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

Mise en contexte

Fonctionnalités

Enchère de Vickrey

Persistance des signatures

Chiffrement

Echanges sécurisés

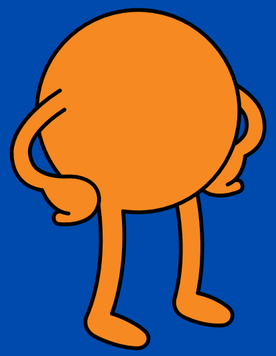
Signatures

Signalement

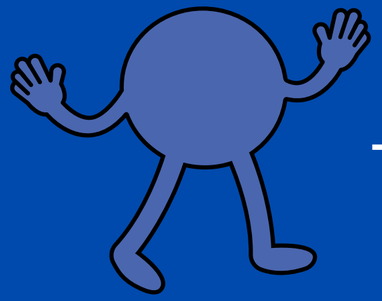
Objectifs du Sprint 1 :

- Implémenter le nouveau protocole d’enchères
- Restructurer le code
- Remplacer l’algorithme de chiffrement
- Rédiger des tests unitaires
- Réfléchir à une nouvelle interface graphique

Protocole d’enchère



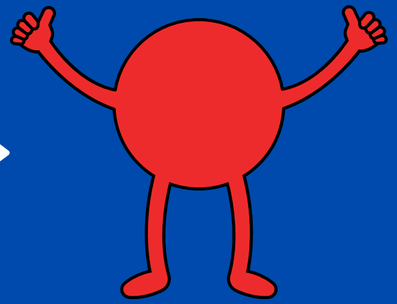
Manager



Bidder

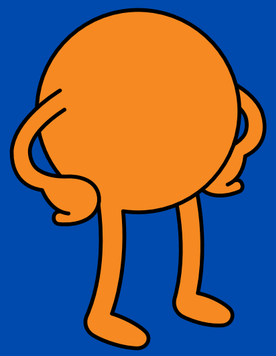
Participation

(Signé, Prix chiffré, Clé pub)

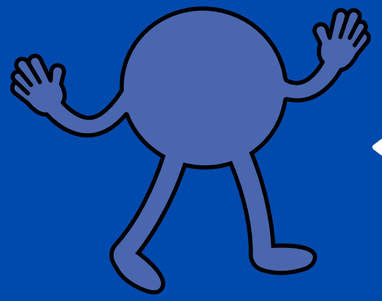


Seller

Vérification

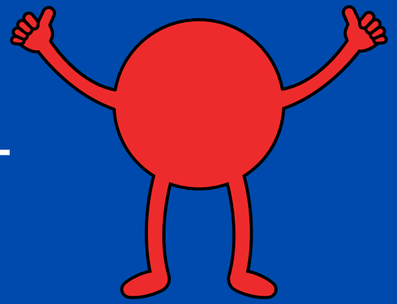


Manager



Broadcast

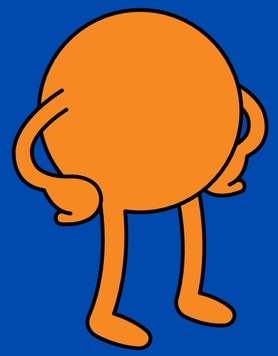
(C,c, z)



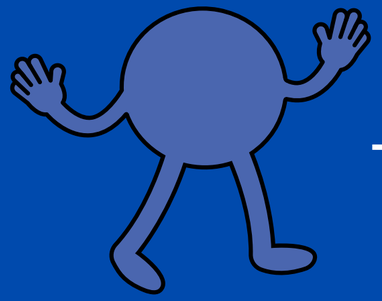
Bidder

Seller

Vérification sur C



Manager



Bidder

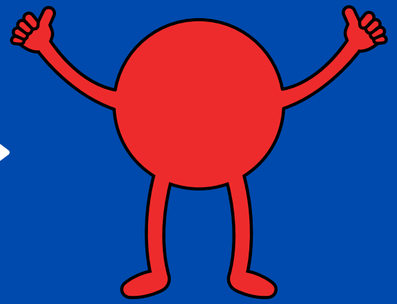
Confirme ou signale

Répond

(1,signé, clé pk signature)

ou

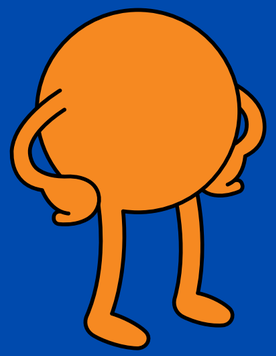
(0,signé, clé pk signature)



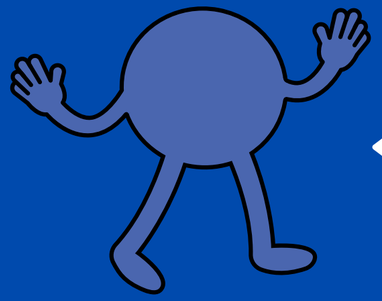
Seller

Liste de B ok

Liste de B non ok



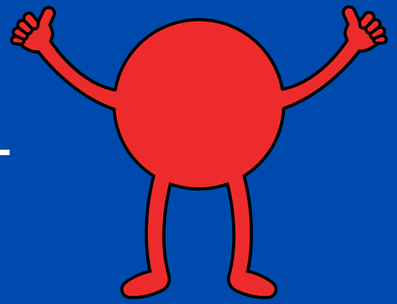
Manager



Bidder

Répond

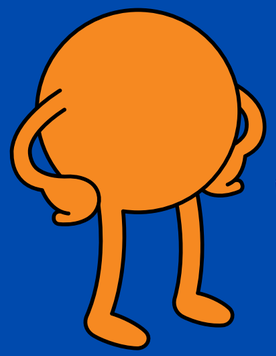
(PlayerStatus)



Seller

Seller signe (PlayerStatus) ?

Vérifie et éjecte les B falsifiés *ou non présents* dans C



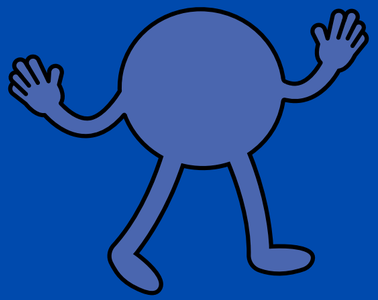
Manager

Traitement des offres sur c

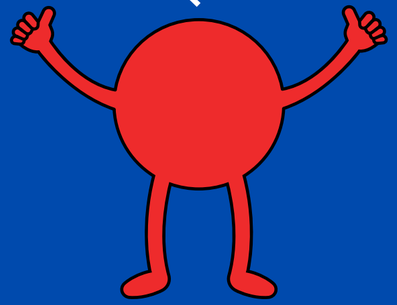
C ?

(C,c,z)

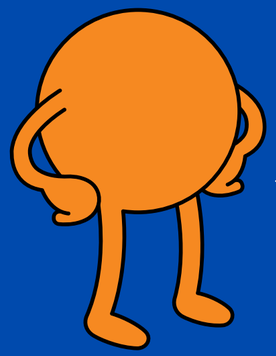
Transmission



Bidder

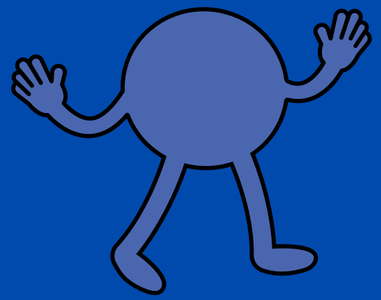


Seller

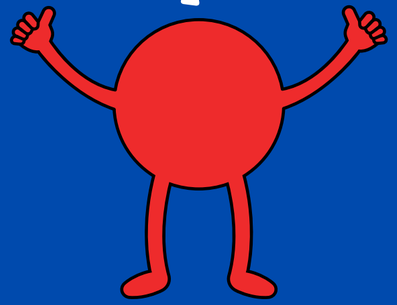


Manager

(p2,z’, p1Enc)

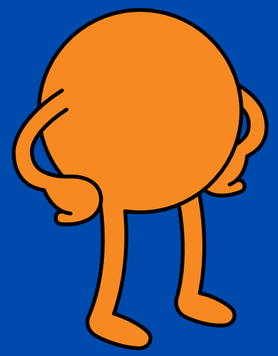


Bidder

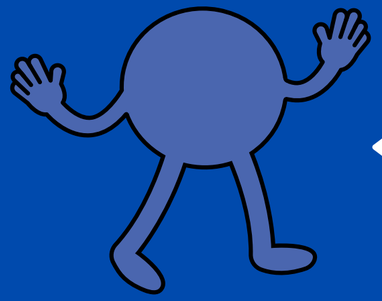


Seller

Vérification z’ et ajout z sur (p2,z’)
Garde en variable p1Enc



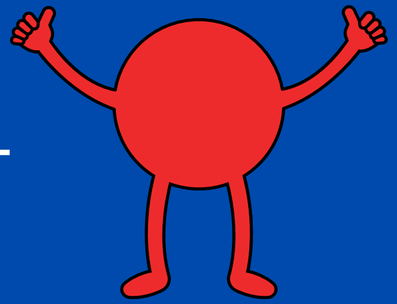
Manager



Bidder

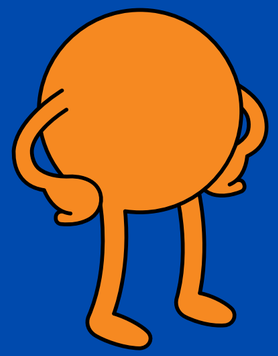
Résultats

(z,(p2,z'))

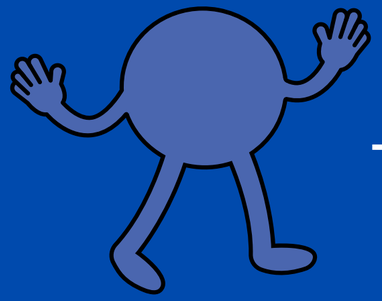


Seller

Vérification des signatures de M et de S



Manager

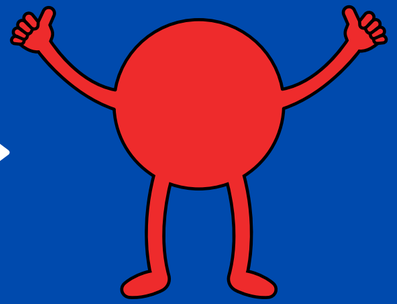


Bidder

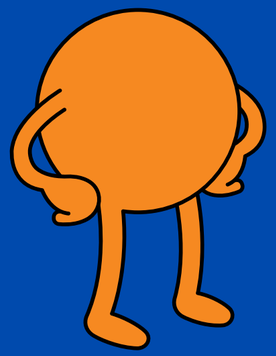
Si gagnant

Manifestation

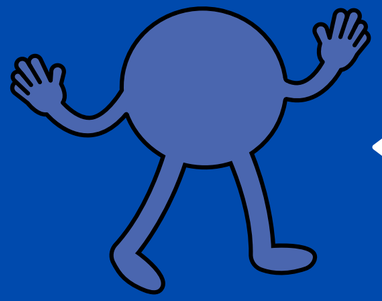
(1,signé, signature pk, p1Enc)



Seller



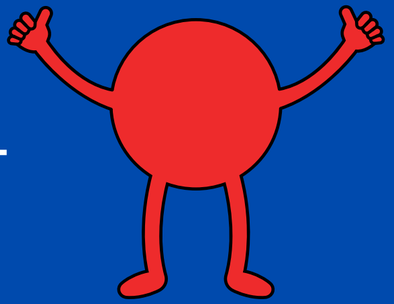
Manager



Bidder

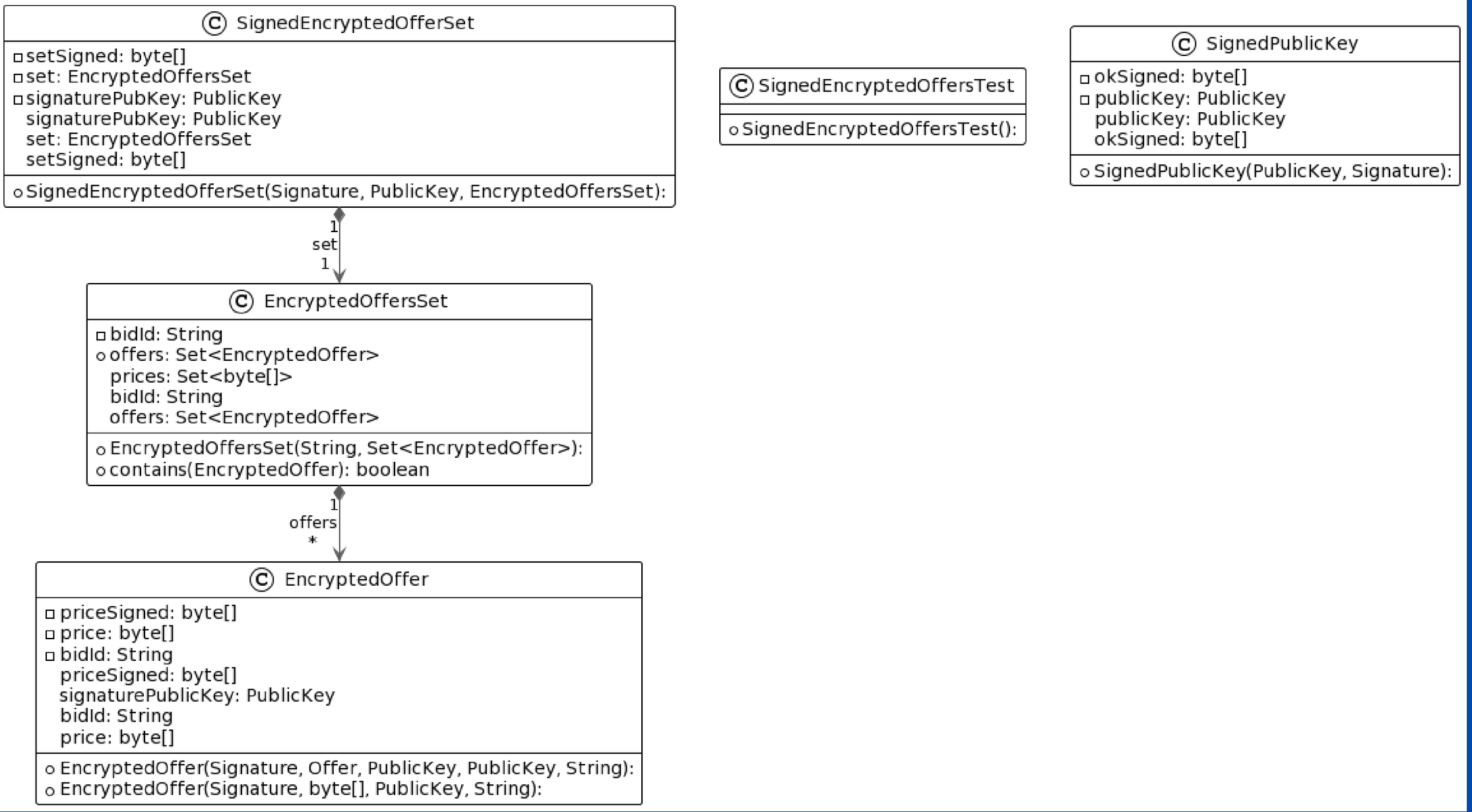
Confirmation ou non

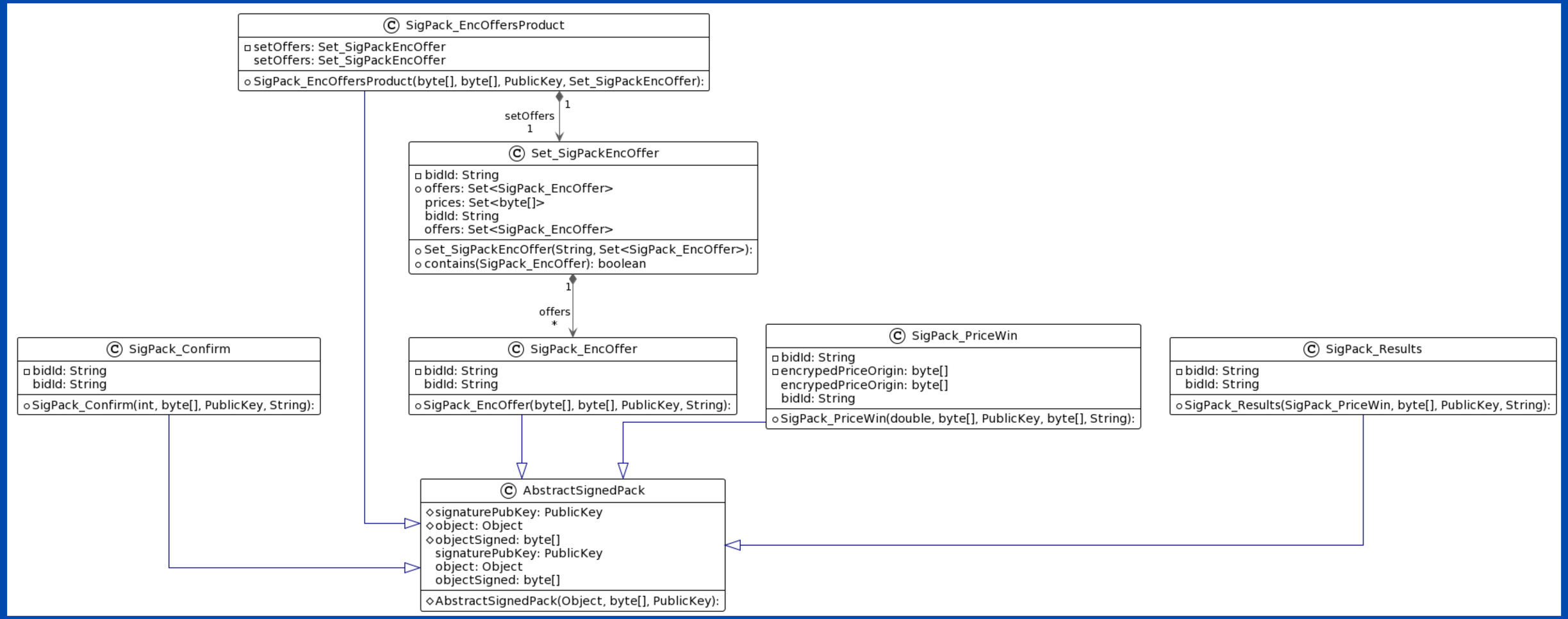
(PlayerStatus)



Seller

Restructuration


SignedEncryptedOfferSet
setSigned: byte[]
set: EncryptedOffersSet
signaturePubKey: PublicKey
signaturePubKey: PublicKey
set: EncryptedOffersSet
setSigned: byte[]
SignedEncryptedOfferSet(Signature, PublicKey, EncryptedOffersSet):
1
set
1
EncryptedOffersSet
bidId: String
offers: Set<EncryptedOffer>
prices: Set<byte[]>
bidId: String
offers: Set<EncryptedOffer>
EncryptedOffersSet(String, Set<EncryptedOffer>):
contains(EncryptedOffer): boolean
1
offers
*
EncryptedOffer
priceSigned: byte[]
price: byte[]
bidId: String
priceSigned: byte[]
signaturePublicKey: PublicKey
bidId: String
price: byte[]
EncryptedOffer(Signature, Offer, PublicKey, PublicKey, String):
EncryptedOffer(Signature, byte[], PublicKey, String):
SignedEncryptedOffersTest
SignedEncryptedOffersTest():
SignedPublicKey
okSigned: byte[]
publicKey: PublicKey
publicKey: PublicKey
okSigned: byte[]
SignedPublicKey(PublicKey, Signature):


SigPack_EncOffersProduct
setOffers: Set_SigPackEncOffer
setOffers: Set_SigPackEncOffer
SigPack_EncOffersProduct(byte[], byte[], PublicKey, Set_SigPackEncOffer):
setOffers
1
1
Set_SigPackEncOffer
bidId: String
offers: Set<SigPack_EncOffer>
prices: Set<byte[]>
bidId: String
offers: Set<SigPack_EncOffer>
Set_SigPackEncOffer(String, Set<SigPack_EncOffer>):
contains(SigPack_EncOffer): boolean
1
offers
*
SigPack_Confirm
bidId: String
bidId: String
SigPack_Confirm(int, byte[], PublicKey, String):
SigPack_EncOffer
bidId: String
bidId: String
SigPack_EncOffer(byte[], byte[], PublicKey, String):
SigPack_PriceWin
bidId: String
encrypedPriceOrigin: byte[]
encrypedPriceOrigin: byte[]
bidId: String
SigPack_PriceWin(double, byte[], PublicKey, byte[], String):
SigPack_Results
bidId: String
bidId: String
SigPack_Results(SigPack_PriceWin, byte[], PublicKey, String):
AbstractSignedPack
signaturePubKey: PublicKey
object: Object
objectSigned: byte[]
signaturePubKey: PublicKey
object: Object
objectSigned: byte[]
AbstractSignedPack(Object, byte[], PublicKey):

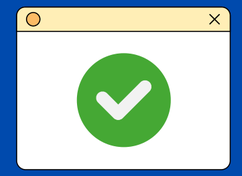
Système de Damgård–Jurik

Refonte graphique

Refonte graphique ?

Animations de chargement

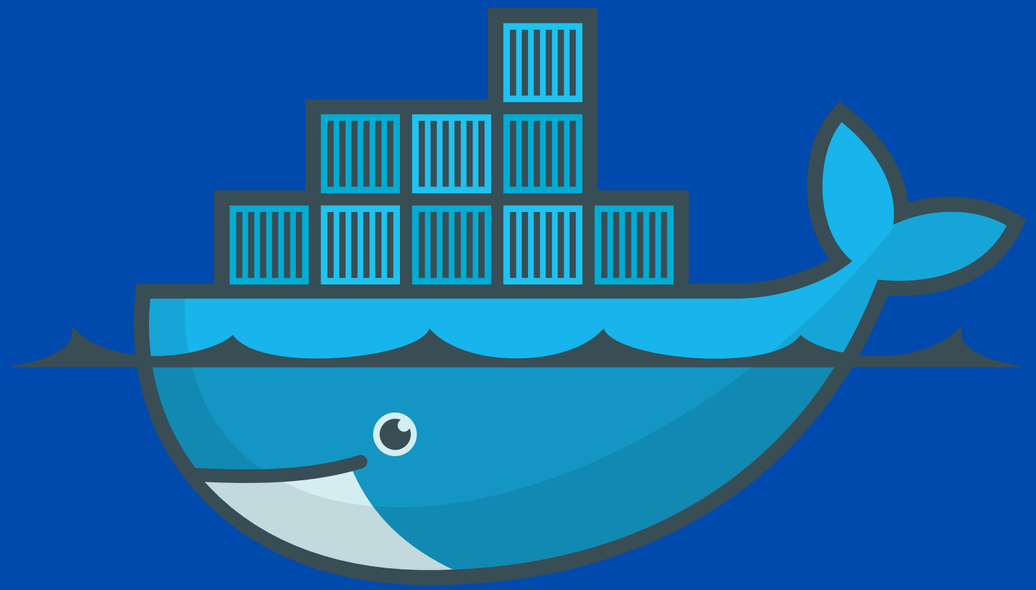
Animations Pop-Ups



Mode Sombre

Activer/désactiver la console

Docker



Objectifs pour la suite :

- Ajuster le nouveau protocole d’enchères et l’algorithme de chiffrement.
- Continuer de restructurer le code et rédiger les tests unitaires.
- Implémenter une nouvelle interface graphique.
- Déploiement sur Docker.
- Attaquer une autre application.


Merci de votre écoute