IUT ANNECY
UNIVERSITÉ SAVOIE MONT BLANC

Cryptographie et sécurité

Cours 4: TLS et certificats

Mickaël Bettinelli
(mickael.bettinelli@univ-smb.fr)

Prérequis et objectifs

Compétences nécessaire pour ce cours:

- Comprendre le fonctionnement des chiffrements asymétriques

Compétences maîtrisées à la fin du cours:

- Connaître TLS et savoir ce qu’est un certificat

Sommaire

1. Infrastructures de gestion de clés
2. Les certificats
3. TLS / SSL

Comment gérer des clés

Les services proposés par les outils de gestion de clés:

1. Lier des clés publiques à des identités
2. Stocker des clés et les distribuer
3. Maintenance des clés

Quelques noms d’outils:

- L’autorité de certification
- La toile de confiance
- DANE

Autorité de certification (AC) - introduction

Objectif. authentifier l'identité de correspondants

Conditions d'utilisation. sécurisation des communications avec le protocole TLS (anciennement SSL)

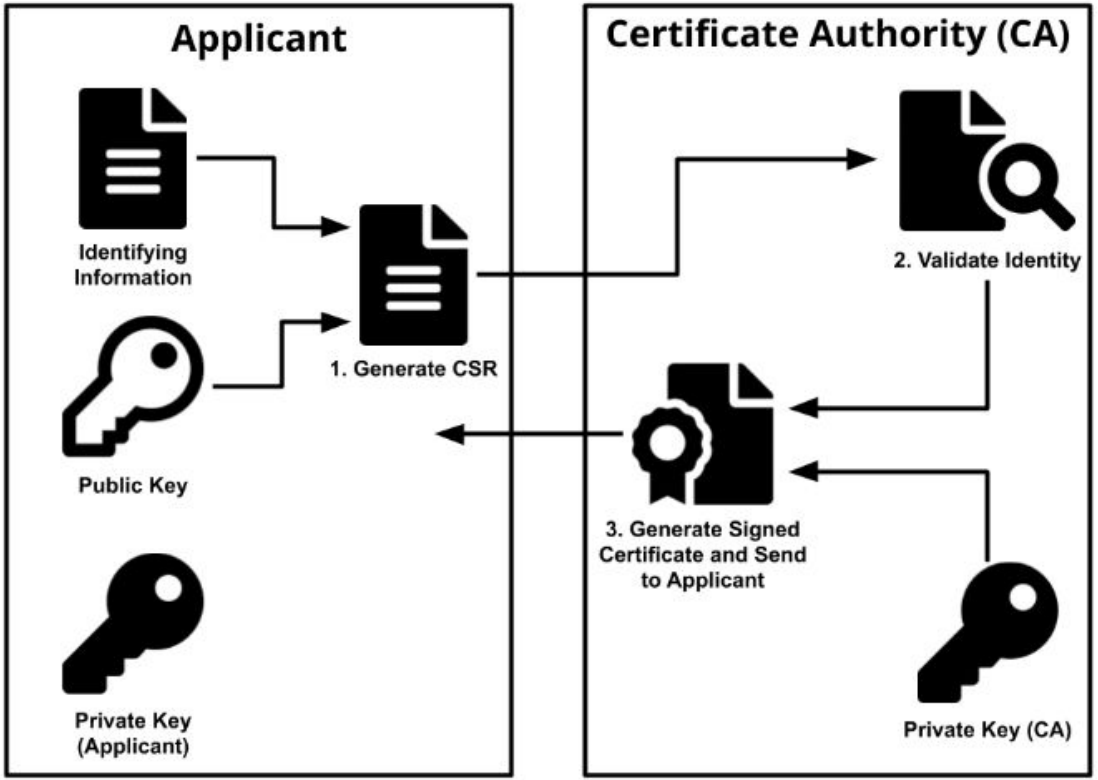
Fonctions.

1. Assure que les données entre le serveur et le client n'ont pas été modifiées durant le transfert
2. Protège de l'usurpation d'identité
3. Assure la confidentialité des données transmises

Obtenir un certificat

Fonctionnement.

1. Génération d'une clé publique et privée
2. Envoie de la clé publique + identité (coordonnées postales, téléphonique, etc.) à l'autorité de certification
3. L'AC vérifie l'identité
4. Elle génère et envoie un certificat au candidat
5. Le candidat intègre la clé sur son serveur web



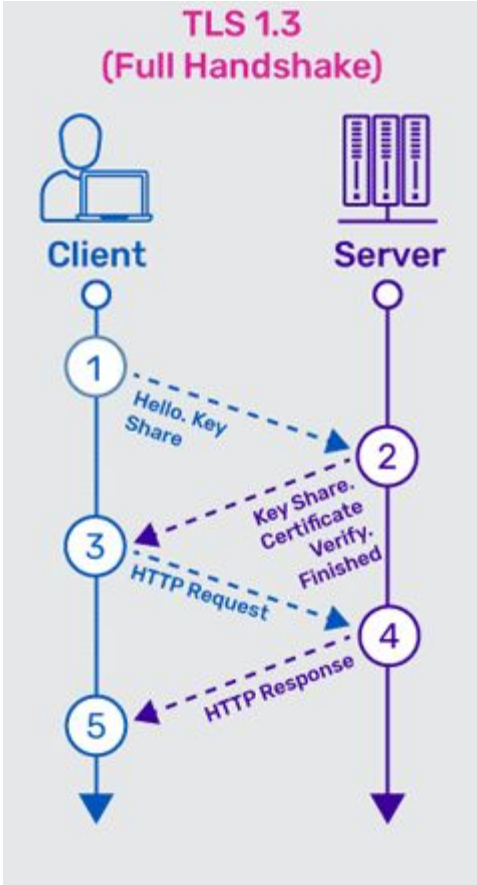
TLS 1.3 (dernière version, 2018)

Secure **S**ocket **L**ayer → SSL
Transport **L**ayer **S**ecurity → TLS

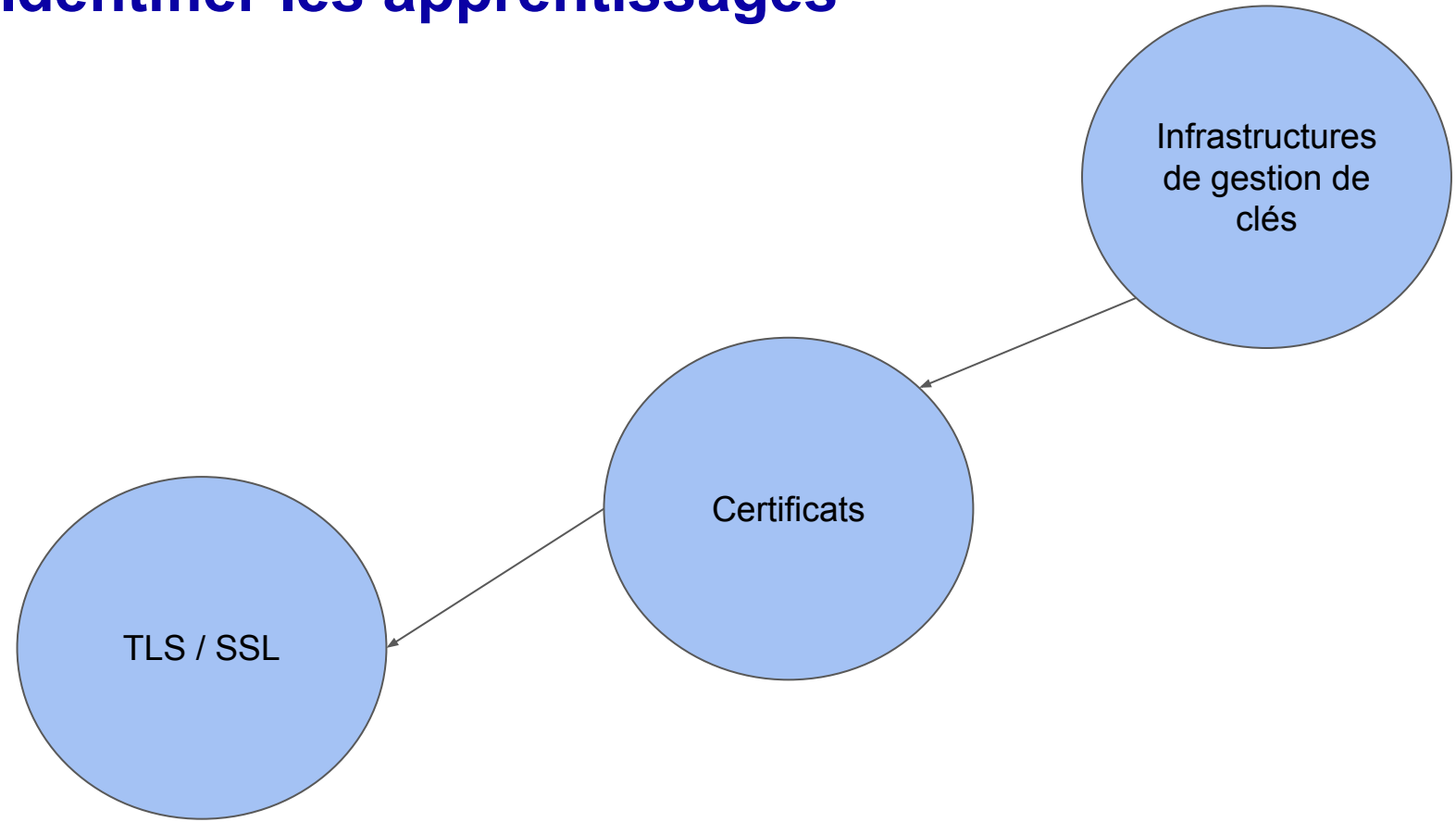
La différence entre les deux ?

- **TLS est la nouvelle version de SSL**

Dernière version de SSL: 1996



Identifier les apprentissages



Ressources complémentaires

- https://fr.wikipedia.org/wiki/Transport_Layer_Security
- https://www.a10networks.com/glossary/key-differences-between-tls-1-2-and-tls-1-3/