pour un échange de clés hybride, un seul échange IKE_INTERMEDIATE est nécessaire. L'initiateur envoie sa clé publique du KEM post-quantique, et le répondeur envoie le chiffré résultant de l'encapsulation sur cette clé. Enfin, la RFC 9370 [17] propose une façon de combiner les différents secrets partagés successivement dans les secrets partagés finaux. La RFC 9370 [17] propose également des échanges similaires dans le cas de l'échange de clés dans CREATE_CHILD_SA, avec des messages intermédiaires IKE_FOLLOWUP_KE. Remarquons que les échanges CREATE_CHILD_SA sont chiffrés de base. La solution permet en particulier de généraliser l'échange de clés hybride à plusieurs mécanismes.

**Documents.** Un draft internet [8] applique la solution proposée dans la RFC 9370 [17] en utilisant le KEM post-quantique ML-KEM [13] pour des échanges de clés hybrides dans IKEv2.

**Implémentations.** strongSwan implémente la gestion de la fragmentation proposée dans [14]. De plus, strongSwan implémente dans sa version 6.0 [3] l'échange de clés hybride tel que défini dans [17] et intègre également ML-KEM [13].

### 3.2.2 Hybridation de l'authentification par signature

L'hybridation de l'authentification par signature nécessite l'hybridation des signatures et des certificats utilisés dans IKEv2. Il existe différents formats pour hybrider les certificats (authentifiant

3. https://github.com/strongswan/strongswan/releases

les clés de signature classique et post-quantique), par exemple avec deux certificats distincts (un pour la clé de signature classique, et un autre pour la clé de signature post-quantique), ou un seul certificat authentifiant la concaténation des clés de signature, etc. L'hybridation concerne aussi les chaînes de certification. Pour l'instant, il n'existe pas de standards pour l'authentification hybride.

L'authentification par signature dans IKEv2 se passe dans les échanges IKE_AUTH. Dans le cas d'une authentification par signature hybride, les champs AUTH contiennent des signatures hybrides (composées d'une signature classique et d'une signature post-quantique). De la même manière, les champs Cert contiennent des certificats hybrides.

**Fragmentation des données dans IKEv2.** Le mécanisme de gestion de la fragmentation proposée dans [14] (*c.f.*, Section 3.2.1) permet d'échanger des certificats et des signatures hybrides. En effet, ces données sont envoyées dans des messages IKEv2 chiffrés, pris en charge par [14]. Ainsi, l'hybridation de l'authentification par signature dans IKEv2 nécessite principalement l'implémentation du mécanisme de gestion de la fragmentation proposée dans [14].

Enfin, il n'existe pas pour l'instant de standards permettant l'intégration de l'authentification par signature hybride dans IKEv2.

# 4
# Conclusion

La transition post-quantique du protocole IPsec concerne le protocole IKEv2, où l'initiateur et le répondeur négocient les suites cryptographiques, effectuent des échanges de clés basés sur le schéma DH et s'authentifient mutuellement. L'ANSSI recommande d'utiliser l'hybridation pour les échanges de clés et l'authentification par signature. Le protocole IKEv2 propose l'utilisation d'une clé pré-partagée pour assurer l'authentification mutuelle entre l'initiateur et le répondeur. En 2020, la RFC 8784 [5] a été publiée, permettant d'utiliser une clé pré-partagée pour assurer une confidentialité post-quantique, différente de la clé pré-partagée pour l'authentification. Cette solution permet de protéger le trafic des paquets IP en confidentialité post-quantique, mais ne permet pas de protéger les échanges IKEv2. En 2025, la RFC 9867 [16] a été publiée notamment pour corriger ce problème. La mise en œuvre des clés pré-partagées pour assurer une confidentialité et une authentification résistantes à la menace quantique peut être envisageable mais temporaire, l'hybridation doit être implémentée à terme. strongSwan implémente l'authentification par clé pré-partagée dans IKEv2, ainsi que la solution de la RFC 8784 [5] depuis la version 5.7.0.

L'hybridation des échanges de clés dans le protocole IKEv2 nécessite un échange de clés basé sur un KEM post-quantique, en plus de l'échange de clés basé sur le schéma DH. Les échanges de clés ont lieu dans les échanges IKE_SA_INIT pour l'établissement de l'association de sécurité IKE SA, ainsi que dans les échanges CREATE_CHILD_SA pour le rafraîchissement de l'association de sécurité IKE SA, ou l'établissement et le rafraîchissement d'une paire d'associations de sécurité Child SA. La RFC 9370 [17] permet d'effectuer plusieurs échanges de clés successifs dans IKE_SA_INIT et CREATE_CHILD_SA, donnant la possibilité de réaliser des échanges de clés hybrides. La solution est basée sur un format de messages défini dans [15] et une nouvelle gestion de la fragmentation des messages dans IKEv2 définie dans [14]. Un draft internet [8] applique la solution proposée dans la RFC 9370 [17] en utilisant le KEM post-quantique ML-KEM [13]. Enfin, la version 6.0[4] de strongSwan implémente l'échange de clés hybride tel que défini dans [17] (avec les mécanismes nécessaires [14, 15]) et intègre ML-KEM [13].

L'hybridation de l'authentification par signature dans le protocole IKEv2 nécessite l'hybridation des certificats utilisés pour authentifier l'initiateur et le répondeur, ainsi que l'hybridation des signatures envoyées dans les messages d'authentification. L'hybridation de l'authentification nécessite plus de travaux. La taille de ces données envoyées dans les échanges IKE_AUTH est gérée par le mécanisme de la fragmentation des messages défini dans [14]. Il n'existe pas pour l'instant de standards officiels permettant l'authentification par signature et certificat hybrides dans IKEv2.

La transition post-quantique du protocole IPsec étant un sujet très étudié, il est nécessaire de suivre l'évolution des travaux et des implémentations.

4. https://github.com/strongswan/strongswan/releases

# Annexe A
# Fragmentation des données

Les données applicatives transitent sur les différentes couches du réseau avant d'arriver à destination, comme présenté dans la Figure 4. Une donnée envoyée d'une application est encapsulée dans un segment de transport grâce à un protocole de transport comme TCP ou UDP. Ce segment est ensuite encapsulé dans un paquet IP permettant de transiter sur internet. Ce paquet est enfin encapsulé dans une trame réseau grâce au protocole Ethernet afin de circuler sur les réseaux physiques. Ensuite, une trame reçue sur la carte réseau physique est décapsulée par les couches successives jusqu'à pouvoir lire la donnée applicative associée.

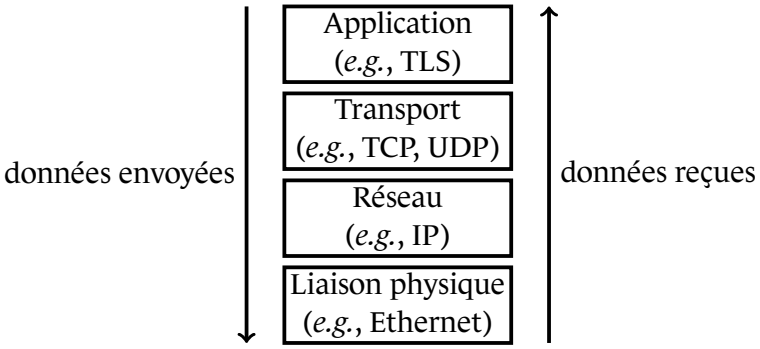



FIGURE 4 – Modèle réseau TCP/IP simplifié

Un paquet IP doit respecter une taille maximale de paquet appelée unité de transmission maximale (MTU) configurée pour chaque interface réseau.

### Information

Pour IPv6, la MTU minimale à implémenter est égale à 1280 octets. En pratique, il existe des implémentations qui fixent la MTU à une taille supérieure (*e.g.*, 1500 octets).

Un paquet IP qui dépasse cette limite sera fragmenté par le protocole IP en plusieurs paquets. La fragmentation au niveau IP peut présenter certains problèmes. Par exemple, certains pare-feux décident de rejeter les paquets IP fragmentés pour éviter des attaques comme celles par déni de service (*e.g.*, [3, 4, 6]). Ceci empêche la bonne transmission des messages. De ce fait, de nombreux protocoles évitent de dépendre de la fragmentation IP. Les solutions suivantes sont envisageables :

- le protocole s'assure de générer des messages dont la taille ne dépasse pas la MTU.
- Le protocole repose sur un protocole de transport fiable, qui prend en charge la segmentation et le réassemblage des données comme TCP.

- Le protocole prend en charge lui-même la fragmentation au niveau applicatif.

Les clés, les chiffrés et les signatures des mécanismes post-quantiques augmentent considérablement la taille des messages échangés pendant les phases d'échange de clés et d'authentification par signature. Ainsi, la fragmentation des paquets envoyés avec ces données devient inévitable. Par conséquent, la complexité de la transition post-quantique d'un protocole de communication dépend de la conception de ce dernier.

### Exemple

Un protocole de communication sécurisé s'assure de générer des petits messages pendant le *handshake*. Le protocole fonctionne sur UDP pour des raisons d'efficacité. Dans ce cas, la transition post-quantique impliquera des modifications conséquentes du protocole pour gérer les nouvelles tailles des messages du *handshake*. Ceci nécessitera une étude plus approfondie du protocole modifié et de son implémentation.

# Bibliographie


[1] ANSSI. Avis de l'anssi sur la migration vers la cryptographie post-quantique. https://cyber.gouv.fr/publications/avis-de-lanssi-sur-la-migration-vers-la-cryptographie-post-quantique.

[2] ANSSI. Avis de l'anssi sur la migration vers la cryptographie post-quantique. https://cyber.gouv.fr/publications/avis-de-lanssi-sur-la-migration-vers-la-cryptographie-post-quantique-0.

[3] Antonios Atlasis. Attacking ipv6 implementation using fragmentation. *Blackhat europe*, pages 14–16, 2012.

[4] Jeffrey Bosma, Benno Overeinder, and Willem Toorop. Discovering path mtu black holes on the internet using ripe atlas, 2012.

[5] Scott Fluhrer, Panos Kampanakis, David McGrew, and Valery Smyslov. Mixing Preshared Keys in the Internet Key Exchange Protocol Version 2 (IKEv2) for Post-quantum Security. RFC 8784, June 2020.

[6] Justin Iurman and Benoit Donnet. The razor's edge : Ipv6 extension headers survivability. In *International Conference on Passive and Active Network Measurement*, pages 3–29. Springer, 2025.

[7] Rajeshwar Jenwar, DENG Hui, Hannes Tschofenig, and Yoav Nir. A Childless Initiation of the Internet Key Exchange Version 2 (IKEv2) Security Association (SA). RFC 6023, October 2010.

[8] Panos Kampanakis. Post-quantum Hybrid Key Exchange with ML-KEM in the Internet Key Exchange Protocol Version 2 (IKEv2). Internet-Draft draft-ietf-ipsecme-ikev2-mlkem-03, Internet Engineering Task Force, September 2025. Work in Progress.

[9] Charlie Kaufman, Paul Hoffman, Yoav Nir, Parsi Eronen, and T Kivinen. Rfc 7296 : Internet key exchange protocol version 2 (ikev2), 2014.

[10] Stephen Kent. Rfc 4302 : Ip authentication header, 2005.

[11] Stephen Kent. Rfc 4303 : Ip encapsulating security payload (esp), 2005.

[12] Stephen Kent and Karen Seo. Rfc 4301 : Security architecture for the internet protocol, 2005.

[13] NIST. Module-lattice-based key-encapsulation mechanism standard. https://csrc.nist.gov/pubs/fips/203/final.

[14] Valery Smyslov. Internet Key Exchange Protocol Version 2 (IKEv2) Message Fragmentation. RFC 7383, November 2014.

[15] Valery Smyslov. Intermediate Exchange in the Internet Key Exchange Protocol Version 2 (IKEv2). RFC 9242, May 2022.

[16] Valery Smyslov. Mixing Preshared Keys in the IKE_INTERMEDIATE and CREATE_CHILD_SA Exchanges of the Internet Key Exchange Protocol Version 2 (IKEv2) for Post-Quantum Security. RFC 9867, November 2025.

[17] C. Tjhai, M. Tomlinson, G. Bartlett, Scott Fluhrer, Daniel Van Geest, Oscar Garcia-Morchon, and Valery Smyslov. Multiple Key Exchanges in the Internet Key Exchange Protocol Version 2 (IKEv2). RFC 9370, May 2023.

Version 1.0 - 02/02/2026 - ANSSI-FT-117


**AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION**

ANSSI - 51 boulevard de La Tour-Maubourg 75000 PARIS 07 SP

cyber.gouv.fr / conseil.technique@ssi.gouv.fr

RÉPUBLIQUE FRANÇAISE

*Liberté*
*Égalité*
*Fraternité*