

Fabien LAGUILLAUMIE  
Francis GARCIA

# SecureWin.

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

# Membres de l'équipe

**SALA-MOCHIZUKI  
YÛKI**

Scrum Master & Développeur



**AUXILIEN KATIA**

Product Owner & Développeuse



**VACHALDE RÉMI**

Développeur



**JACQUEMIN PAUL**

Développeur



**TREMOULET-  
BRETON LOAN**

Développeur



# Table des matières

I - Présentation de SecureWin

II - Fonctionnalités

III - Développement

IV - Choix technique

V - Pistes d'amélioration

VI - Démonstration

# Qu'est-ce que SecureWin ?

Septembre 2023

Fabien LAGUILLAUMIE

Antoine CHOLLET

Francis Garcia

Trois applications

# Fonctionnalités



Enchère de Vickrey



Persistance des signatures



Chiffrement **homomorphe**



Échanges sécurisés sur le réseau



Signatures RSA



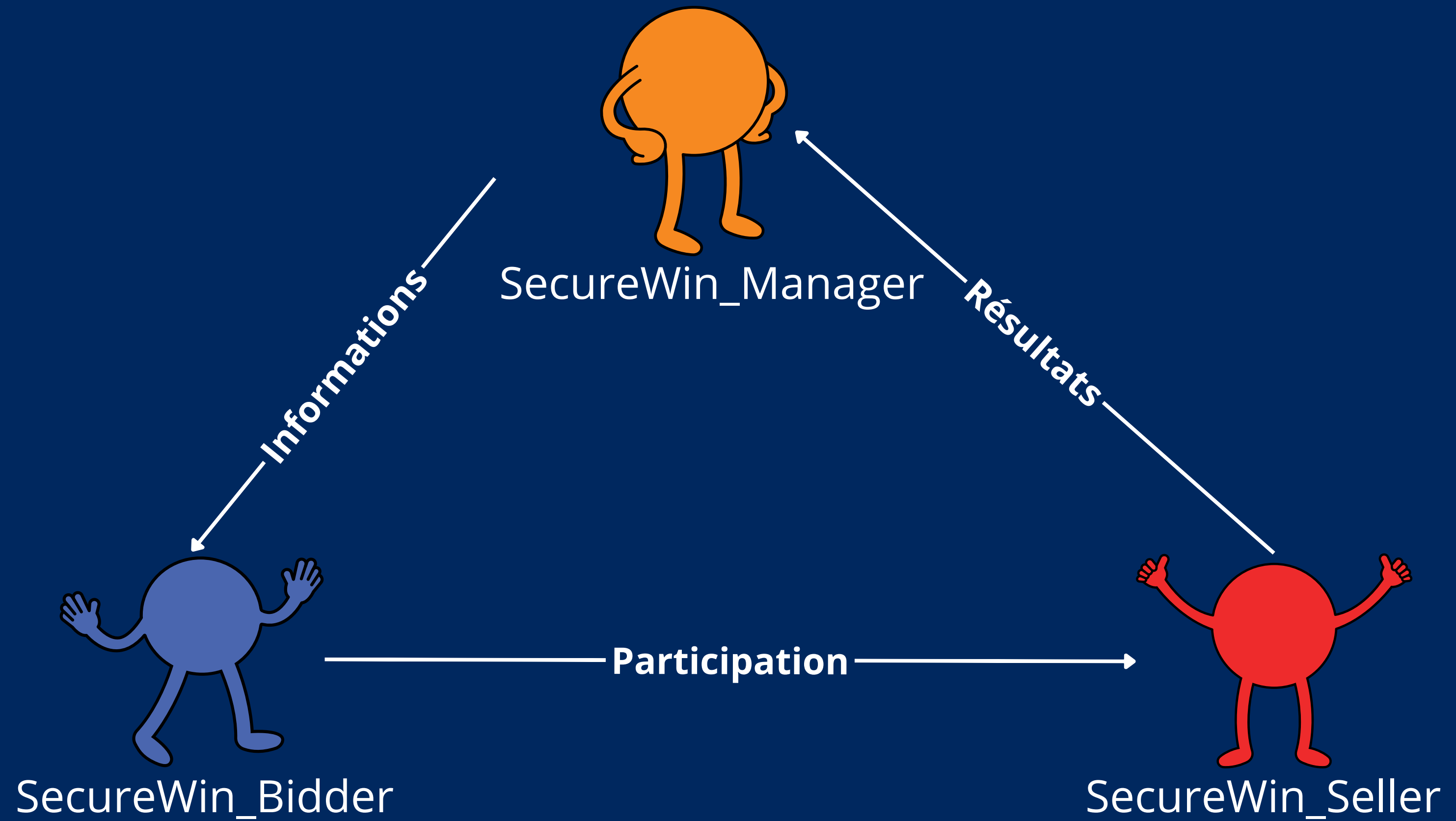
Conteneurisation



Signalement



Interface graphique et en ligne de commande



# Systeme de Damgård–Jurik

# Docker





# Développement du projet

AGILE  
SCRUM

TESTS

PRINCIPES  
SOLID


DESIGN  
PATTERNS

## Structure du code

INTERFACE

SIGPACK

# Choix technique

- Java version 17
- OS Linux 
- JavaFX
- Fichiers .jks .cer ~/.config/securewin
  - Stockés côté utilisateur
- Signature RSA et AES-256



config\_signature\_keypair.jks



config\_signature\_certificate.cer



Clé secrète



Clé publique

# Pistes d'amélioration

## Encoder prix

Utiliser les avantages du  
chiffrement homomorphe

## Historique

Historique des enchères

## Design

Créer une identité visuelle à  
securewin

## Interopérabilité

Étendre l'application à  
plusieurs OS

## Personnalisation

Thème sombre, langues etc..

## Mot de passe

Protéger la signature d'un  
poste

# Démonstration



**Merci de votre écoute**