Réseau de confiance

Un **réseau de confiance** est un modèle dans lequel chaque participant (par exemple, une maison connectée ou un appareil IoT) accorde sa confiance à d'autres participants sur la base de relations directes ou indirectes. Cette confiance est essentielle pour assurer la validité des échanges.

2 aspects fondamentaux

Pour réaliser un réseau de confiance, au moins deux élements sont à prendre en compte :

Identité

Chaque nœud doit pouvoir être identifié et reconnaissable, du point de vue des deux partenaires d'un échange:

- Le récepteur est certain de l'identité de l'émetteur
- L'émetteur ne peut pas prétendre ne pas être à l'origine du message

On parle alors de **non-répudiation**, ce qui implique une architecture de type PKI.

Cela passe donc par des **certificats de confiance** :

- Les nœuds possèdent des certificats émis par une autorité centrale ou décentralisée.
- Chaque certificat associe une identité à une clé publique.

tout en permettant la **propagation de la confiance** :

- Les relations de confiance peuvent être directes (maison A connaît maison B) ou transitives (A fait confiance à B, qui fait confiance à C).

ce qui implique une **validation mutuelle** avant de partager des informations.

Validité

Chaque nœud doit agir pour le bien commun du réseau. Ceci implique différentes stratégies comme l'analyse du traffic pour un `contrôleur` pour éviter, par exemple, qu'une maison modifie sa trésorerie de manière illicite...

Importance du logging

On peut aussi imaginer analyser les logs quotidiens pour détecter des opérations illicites... Ceci mène naturellement à l'utilisation de mécanismes en lien avec la blockchain, ce qui d'ailleurs résout aussi un problème lié à la confiance initiale

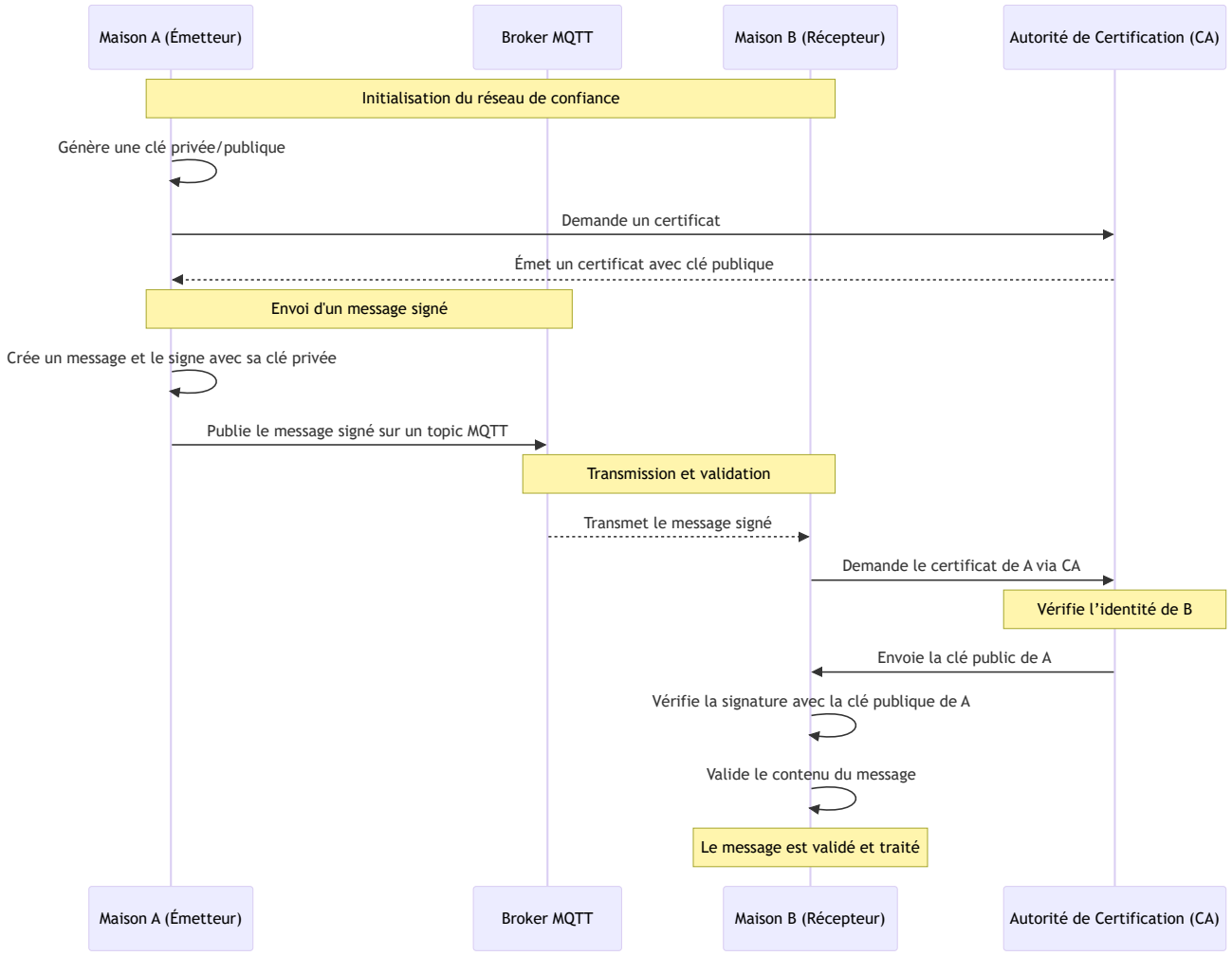
Exemple d'application avec PKI (Public Key Infrastructure)

1. **Établissement de la confiance** :
    - Chaque maison s'enregistre auprès d'une autorité de certification (CA, par exemple Verisign...) pour obtenir un certificat X.509, qui contient sa clé publique.

- Ces certificats peuvent être validés par d'autres maisons avant de commencer les échanges.

2. **Signature des messages MQTT** :
    - Les messages envoyés via le broker sont **signés** avec la clé privée de l’émetteur.
    - Exemple : Une maison publie un message sur le **topic "powercher"**, accompagné de la signature de son contenu.
3. **Vérification au niveau du broker ou des abonnés** :
    - Les abonnés (maisons connectées) utilisent la clé publique de l’émetteur (disponible via le certificat) pour valider la signature et s'assurer que :
        - Le message provient bien de l’émetteur déclaré.
        - Les données n’ont pas été modifiées en transit.
4. **Gestion des fichiers multimédias** :
    - Les fichiers sont hachés (ex. SHA-256) avant transmission.
    - Le hachage est signé.

Diagramme de séquence



Défis et solutions de la version PKI

1. **Gestion des certificats** :
    - Problème : Distribution et révocation des certificats.
    - Solution : Utiliser un protocole comme **OCSP (Online Certificate Status Protocol)** pour vérifier l'état des certificats.
2. **Latence et overhead** :
    - Problème : Les opérations cryptographiques peuvent augmenter la latence.
    - Solution : Optimiser les algorithmes (ex. ECDSA au lieu de RSA) et utiliser des matériels dédiés (ex. puces TPM).
3. **Confiance initiale** :
    - Problème : Établir un réseau de confiance initial sans point central fort.
    - Solution : Modèle hybride avec une autorité initiale décentralisée ou une blockchain.