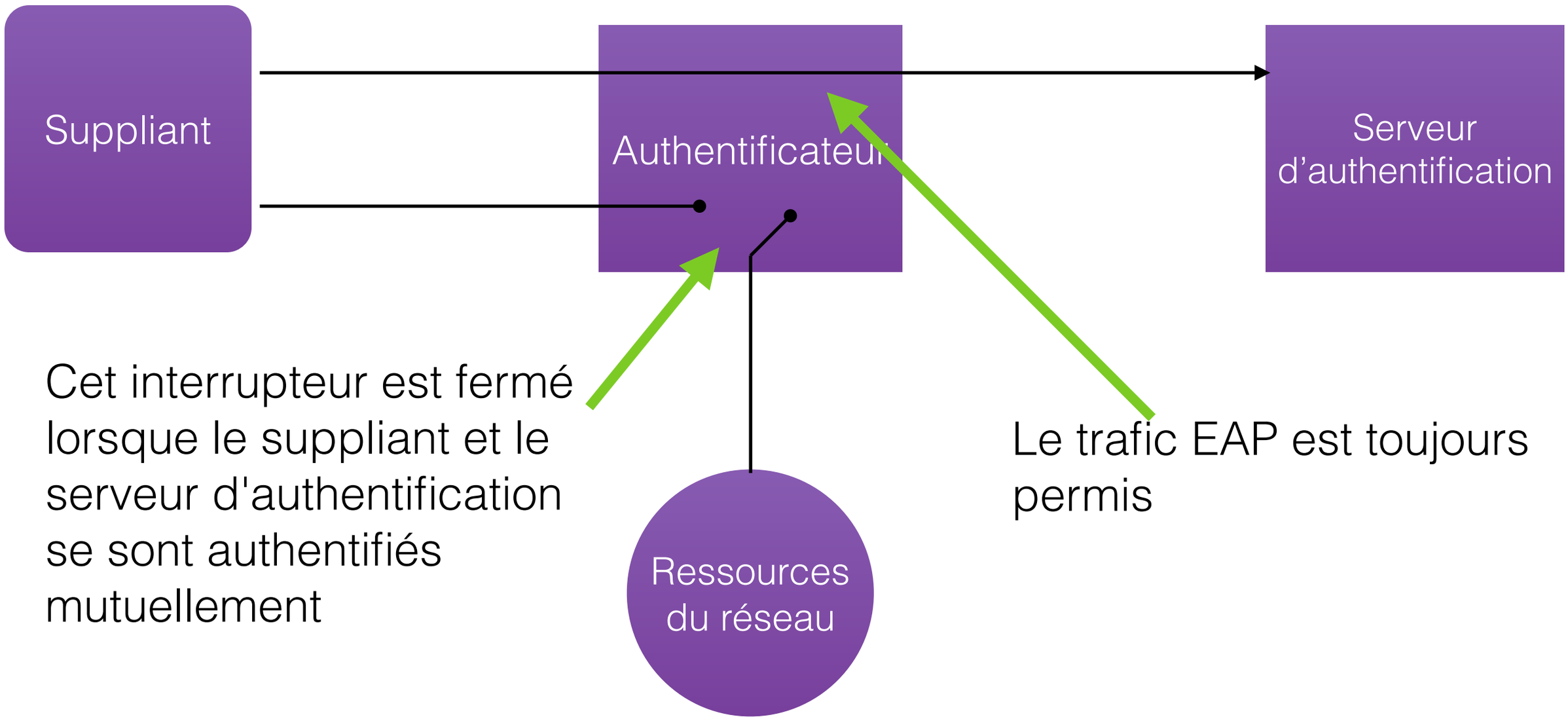
EAP-TLS

Marcos Rubinstein
Abraham Rubinstein

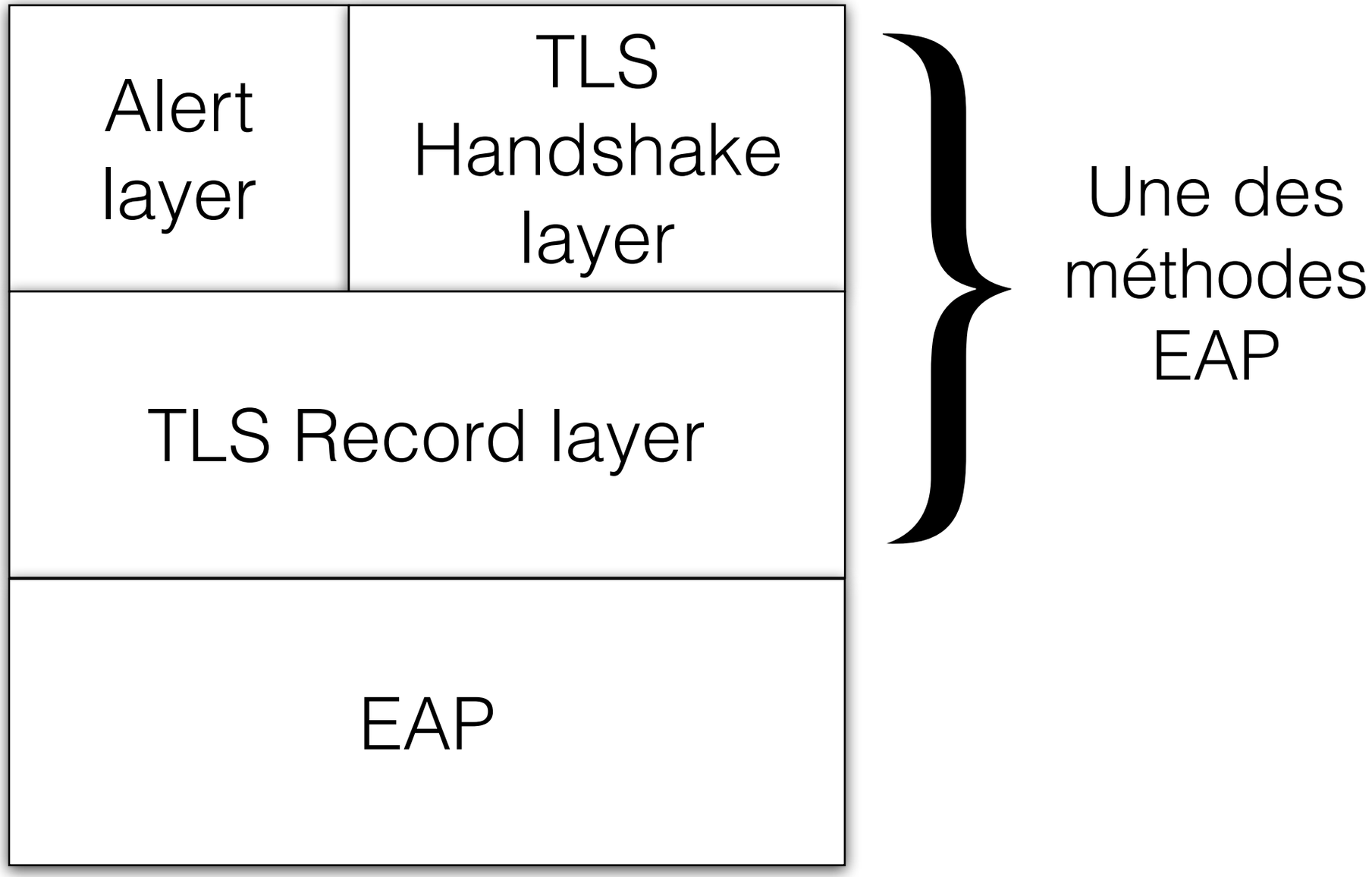
Basé sur RFC4366 and RFC5246

Protocole 802.1X pour accès basé sur ports

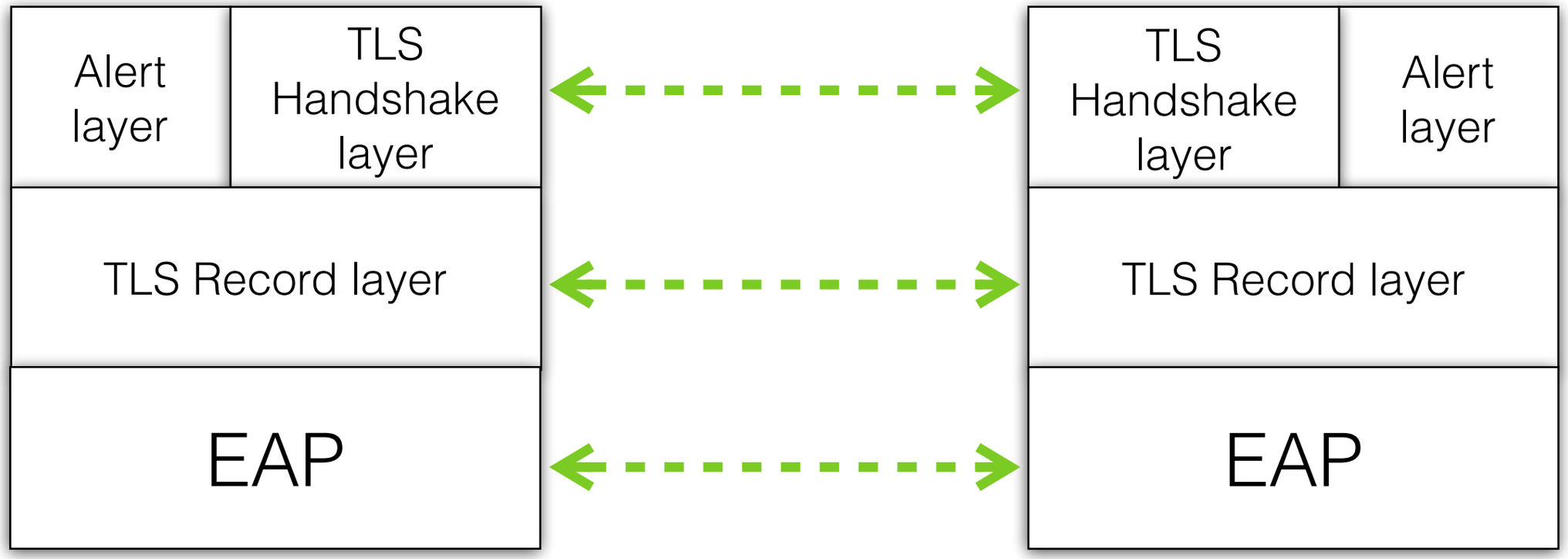
Contient également EAP



L’architecture des couches EAP-TLS

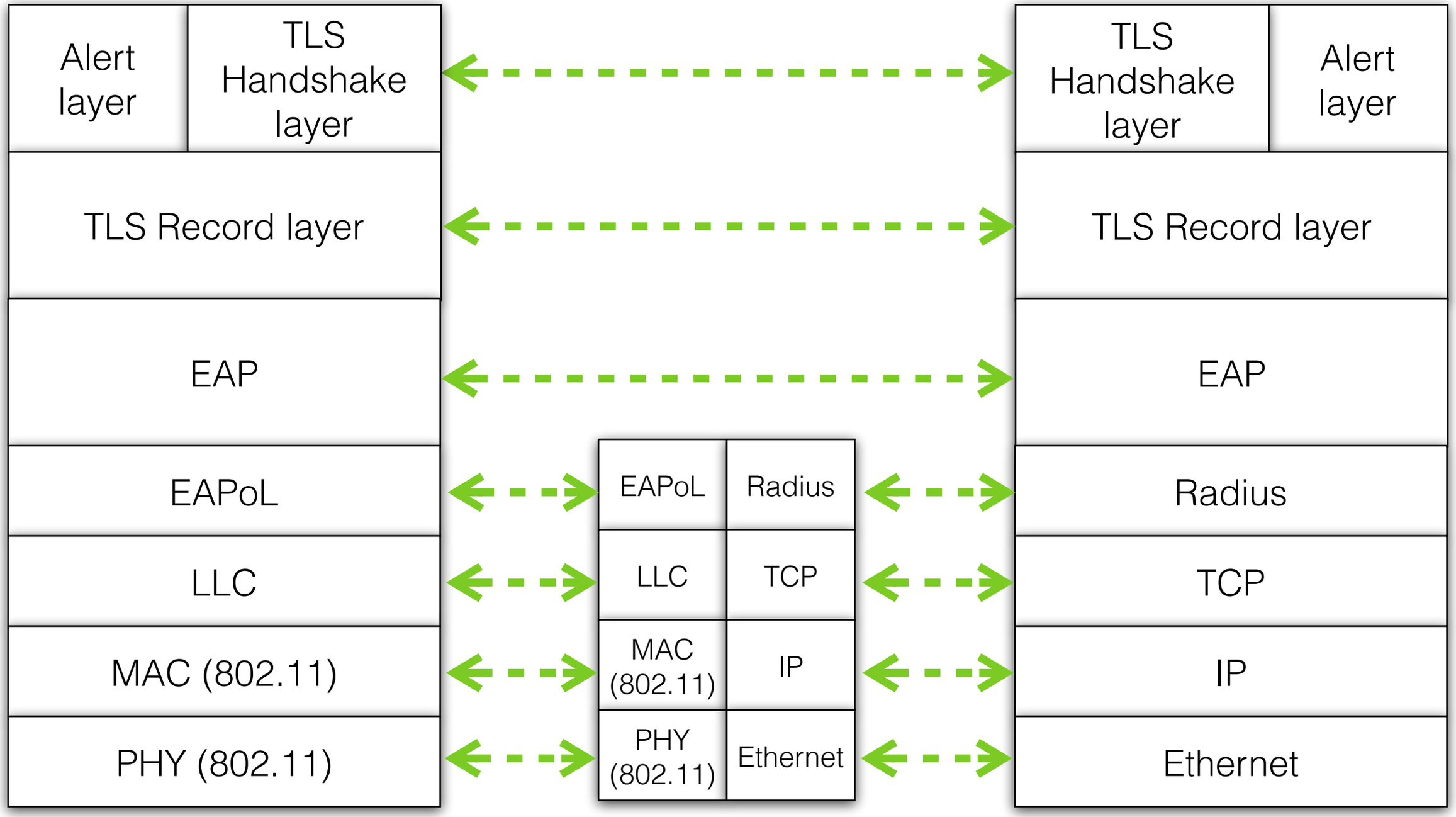


Les couches EAP-TLS



Entre le suppliant et le serveur d'authentification, il y a l'AP qui joue le rôle de l'authentificateur

Les couches EAP-TLS



Phases EAP-TLS

1.Initiation

2.Phase Hello

- échange de Nonces (ClientHello.random et ServerHello.random),
- accord sur les algorithmes
- contrôler s'il s'agit d'une nouvelle session

3.Phase d'échange de certificats

- transmission des certificats
- transmission du Pré Master Secret

4.Génération du Master Secret à partir du Pre Master Secret et des nombres aléatoires (les Nonces) et de la clé de session à partir du Master Secret et des deux nombres aléatoires

5.Phase de confirmation de conformité et de fin de l'authentification

6. Phase de transmission des clés du serveur d'authentification vers l'Authentificateur

Phases EAP-TLS

1.Initiation

2.Phase Hello

- échange de Nonces (ClientHello.random et ServerHello.random),
- accord sur les algorithmes
- contrôler s'il s'agit d'une nouvelle session

3.Phase d'échange de certificats

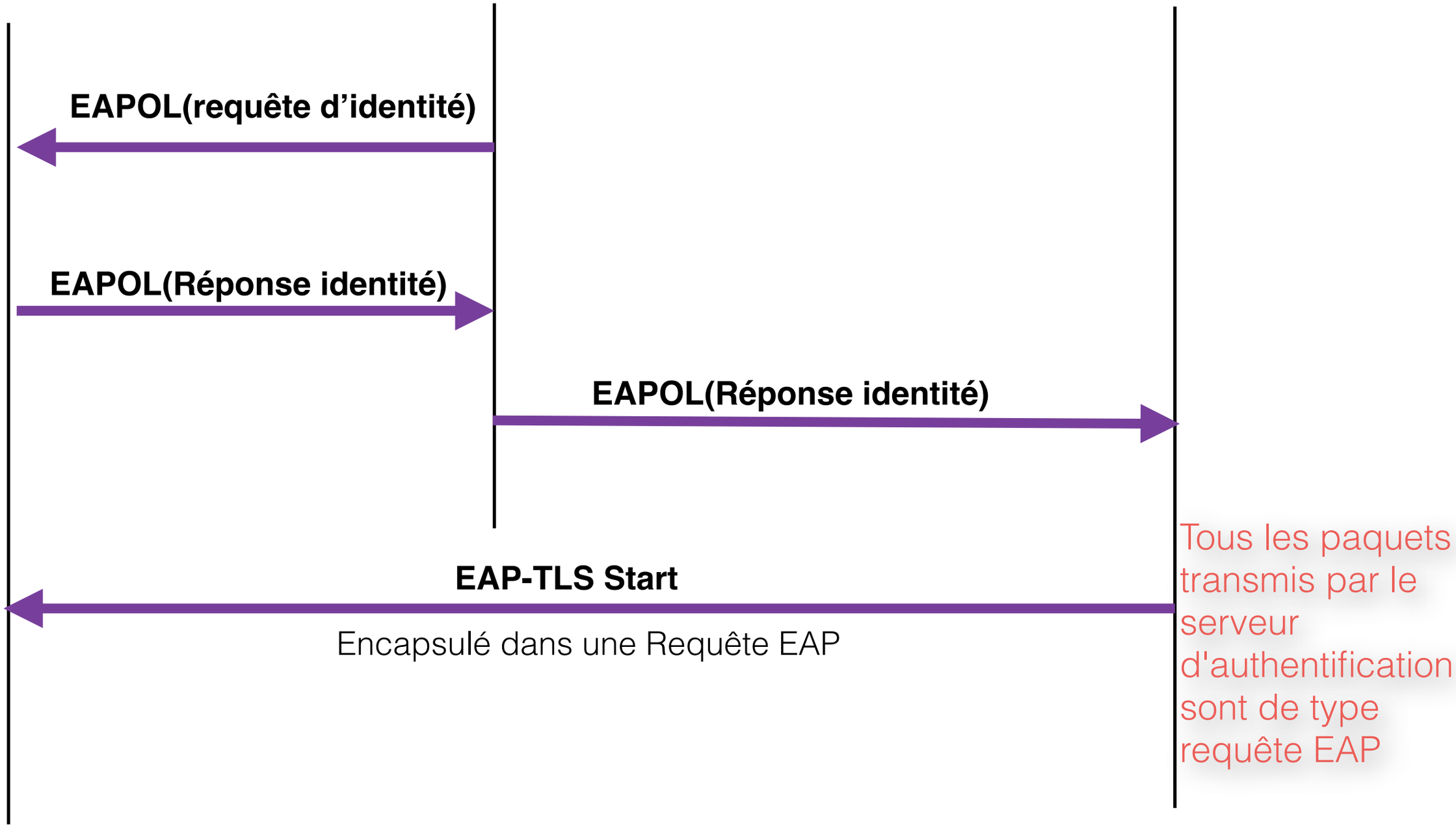
- transmission des certificats
- transmission du Pré Master Secret

4.Génération du Master Secret à partir du Pre Master Secret et des nombres aléatoires (les Nonces) et de la clé de session à partir du Master Secret et des deux nombres aléatoires

5.Phase de confirmation de conformité et de fin de l'authentification

6. Phase de transmission des clés du serveur d'authentification vers l'Authentificateur

Phase d'initiation



Phases EAP-TLS

1.Initiation

2.Phase Hello

- **échange de Nonces (ClientHello.random et ServerHello.random),**
- **accord sur les algorithmes**
- **contrôler s'il s'agit d'une nouvelle session**

3.Phase d'échange de certificats

- transmission des certificats
- transmission du Pré Master Secret

4.Génération du Master Secret à partir du Pre Master Secret et des nombres aléatoires (les Nonces) et de la clé de session à partir du Master Secret et des deux nombres aléatoires

5.Phase de confirmation de conformité et de fin de l'authentification

6. Phase de transmission des clés du serveur d'authentification vers l'Authentificateur

Phase Hello et échange de Nonces

Tous les paquets transmis par le suppliant sont de type réponse EAP

Client Hello

Contient un chiffre aléatoire (ClientHello.random)

Contient la version de TLS

Contient une liste des suites cryptographiques supportées

Contient une liste de méthodes de compression

Contient un identifiant de la session

Server Hello

Contient un chiffre aléatoire (ServerHello.random)

Contient la version de TLS

Contient la suite cryptographique choisie par le serveur

Contient la méthode de compression choisie

Contient un identifiant de la session

Suppliant

Serveur d’authentification

Les nombres aléatoires

- Formés par la concaténation du temps en secondes depuis le premier janvier 1970 (4 octets) et 28 octets aléatoires.

- Il y a encore une centaines d'années de marge avec 4 octets

Les suites cryptographiques

1. Se réfèrent au tunnel

2. Contiennent

- Algorithme pour l'échange de clés
- Algorithme pour chiffrement y compris la longueur de la clé
- Algorithme pour l'intégrité (Message Authentication Code MAC)

Phases EAP-TLS

1.Initiation

2.Phase Hello

- échange de Nonces (ClientHello.random et ServerHello.random),
- accord sur les algorithmes
- contrôler s'il s'agit d'une nouvelle session

3.Phase d'échange de certificats

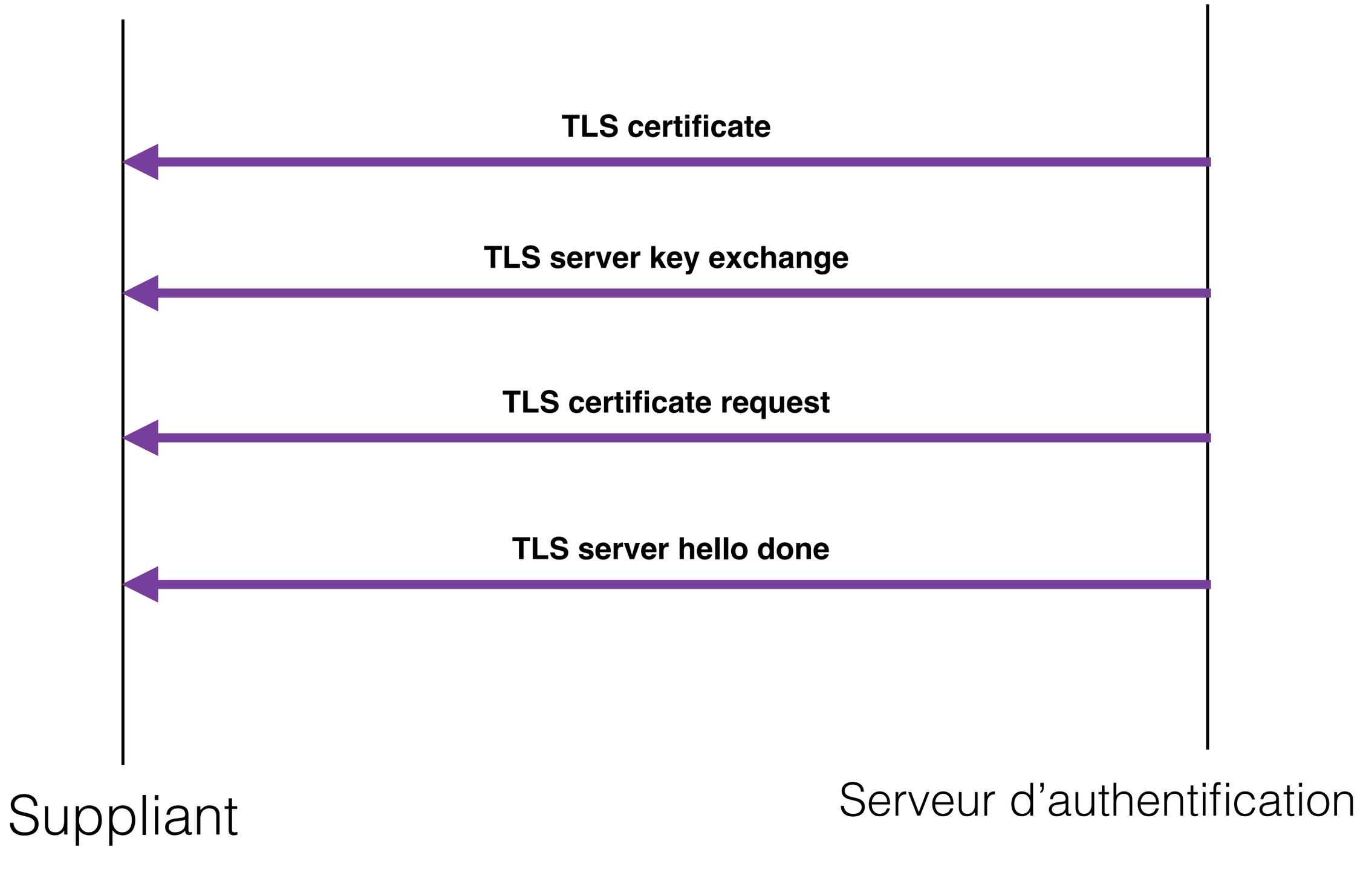
- **transmission des certificats**
- **transmission du Pré Master Secret**

4.Génération du Master Secret à partir du Pre Master Secret et des nombres aléatoires (les Nonces) et de la clé de session à partir du Master Secret et des deux nombres aléatoires

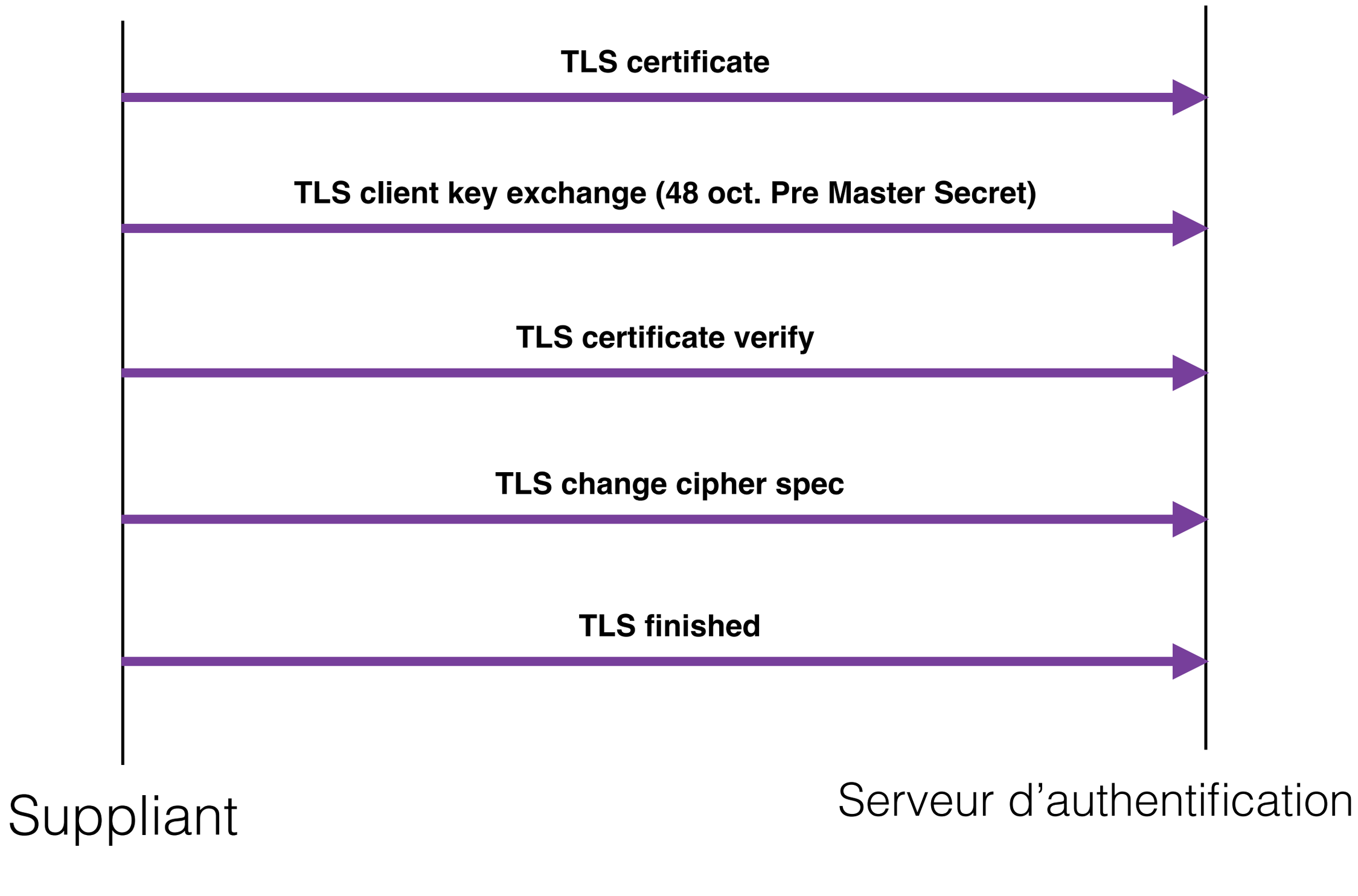
5.Phase de confirmation de conformité et de fin de l'authentification

6. Phase de transmission des clés du serveur d'authentification vers l'Authentificateur

Phase d’échange de certificats et transmission du Pré Master Secret



Phase d'échange de certificats et transmission du Pré Master Secret



TLS client key exchange

- Contient le Pre Master Secret
- Sélectionné par le suppliant
- Chiffré avec la clé publique du serveur d'authentification
- La longueur du Pre Master Secret est 48 octets

TLS certificate verify

- Utilisé pour authentifier de manière explicite le certificat du client
- Contient un hash de la concaténation de tous les messages de Handshake depuis le "client hello" et jusqu'au message qui précède le certificate verify
- Le hash est chiffré avec la clé privé du suppliant.
- Si le serveur d'authentification arrive au même hash en utilisant la clé publique du suppliant, le serveur d'authentification peut être sûr que le client est effectivement en possession de la clé privé du certificat du client

TLS change cipher spec

- Un message
- Indique qu'à partir de ce message, tout sera chiffré et compressé avec les nouvelles clés et algorithmes qui viennent d'être négociés
- Chiffré et compressé avec les clés et algorithmes actuels (pas ceux négociés)

Phases EAP-TLS

1.Initiation

2.Phase Hello

- échange de Nonces (ClientHello.random et ServerHello.random),
- accord sur les algorithmes
- contrôler s'il s'agit d'une nouvelle session

3.Phase d'échange de certificats

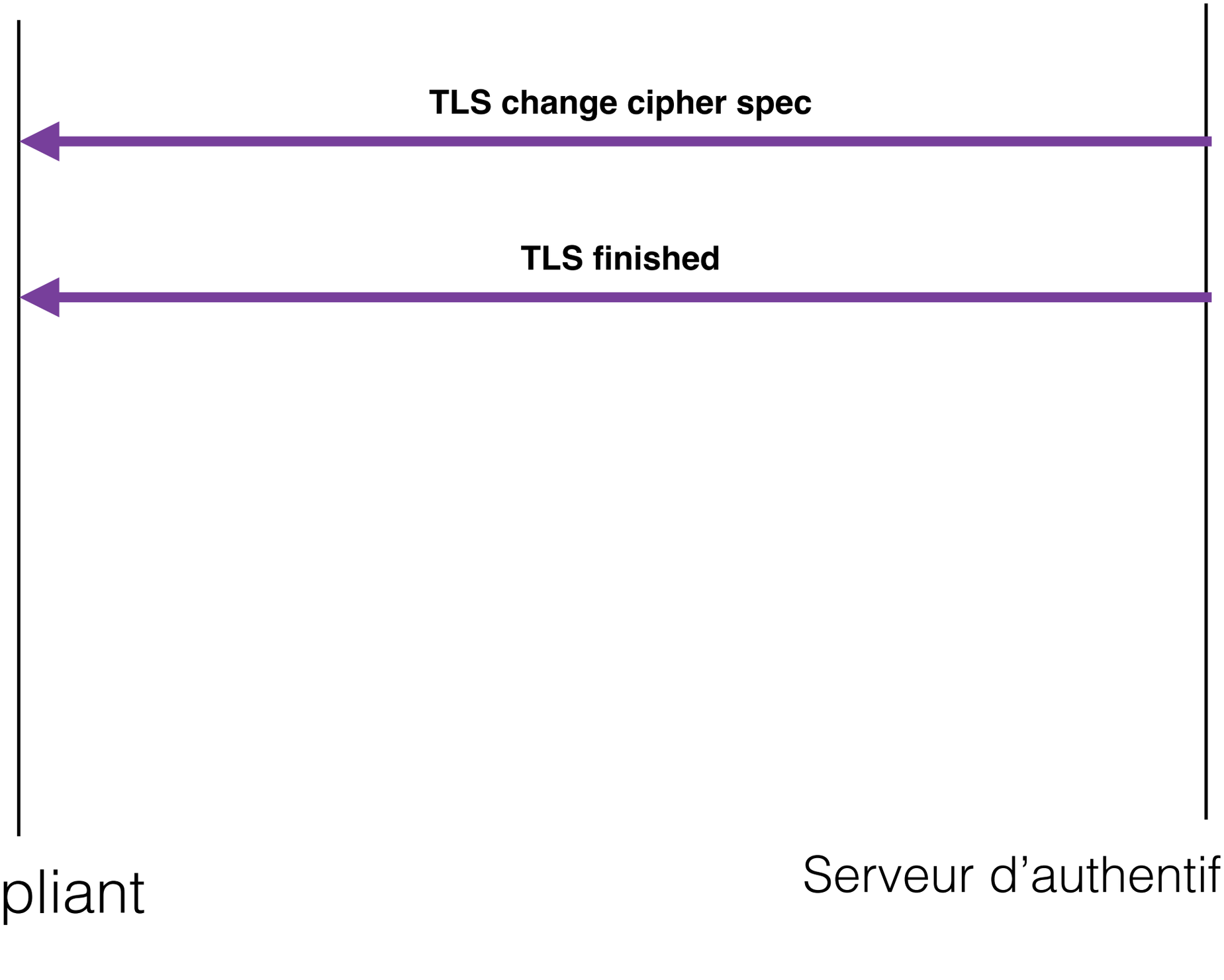
- transmission des certificats
- transmission du Pré Master Secret

4.Génération du Master Secret à partir du Pre Master Secret et des nombres aléatoires (les Nonces) et de la clé de session à partir du Master Secret et des deux nombres aléatoires

5.Phase de confirmation de conformité et de fin de l'authentification

6. Phase de transmission des clés du serveur d'authentification vers l'Authentificateur

Génération du Master Secret à partir du Pre Master Secret et des nombres aléatoires (les Nonces) et de la clé de session à partir du Master Secret et les mêmes deux nombres aléatoires



TLS finished

- Similaire au certificate verify
- Contient un hash chiffré de tous les messages de Handshake qui ont précédé le message présent
- Le chiffrement se fait avec les clés de session
- Le hash est calculé en utilisant

Verify_data = PRF(master_secret, "client finished" ou "finished", MD5(messages Handshake)+SHA-1(messages Handshake))

Phases EAP-TLS

1.Initiation

2.Phase Hello

- échange de Nonces (ClientHello.random et ServerHello.random),
- accord sur les algorithmes
- contrôler s'il s'agit d'une nouvelle session

3.Phase d'échange de certificats

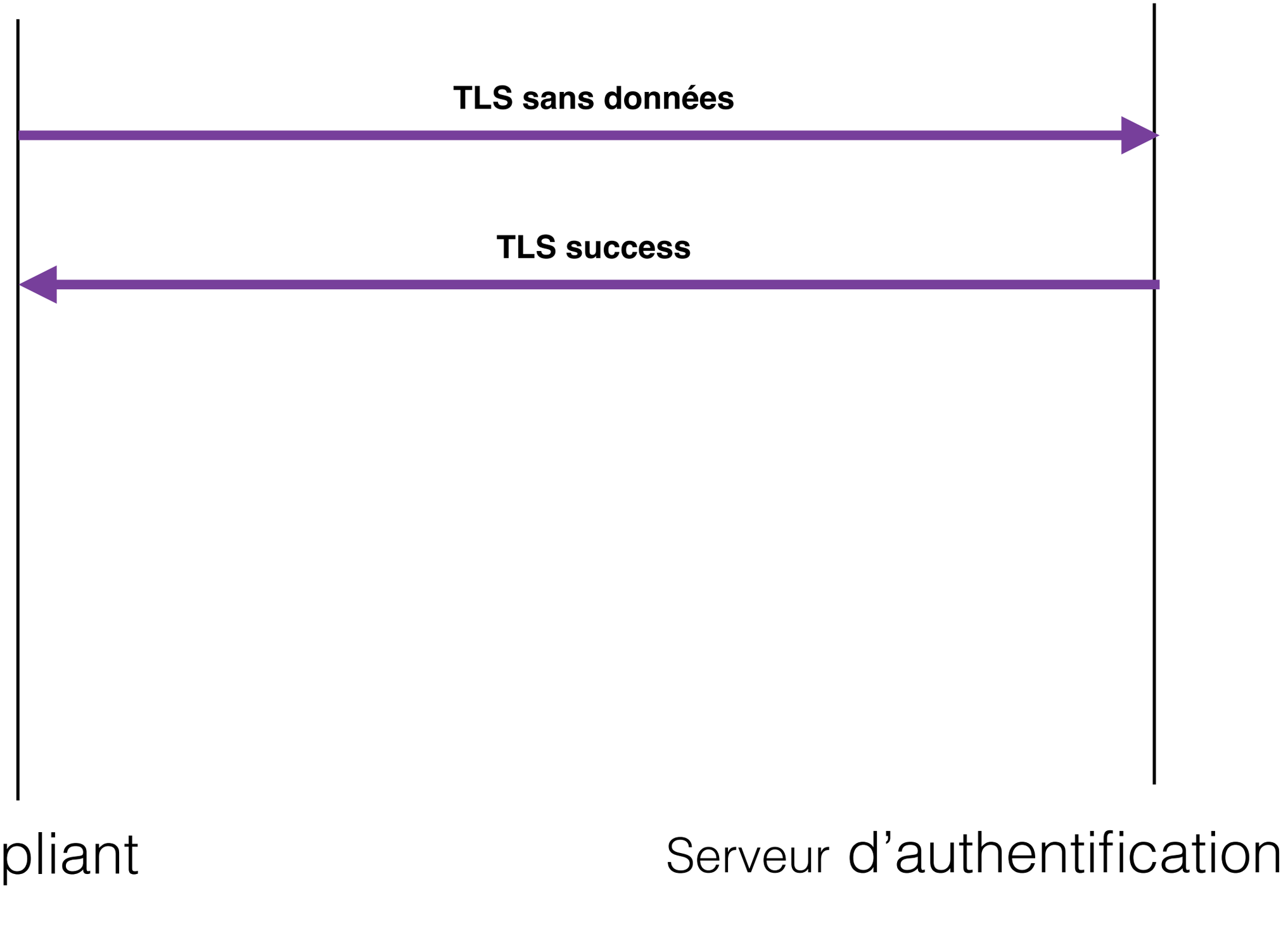
- transmission des certificats
- transmission du Pré Master Secret

4.Génération du Master Secret à partir du Pre Master Secret et des nombres aléatoires (les Nonces) et de la clé de session à partir du Master Secret et des deux nombres aléatoires

5.Phase de confirmation de conformité et de fin de l'authentification

6. Phase de transmission des clés du serveur d'authentification vers l'Authentificateur

Phase de confirmation de conformité et de fin de l'authentification



A la fin du Handshake

- Le suppliant et le serveur d'authentification sont en possession du Pre Master Secret

- Le Master Secret est calculé utilisant la fonction :

master_secret = TLS-PRF-48(pre_master_secret, "master secret", client.random || server.random)

A la fin du Handshake

- Le Key_Material est calculé utilisant la fonction:

Key_Material = TLS-PRF-128(master_secret, "client EAP encyption", client.random || server.random)

La Master session key MSK = Key_Material(0, 63)

PMK = MSK(0, 31)

Canal TLS

- Après le changement de cipher suite, le canal est chiffré en utilisant le protocole Microsoft Point-to-Point Encryption Protocol (MPPE)
- Les clés utilisées pour le chiffrement et pour l'intégrité sont différentes dans chacune des directions
- Elles sont dérivées à partir du keying material

Phases EAP-TLS

1.Initiation

2.Phase Hello

- échange de Nonces (ClientHello.random et ServerHello.random),
- accord sur les algorithmes
- contrôler s'il s'agit d'une nouvelle session

3.Phase d'échange de certificats

- transmission des certificats
- transmission du Pré Master Secret

4.Génération du Master Secret à partir du Pre Master Secret et des nombres aléatoires (les Nonces) et de la clé de session à partir du Master Secret et des deux nombres aléatoires

5.Phase de confirmation de conformité et de fin de l'authentification

6. **Phase de transmission des clés du serveur d'authentification vers l'Authentificateur**