



Cloud Nord

2024



**Confidentialité des
données sur les offres
SaaS EDA**

Agenda



EDA & Contexte
projet cloud AXA



Principe général
démos avec spring-kafka



Vault centralisé
principe et démo spring-kafka



avec pulsar
et avec un vault centralisé

Qui suis-je ?



Guillaume Dufrêne

/ Principal Software Engineer
Axa en France



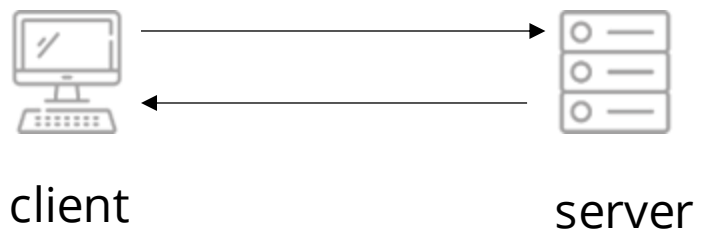
Développeur
Enseignant



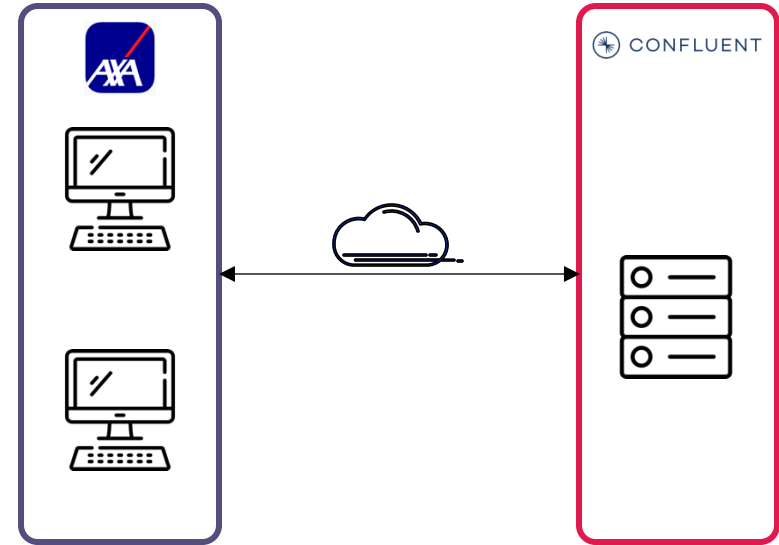
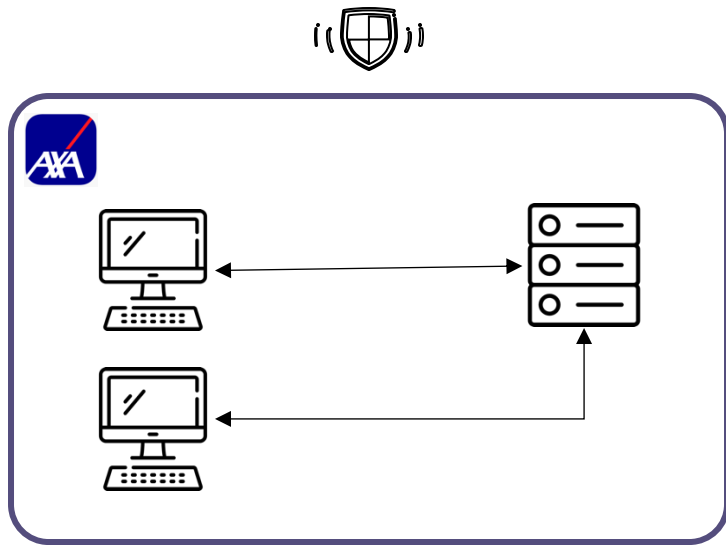
Pilote planeur
Instructeur



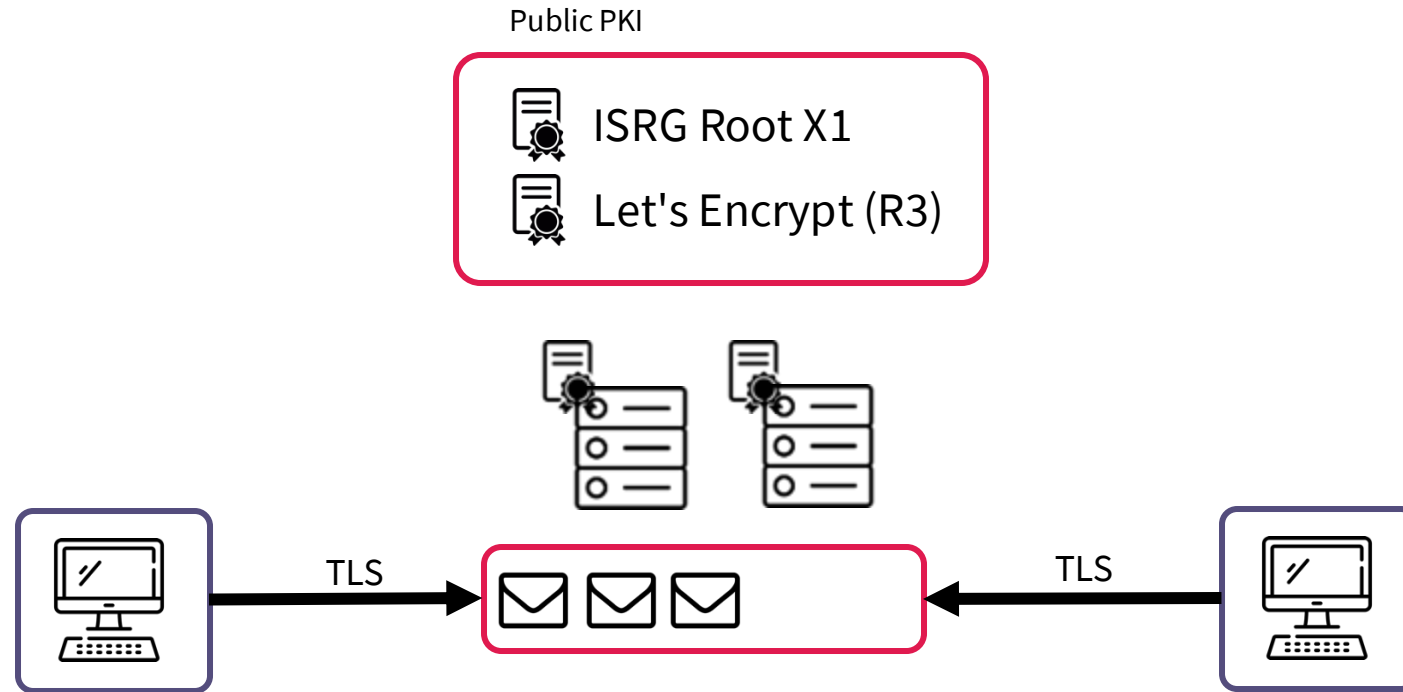
Board Game Geek



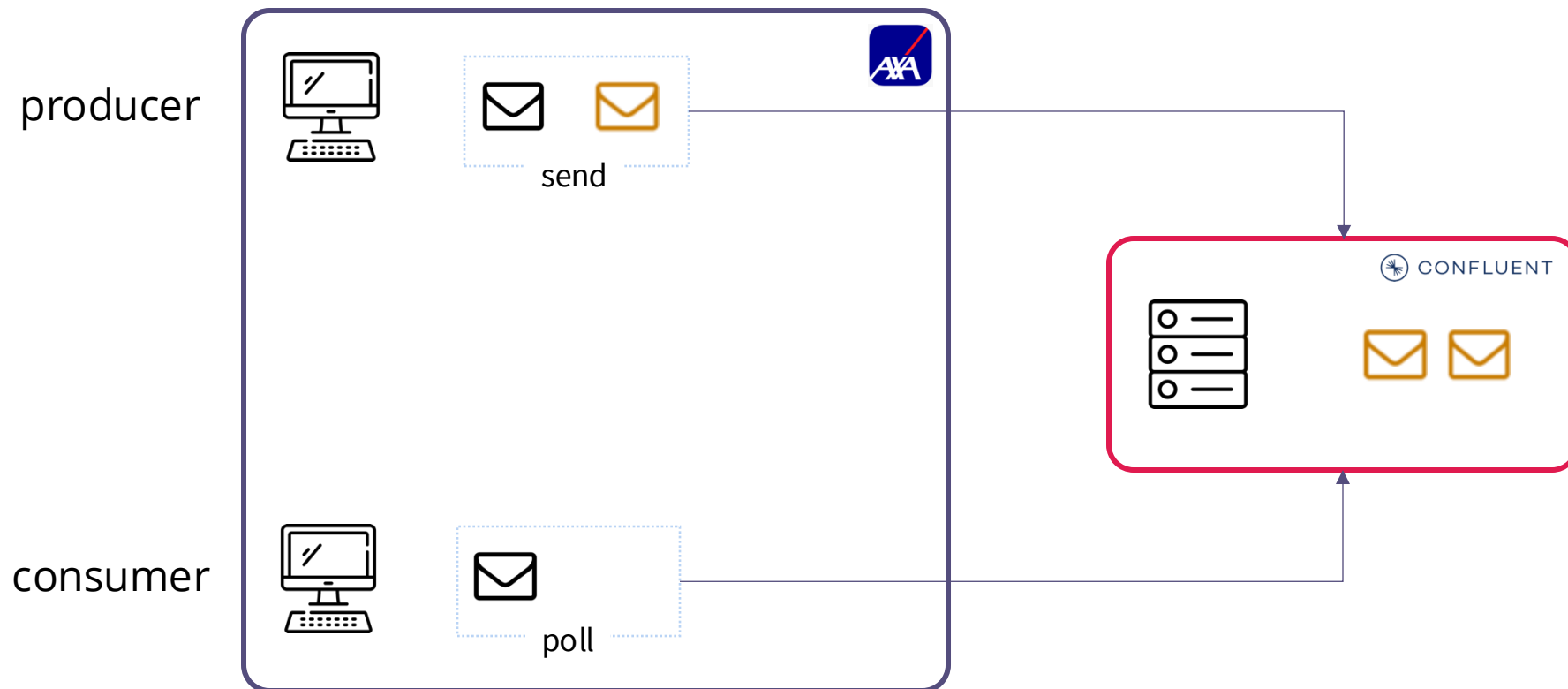
/ To the Cloud



/ TLS



/ Chiffrement



/ AES



[AES Explained \(Advanced Encryption Standard\)](#)



[AES GCM \(Advanced Encryption Standard in Galois Counter Mode\)](#)

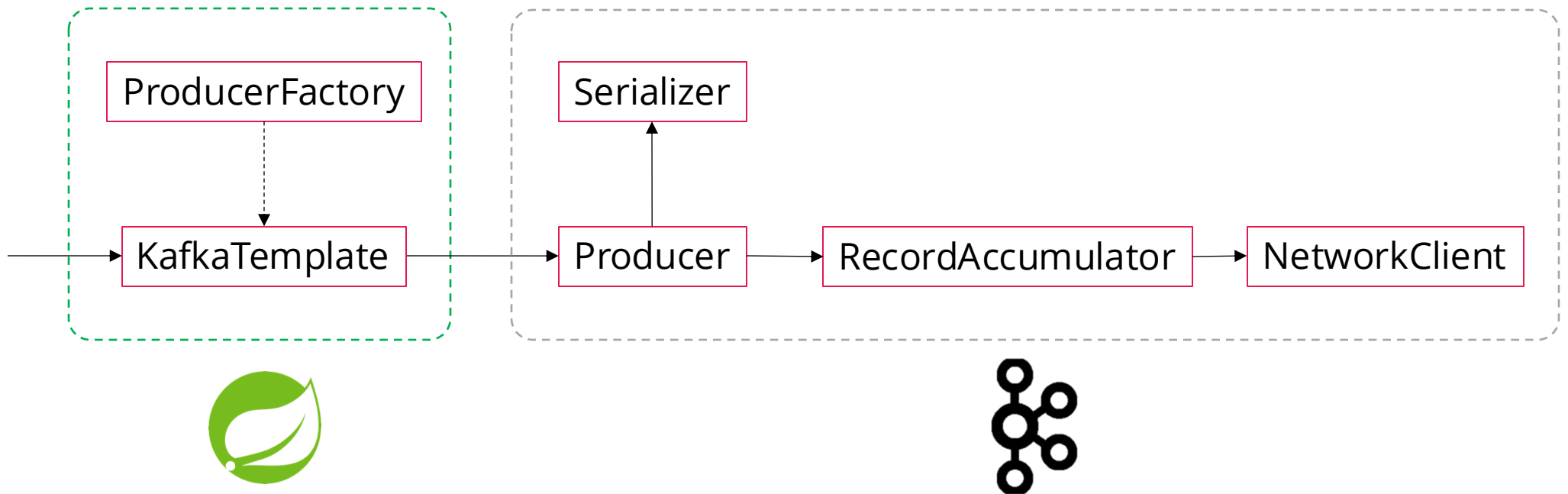


[@Computerphile](#)

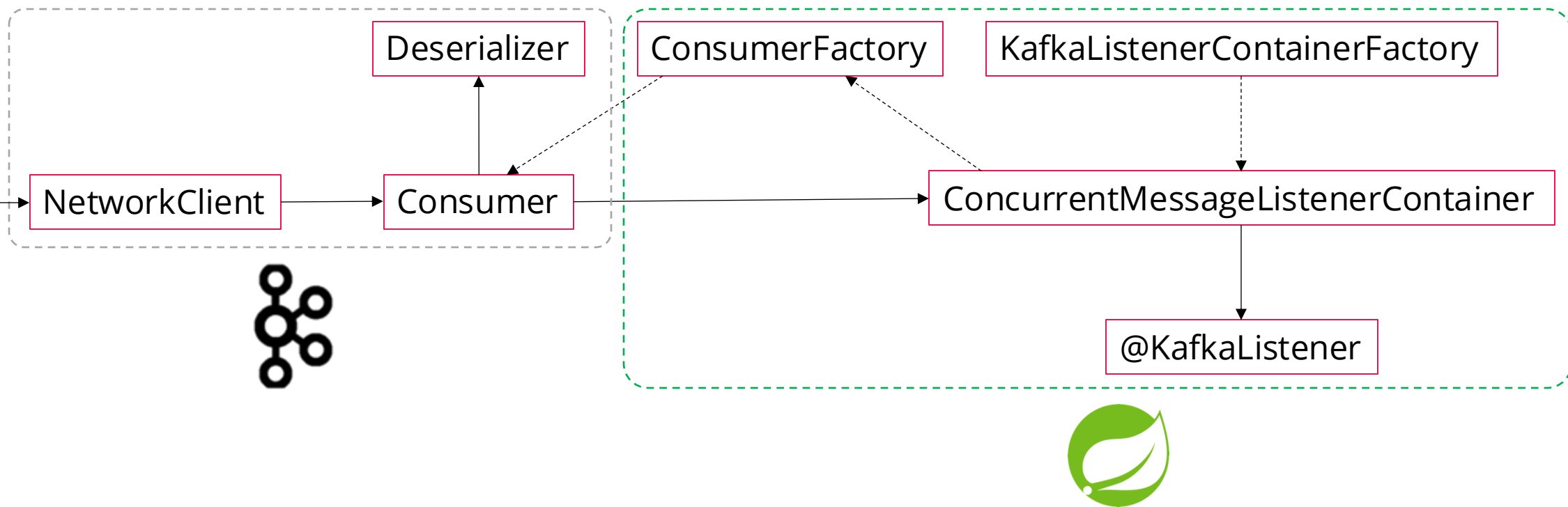
/ Demo 1

- Implémentation naïve avec spring-kafka

/ Production Kafka



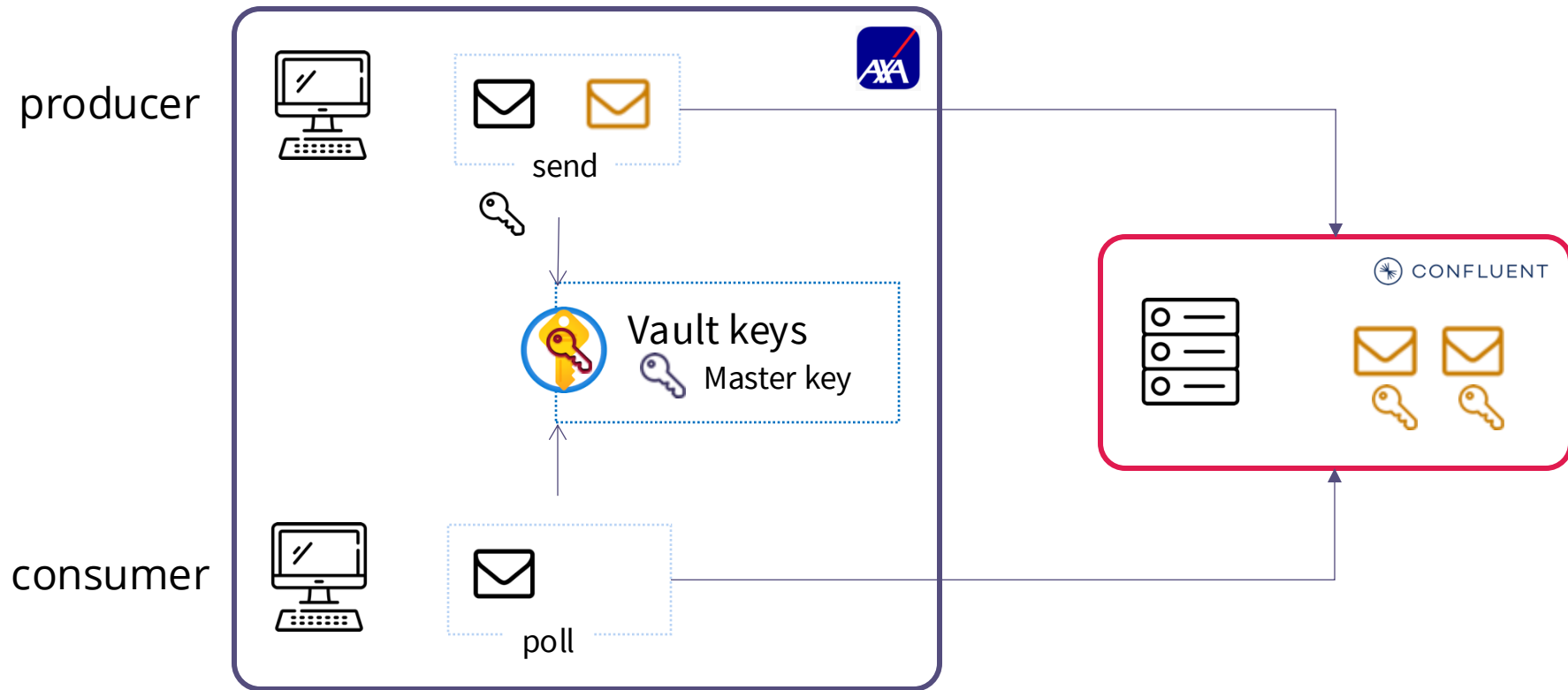
/ Consommation Kafka



/ Démo 2

- Chiffrement-Déchiffrement d'objets JSON
- Utilisation de Serializer / Deserializer

/ Porte clé centralisé



/ Démo 3

- Mock d'un coffre de clés centralisées
- Utilisation du vault centralisé
- Rotation des clés de session / clés centrales

/ Apache Pulsar



Cloud-Native, Distributed Messaging and Streaming

Apache Pulsar is an open-source, distributed messaging and streaming platform built for the cloud.

- Bookkeeper
- Géo-réplication
- Consumer : mode de souscription
- Support du chiffrement bout en bout

/ Apache Pulsar

DEVOXXTM FRANCE



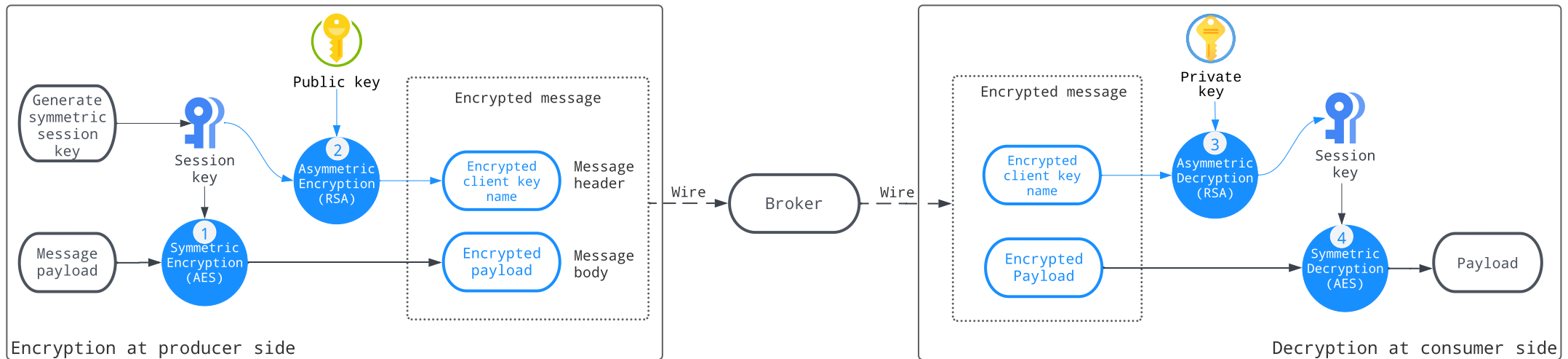
**Apache Pulsar :
enfin une alternative à Kafka ?**

Julien Jakubowski



https://youtu.be/jb2-P_Z3FG0

/ E2E Encryption



<https://pulsar.apache.org/docs/3.2.x/security-encryption/>

/ E2E Encryption

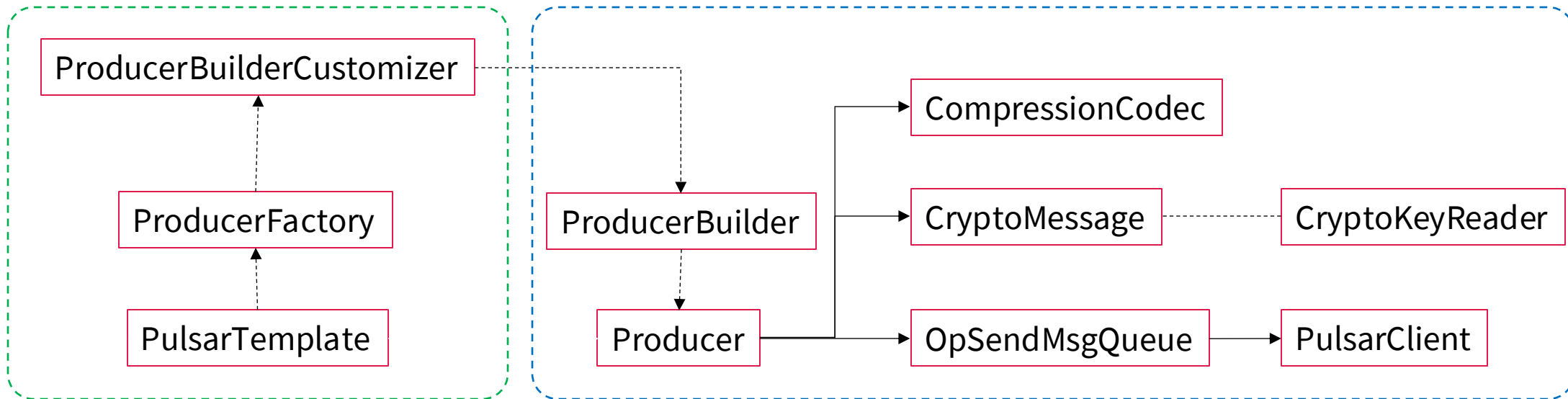
CryptoKeyReader

```
EncryptionKeyInfo getPublicKey(String keyName, Map<String, String> metadata);  
EncryptionKeyInfo getPrivateKey(String keyName, Map<String, String> metadata);
```

EncryptionKeyInfo

```
public class EncryptionKeyInfo {  
  
    private Map<String, String> metadata;  
    private byte[] key;  
    // ...  
}
```

/ production pulsar



Avec pulsar

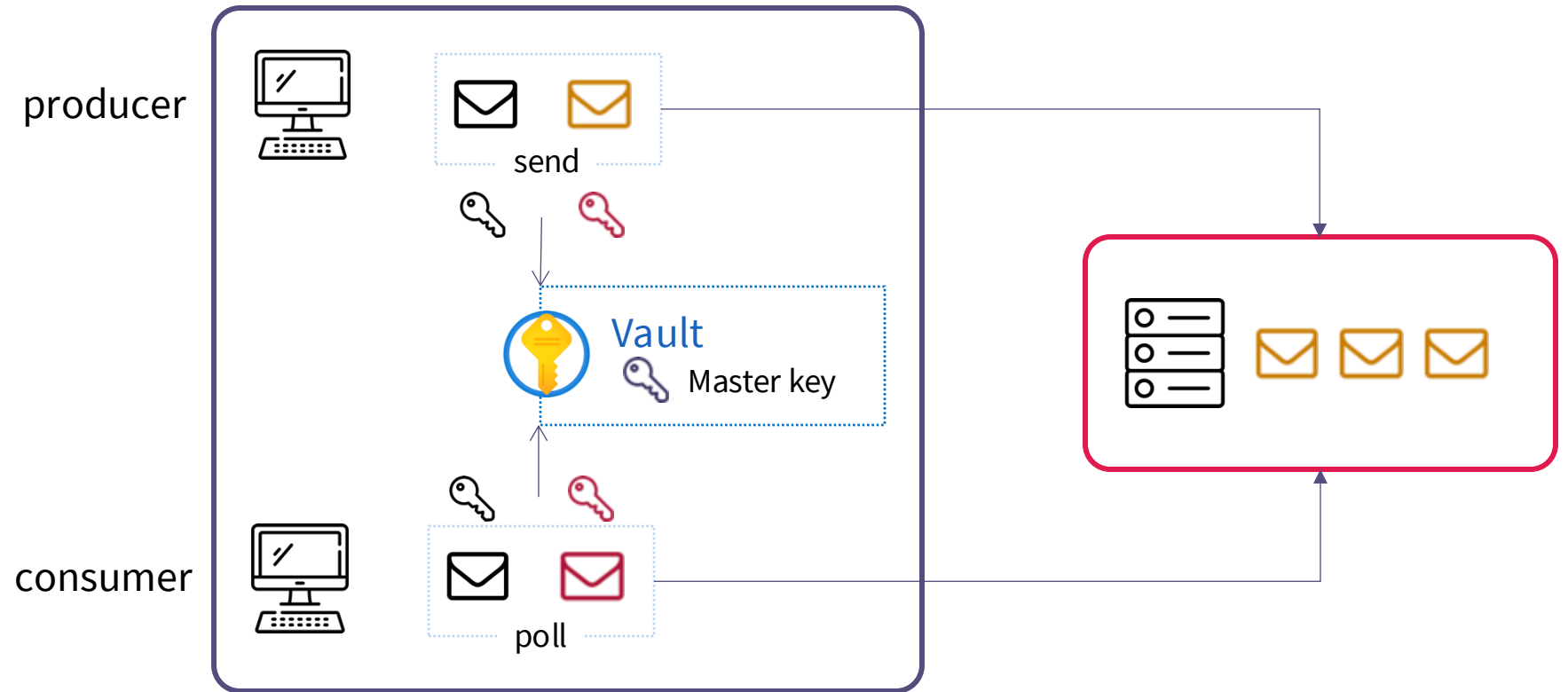


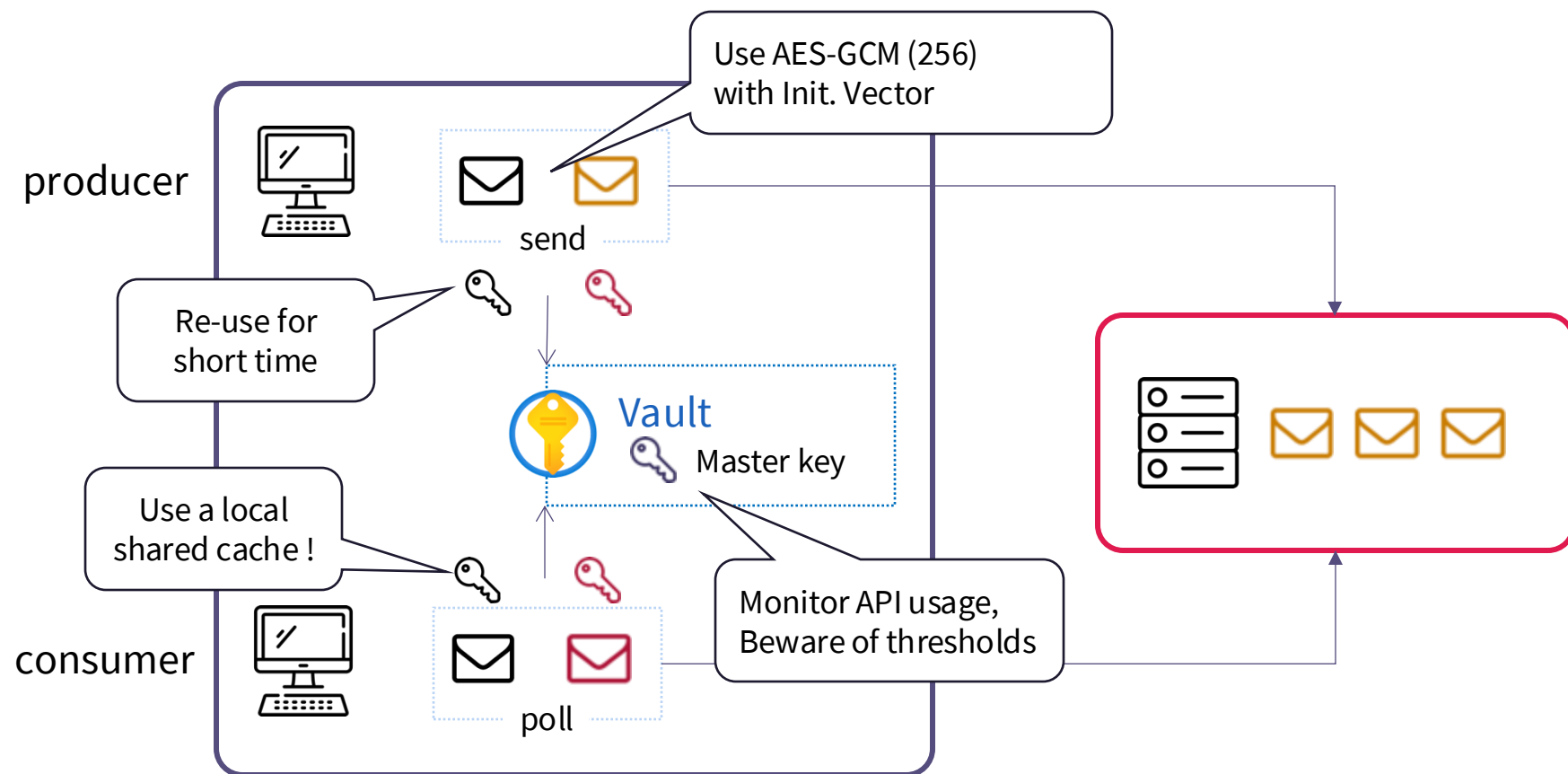
/ DEMO 4

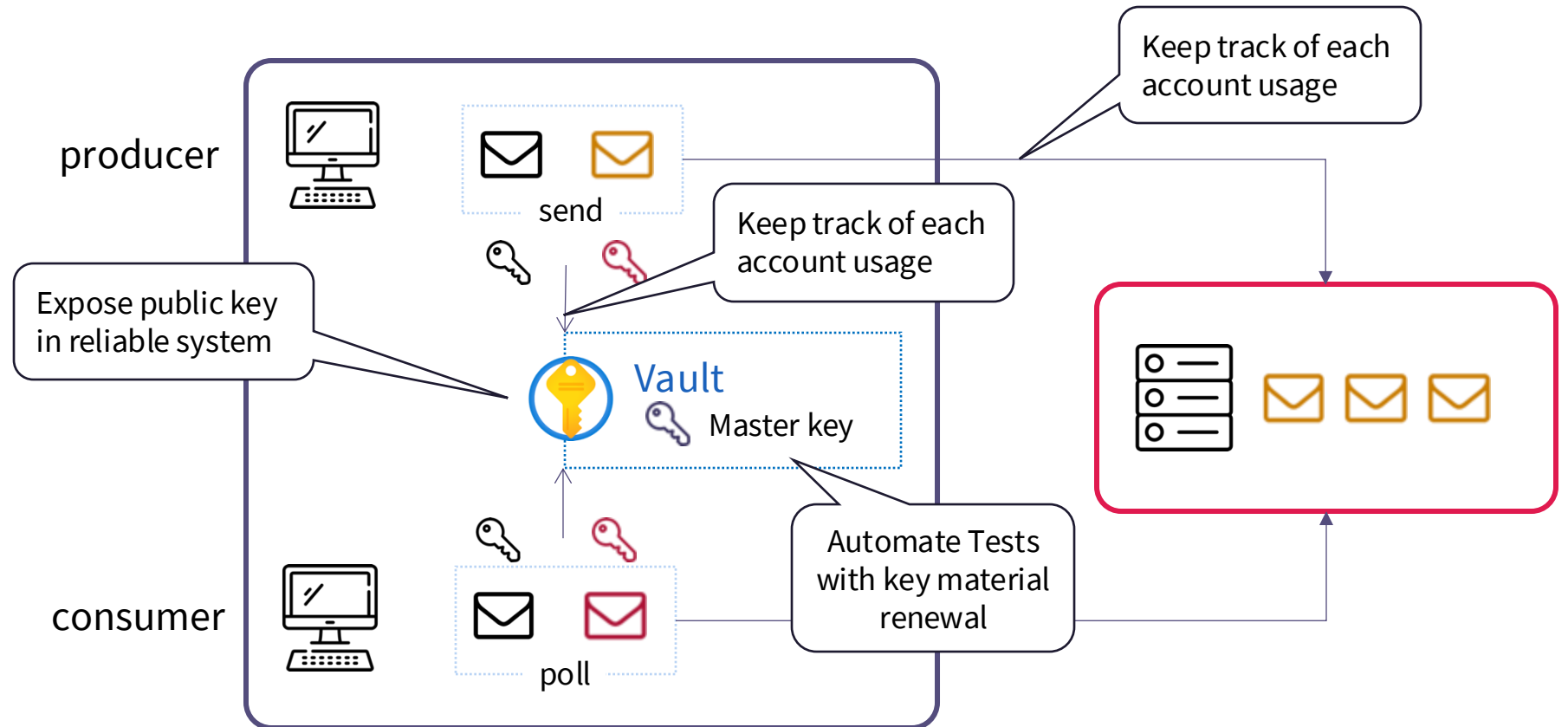
- Chiffrement bout en bout avec spring-pulsar



TakeAway - Conclusion







/ Merci



Confidentialité des données sur les offres SaaS EDA



<https://github.com/gdufrene>