Spécifications Supplémentaires

Besoins non fonctionnels

Ergonomie et interface

Développement en langage **Java 17**, utilisation des **sockets** pour les échanges.

Fiabilité

Les prix sont chiffrés par **RSA**.
Échanges authentifiés par **signature RSA** et **AES-256,** dont la paire de clé correspondant à la signature est enregistré dans un fichier .jks *(.jks : **Java KeyStore (JKS) :** C'est un format de fichier de stockage de clés utilisé par Java pour stocker des clés privées, des certificats publics et des certificats de confiance. C'est le format standard utilisé dans de nombreuses applications Java. Les fichiers JKS sont protégés par mot de passe et peuvent contenir des paires de clés asymétriques.)*

Utilisation des **sockets sécurisés** pour les échanges (avec certificat .JKS)

Performance

Pas de recherche d'amélioration des performances.

Support

Environnement de développement : **Intellij Idea**.
Applications sous **OS Linux** uniquement.
Chemin des fichiers de config de l'application : **`~/.config/securewin`**

Contient les fichiers relatifs à la signature de l'utilisateur :
`config_signature_keypair.jks` correspond à la clé privée de signature.
`config_signature_certificate.cer` correspond à la clé publique de signature.

`~/.config/securewin/ssl` contient le certificat **`certificatssl.jks`** qui assure les échanges par sockets sécurisés.

Ports de communication :
SecureWin_Bidder : **Attribuée par l'application**
SecureWin_Seller : **Attribuée par l'application**
SecureWin_Manager : **2463 Attribuée par l'application?**

Règles et informations dépendantes du domaine

Enchères à pli fermé/de Vickrey. L'enchérisseur ayant proposé le prix le plus élevé paye le second prix le plus élevé.

Fonctionnalités

- Chiffrement
- Echanges par sockets en protocole TCP
- Signatures
- Sauvegarde des signatures