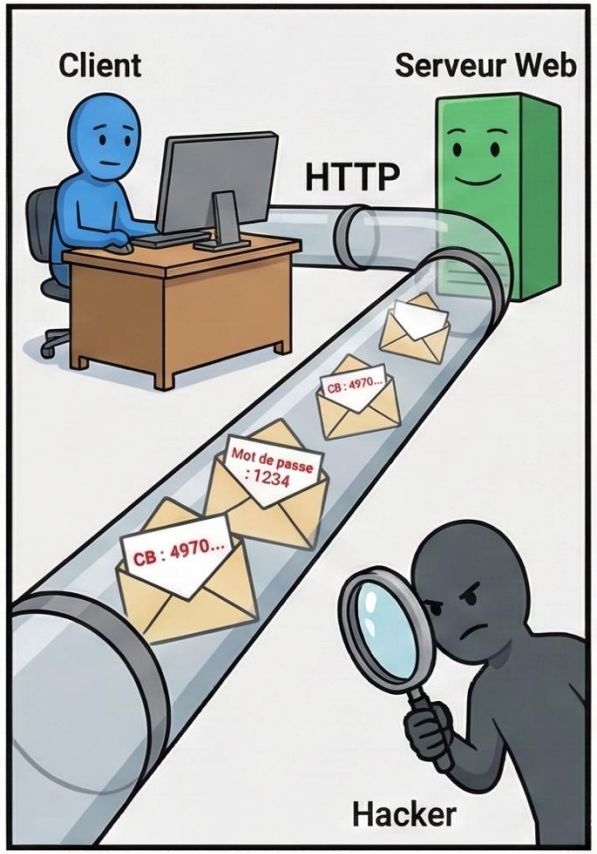
PLANCHE 1 : POURQUOI LES CERTIFICATS SSL ?

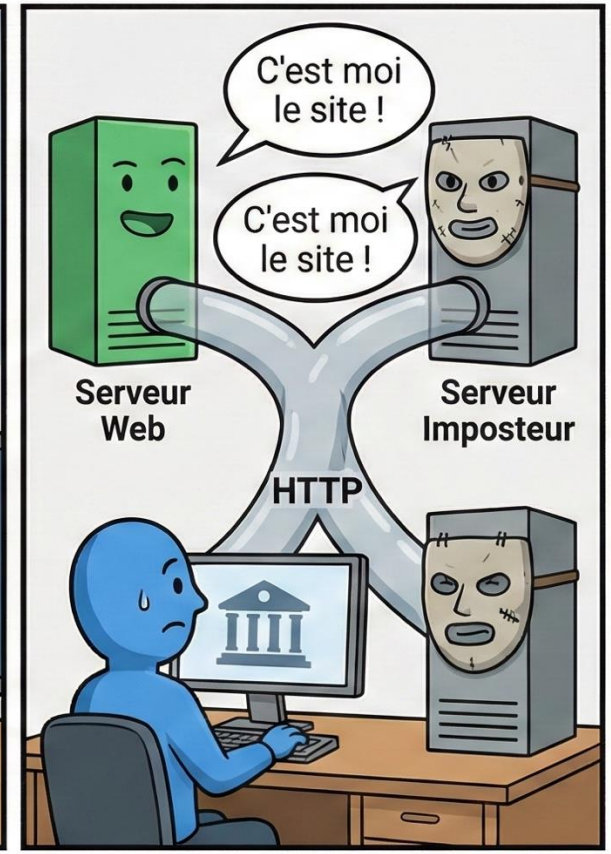
Titre : LE PROBLÈME DE LA CONFIANCE SUR INTERNET

Objectif pédagogique : Comprendre les risques de HTTP (écoute, usurpation)



Sur Internet, le protocole de base (HTTP) fait circuler les données "en clair". N'importe qui sur le chemin peut les intercepter.

J'envoie mes infos... mais comment savoir si je parle vraiment à ma banque et pas à un imposteur ?



HTTP ne garantit pas l'identité du serveur. L'usurpation est facile.

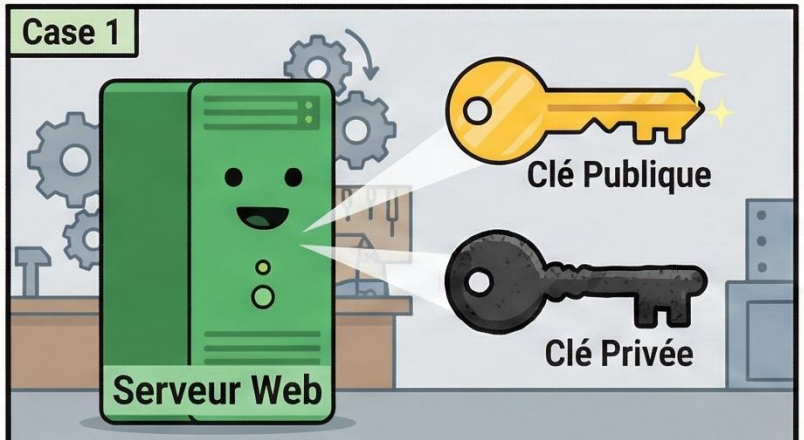
Pour sécuriser le web, il faut un moyen fiable d'identifier un serveur : le certificat numérique.

PLANCHE 2 : CONCEPTION D'UN CERTIFICAT (CÔTÉ SERVEUR)

Titre : LA CARTE D'IDENTITÉ DU SERVEUR

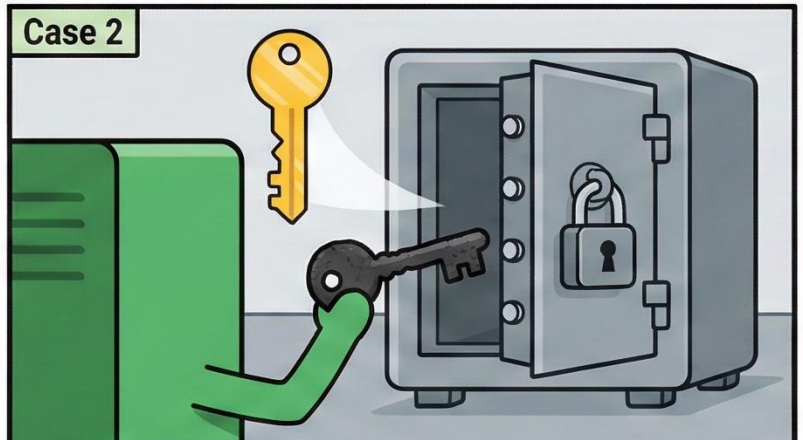
Objectif pédagogique : Comprendre la bi-clé et le contenu d'un certificat avant signature.

Case 1



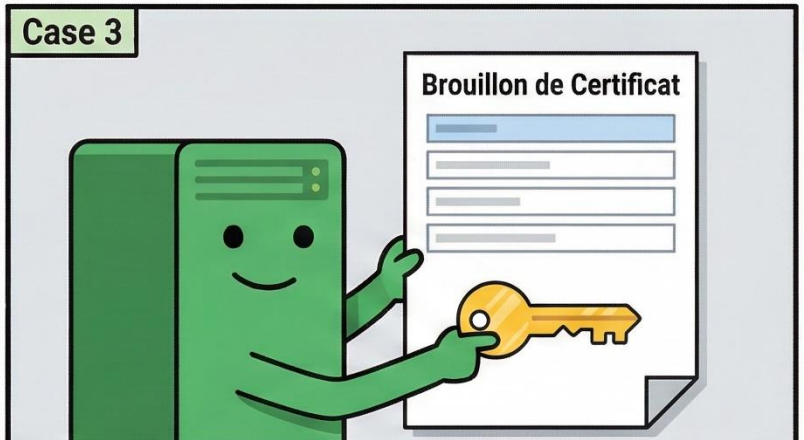
Pour commencer, le serveur génère une paire de clés cryptographiques liées mathématiquement.

Case 2



La clé privée est le secret absolu du serveur. Elle ne doit JAMAIS quitter son coffre-fort.

Case 3



Le serveur crée un certificat contenant ses infos (nom de domaine, organisation) et, surtout, sa clé publique.

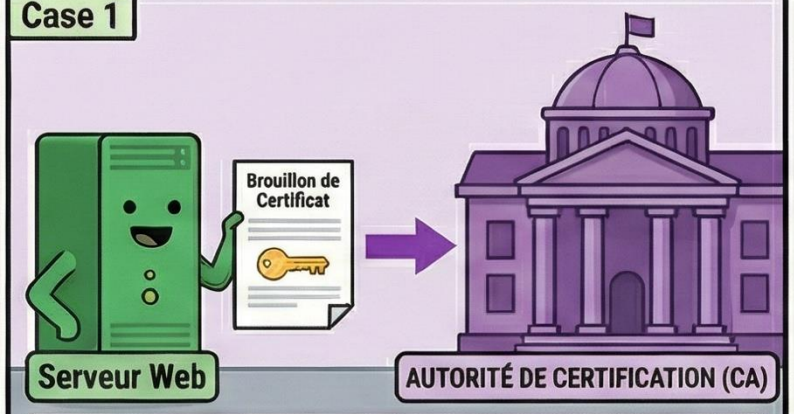
Un certificat non signé par un tiers n'a aucune valeur de confiance. Il faut le faire valider.

PLANCHE 3 : SIGNATURE PAR UNE AUTORITÉ DE CERTIFICATION (CA)

Titre : L'INTERVENTION DU TIERS DE CONFIANCE

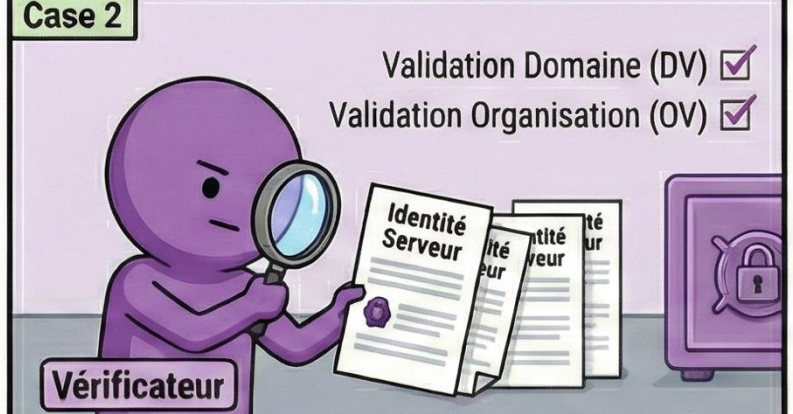
Objectif pédagogique : Comprendre le rôle de la CA et la mécanique de signature (Clé privée de la CA).

Case 1



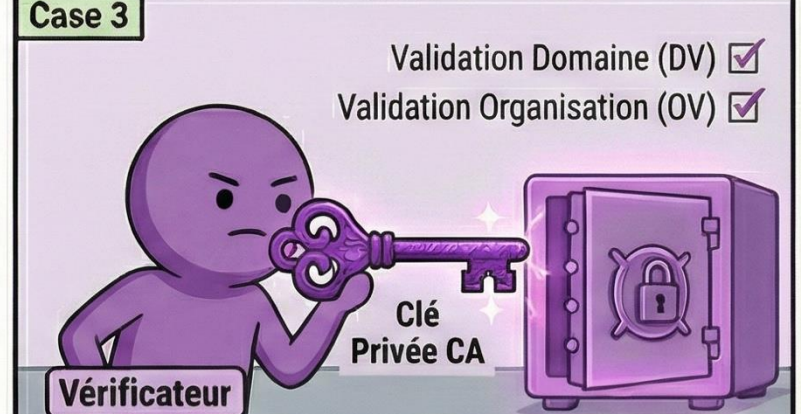
Le serveur envoie une demande de signature à une Autorité de Certification (CA), une organisation reconnue pour sa fiabilité.

Case 2



La CA vérifie rigoureusement que le serveur est bien uil prétend être (contrôle du domaine, de l'entreprise...).

Case 3



Une fois validé, la CA signe le certificat du serveur en utilisant **SA propre clé privée** (celle de la CA).

Case 3

Cette signature cryptographique scelle le document. Elle garantit l'intégrité du certificat et l'identité de la CA émettrice.

Case 4

Une fois validé, la CA signe le certificat du serveur en utilisant **SA propre clé privée** (celle de la CA).

Case 5

PLANCHE 4 : VÉRIFICATION PAR LE NAVIGATEUR & CONNEXION TLS

Titre : L'ÉTABLISSEMENT DE LA CONNEXION SÉCURISÉE (HTTPS)
Objectif pédagogique : Comprendre la chaîne de confiance et la transition vers le chiffrement symétrique.