# AirTransit

Messagerie sécurisée

# Description de la problématique

- Protection de la confidentialité: enjeu majeur d’actualité
- Scandales de divulgation d’informations (Equifax, Facebook, …)
- Milliards de conversations textuelles NON-CHIFFRÉES chaque jour

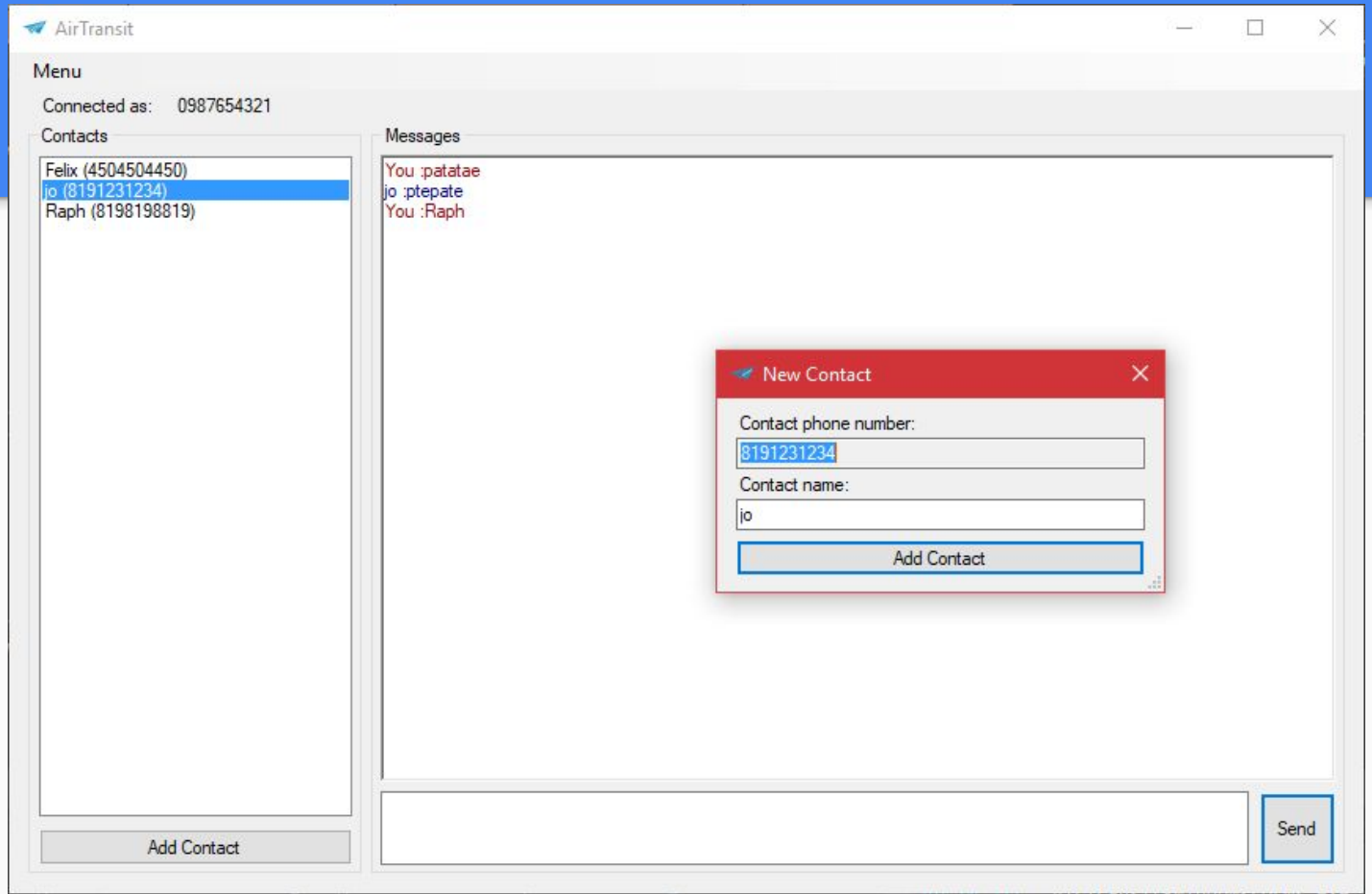

# Solution proposée

Application de messagerie sécurisée

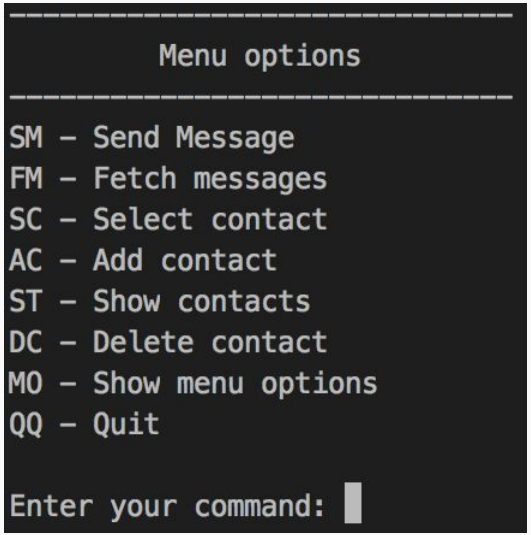
- Portable
- Chiffrement de bout en bout
- Serveur de confiance

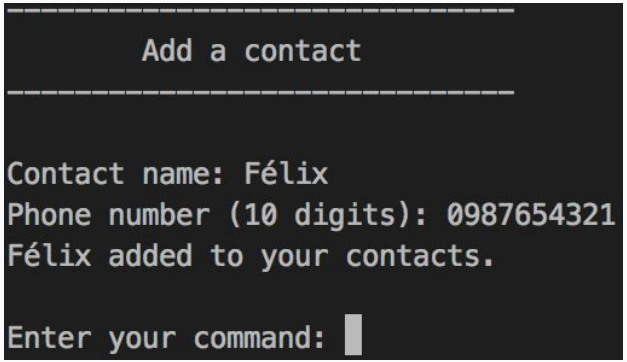
# Interfaces

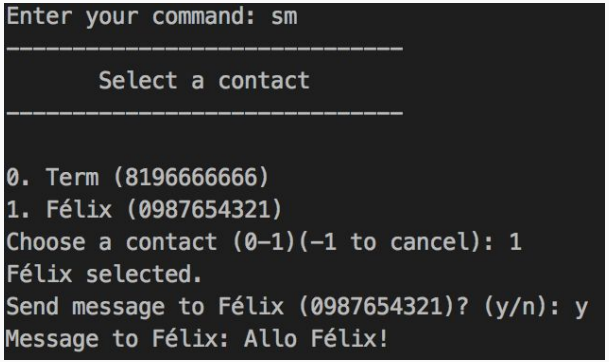
# Windows Forms



# Console


Menu options
SM - Send Message
FM - Fetch messages
SC - Select contact
AC - Add contact
ST - Show contacts
DC - Delete contact
MO - Show menu options
QQ - Quit
Enter your command:


Add a contact
Contact name: Félix
Phone number (10 digits): 0987654321
Félix added to your contacts.
Enter your command:


Enter your command: sm
Select a contact
0. Term (8196666666)
1. Félix (0987654321)
Choose a contact (0-1)(-1 to cancel): 1
Félix selected.
Send message to Félix (0987654321)? (y/n): y
Message to Félix: Allo Félix!

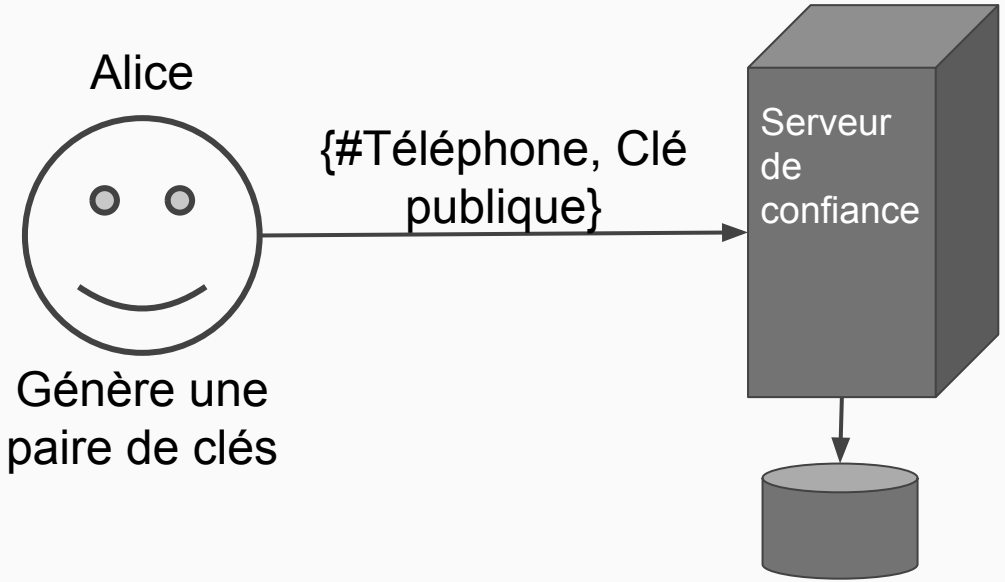
# Chiffrement

# Chiffrement

- Asymétrique (RSA)
- Serveur de confiance pour l’échange de clés publiques et stockage des messages chiffrés
- Signature SHA-256
- HTTPs

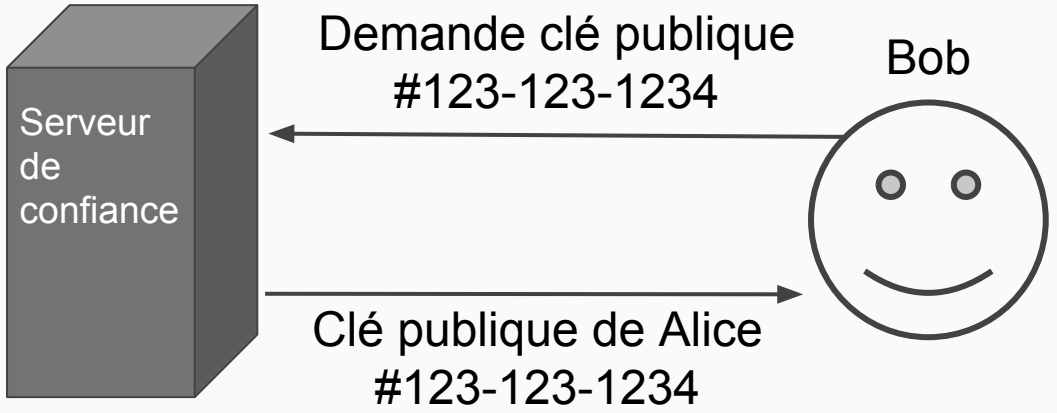
# Authentification

#123-123-1234



# Communication

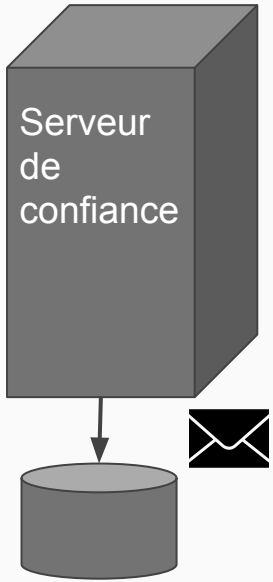
#123-123-1234

# Communication

#123-123-1234

Alice



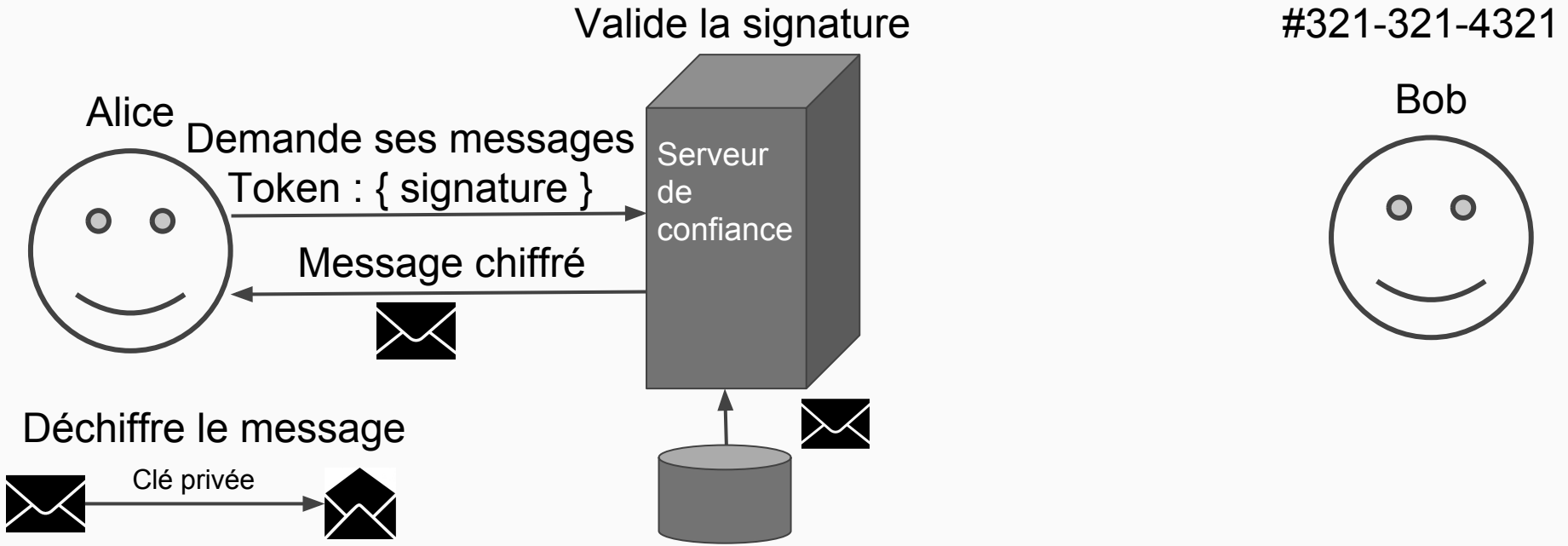

Message chiffré

#321-321-4321

Bob

Signe avec sa clé privée, chiffre avec la clé publique

# Communication



# Communication

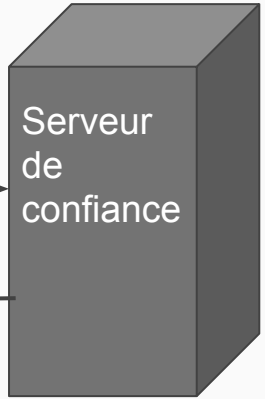
Message contient la signature de Bob

#321-321-4321

Bob

Alice

Demande clé publique de Bob



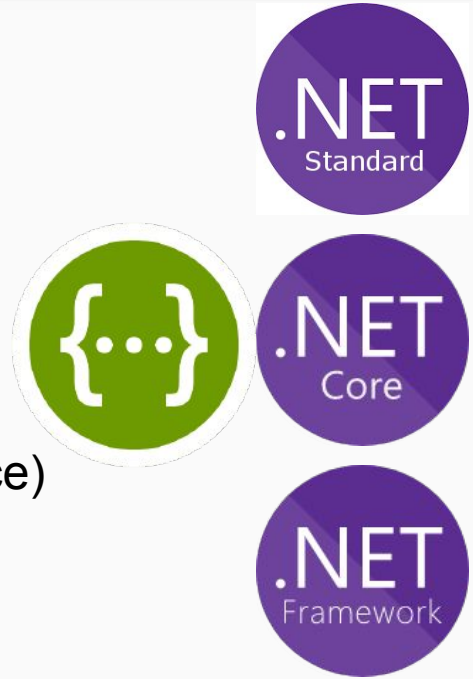

Clé publique de Bob

Vérifie la signature à l'aide de la clé publique de Bob (#321-321-4321)

Invalide -> Rejette le message

# Architecture logicielle

- Injection de dépendances
- Tests unitaires
- Séparation des responsabilités (modulaire)
  - Client
    - Interface console
    - Interface graphique
    - Coeur (chiffrement, communication, persistence)
  - Serveur de confiance
- Multi-plateforme



“Je suis heureux que mes informations soient protégées avec cette merveilleuse application”

- Ancien utilisateur Facebook

Nous n’avons pas accès à vos informations privées, donc nous ne les vendons pas!

# Conclusions

- Garanties réussies
  - Confidentialité
  - Intégrité
  - Authentification
- Limitation
  - Non-répudiation
  - Autorité de confiance

# Merci!

Contactez-nous:

info@airtransit.ca
www.airtansit.ca

https://github.com/Wingjam/AirTransitClient--E2E-Encrypted-Chat

https://github.com/Wingjam/AirTransitServer--E2E-Encrypted-Chat