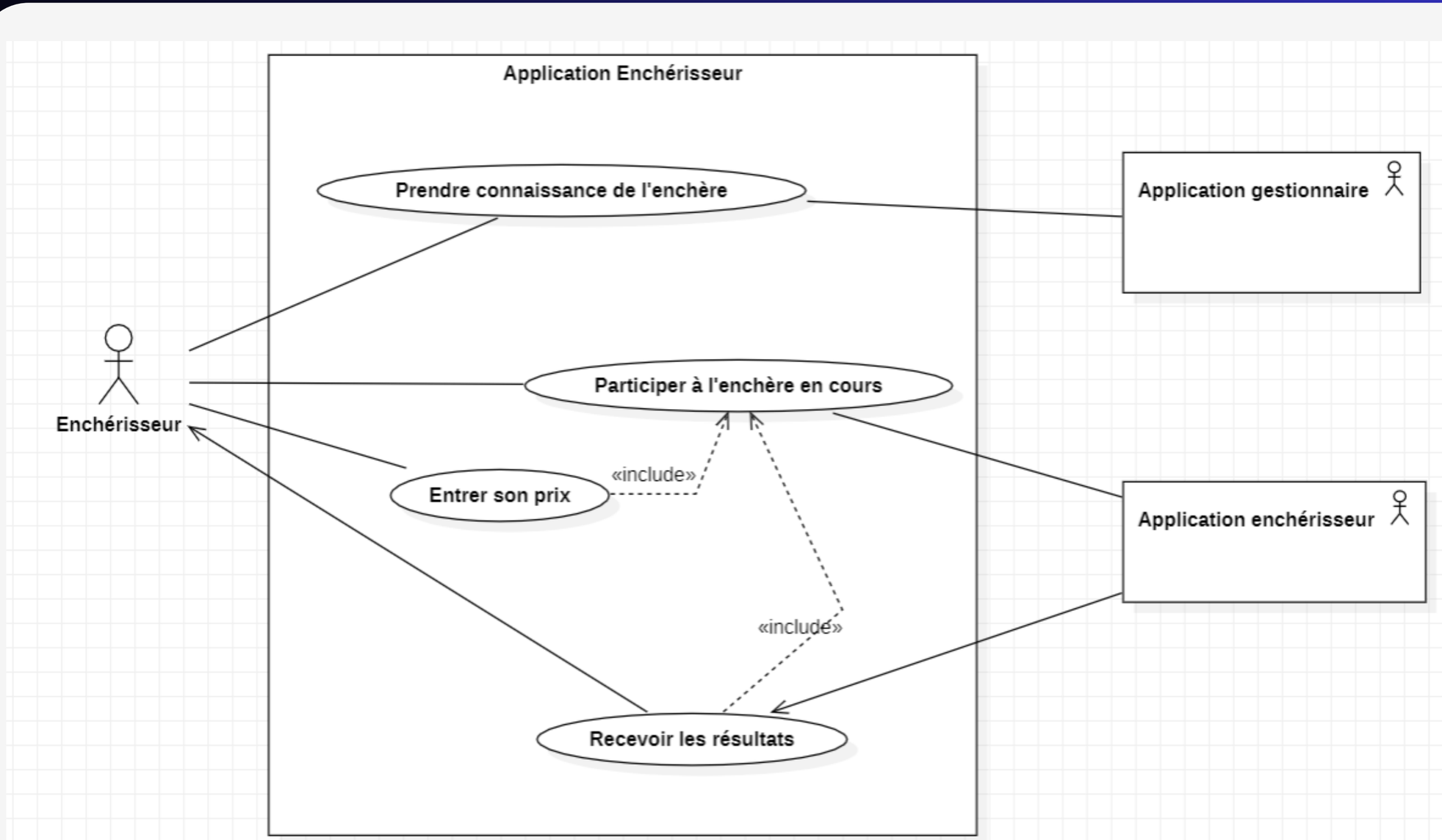
Sprint 3

TREMOULET BRETON Loan
JACQUEMIN Paul
SALA-MOCHIZUKI Yûki
VACHALDE Rémi
AUXILIEN Katia

Mise en contexte

Pour le Sprint 3, nous devions :

- Implémenter les signatures
- Enregistrer la signature de l’utilisateur
- Corriger notre utilisation des sockets sécurisés
- Développer l’attribution automatique des ports


Application Enchérisseur
Prendre connaissance de l'enchère
Application gestionnaire
Enchérisseur
Participer à l'enchère en cours
«include»
Entrer son prix
Application enchérisseur
«include»
Recevoir les résultats

Signature :

~/.config/securewin ✅

C:\Users\Utilisateur\AppData\Local\securewin ❌

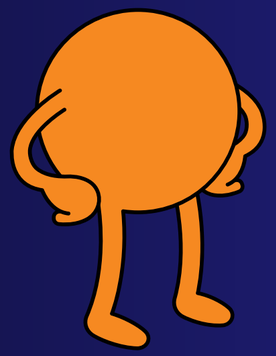
/Library/Application Support/securewin ❌

config_signature_keypair.jks

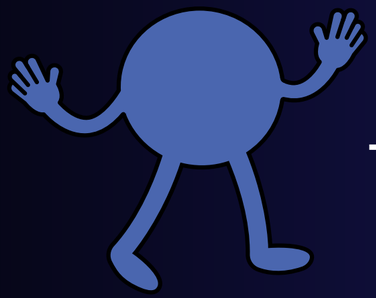
Clé secrète

config_signature_certificate.cer

Clé publique



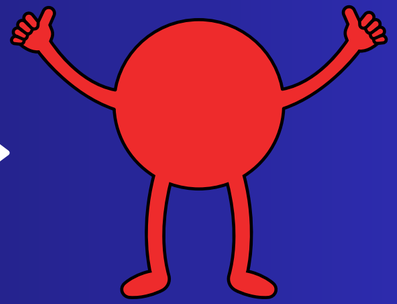
Manager



Bidder

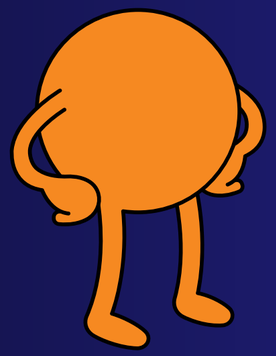
✅ **Participation**

(Signé, Prix chiffré, Clé pub)

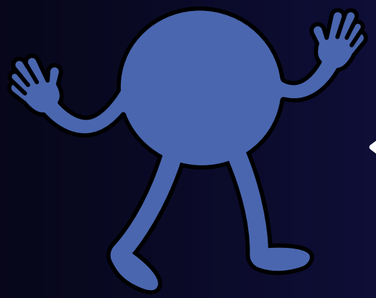


Seller

✅ **Vérification**



Manager

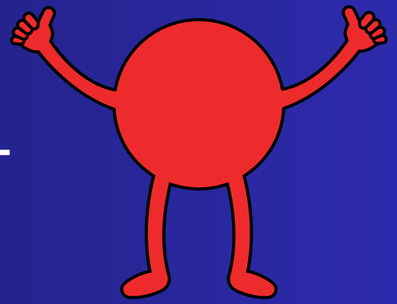


Bidder

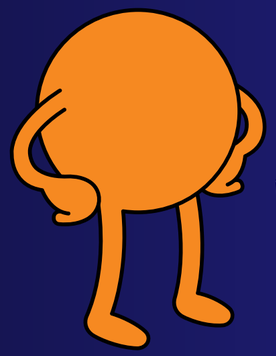
❌ **Vérification**

❌ **Broadcast**

(Ensemble(Signé,Prix chiffré), Signé)



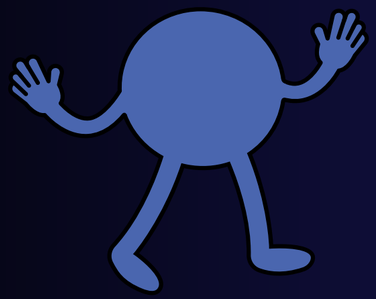
Seller



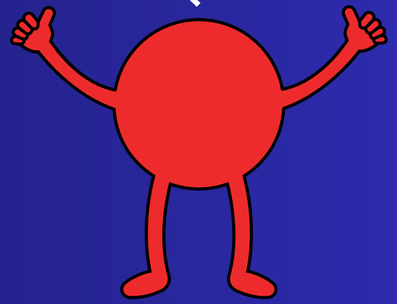
Manager

Ensemble (Prix chiffré, Signé)

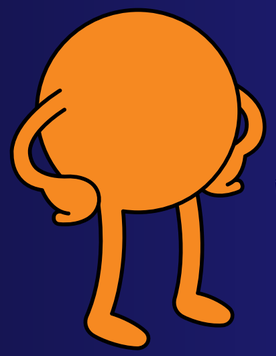
✅ **Transmission**



Bidder



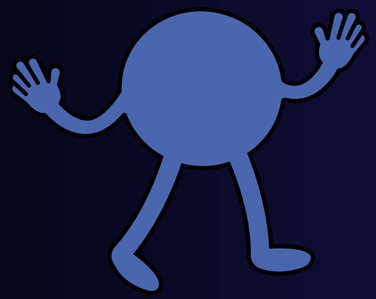
Seller



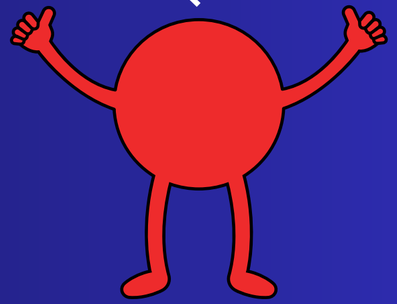
Manager

(Ensemble (Prix chiffré, Signé)**) Signé**

❌**Ensemble non signé**



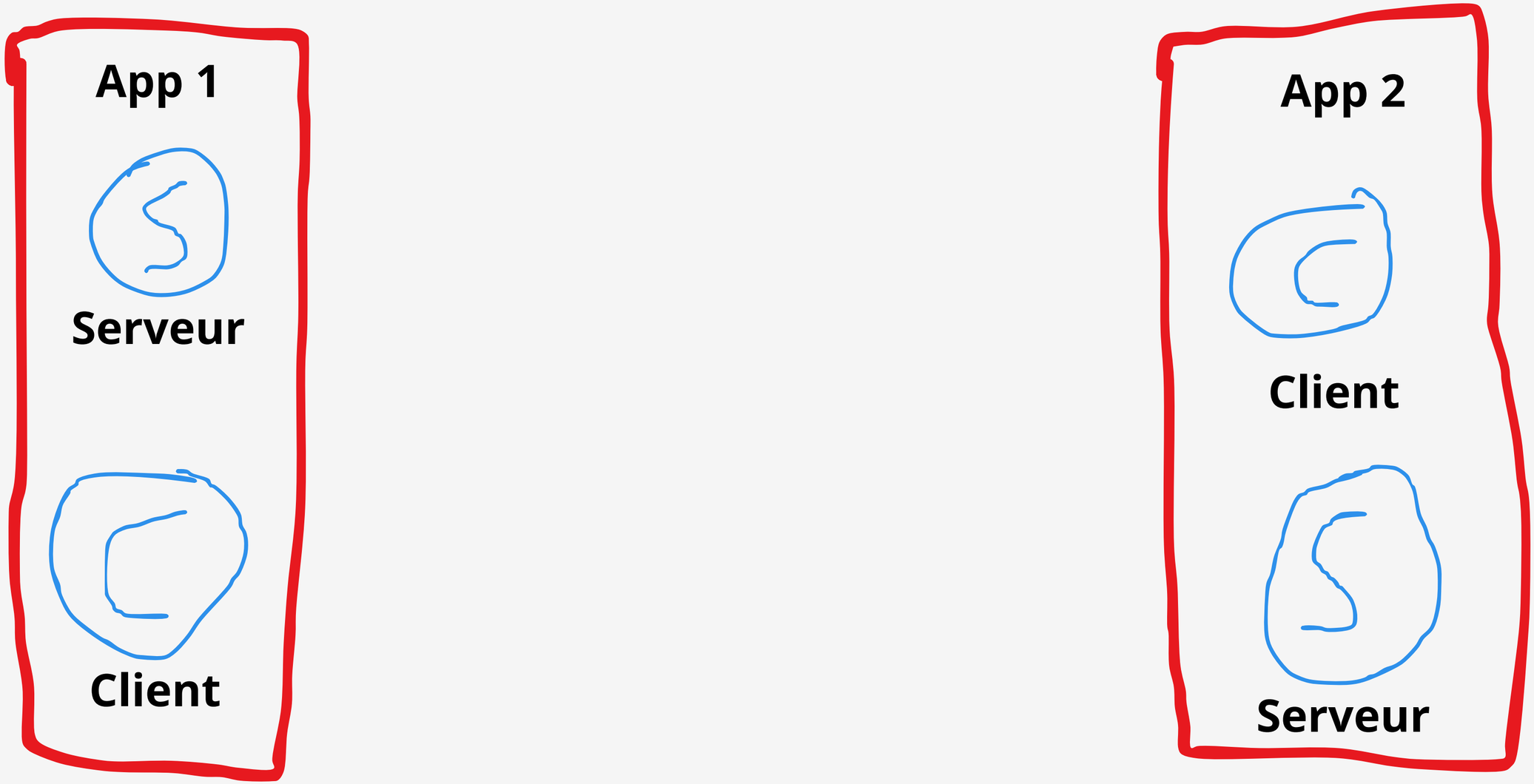
Bidder

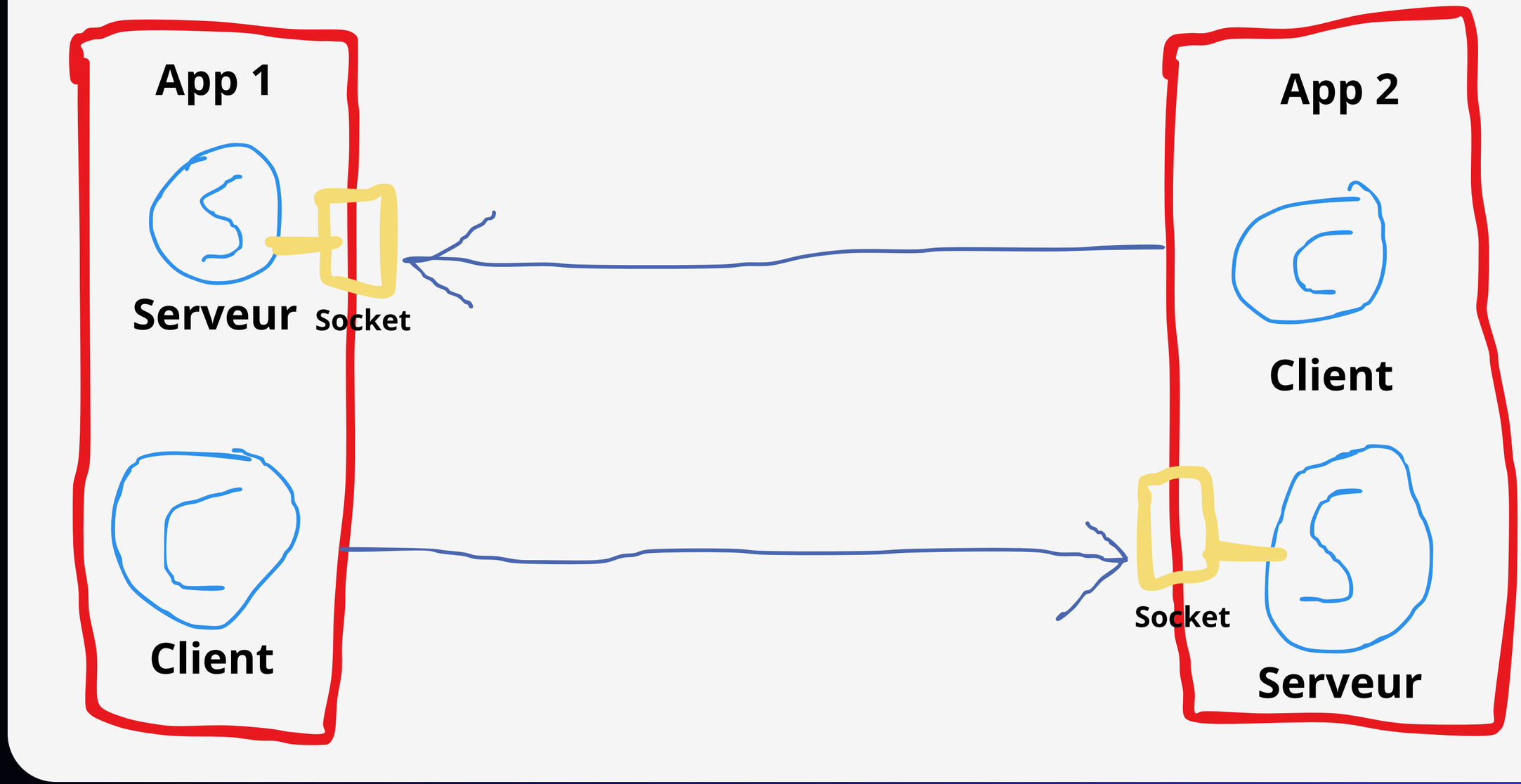


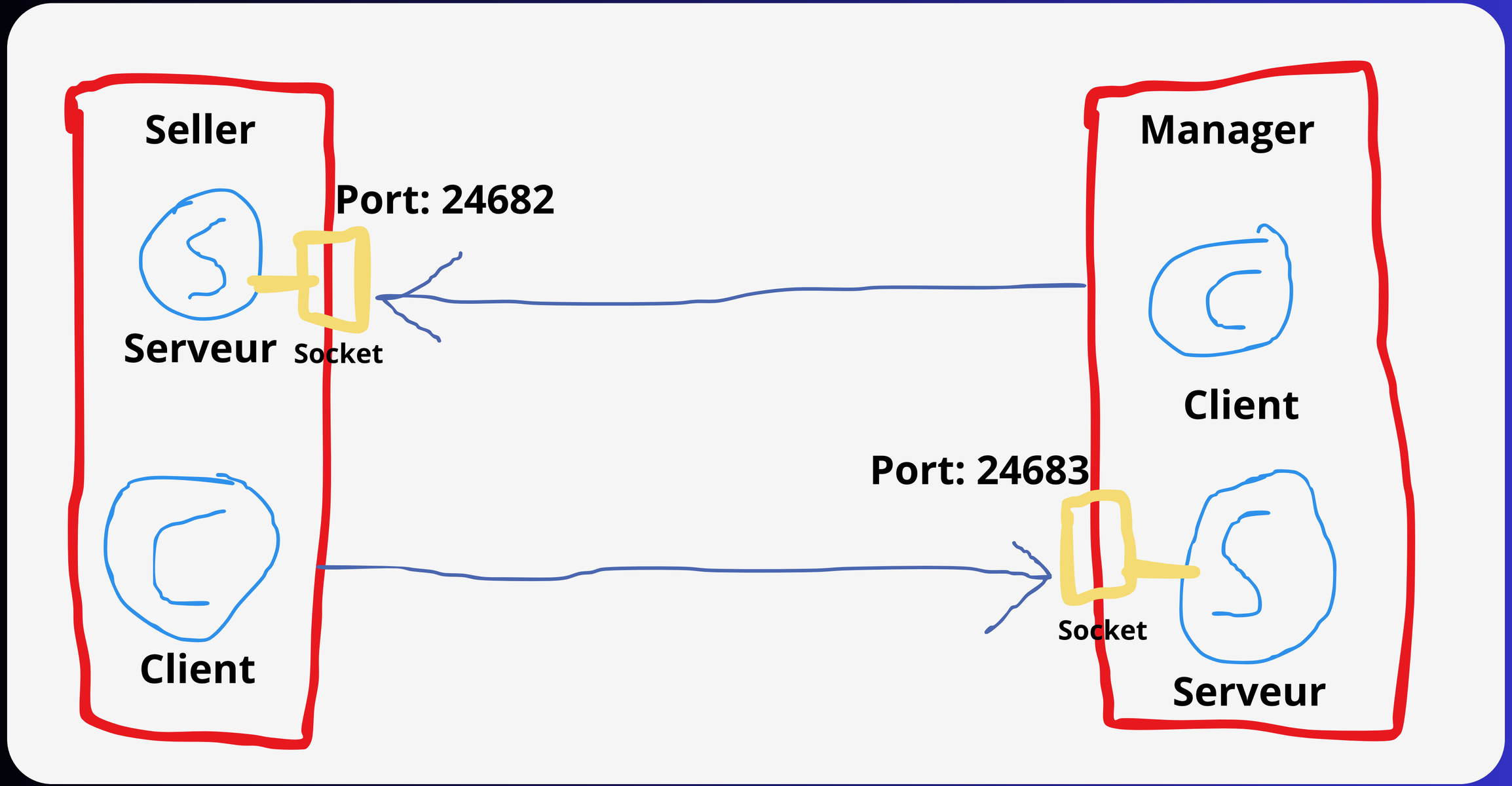
Seller

Sockets Sécurisés

Attribution des ports


App 1
Serveur
Client
App 2
Client
Serveur


App 1
Serveur
Socket
Client
App 2
Client
Socket
Serveur


Seller
Port: 24682
Serveur
Socket
Client
Manager
Client
Port: 24683
Socket
Serveur

Progression :

- ✅ Corriger notre utilisation des sockets sécurisés
- ✅ Développer l’attribution automatique des ports
- 🔁 Implémenter les signatures
- ✅ Enregistrer la signatures de l’utilisateur

Démonstration

Merci de votre attention !