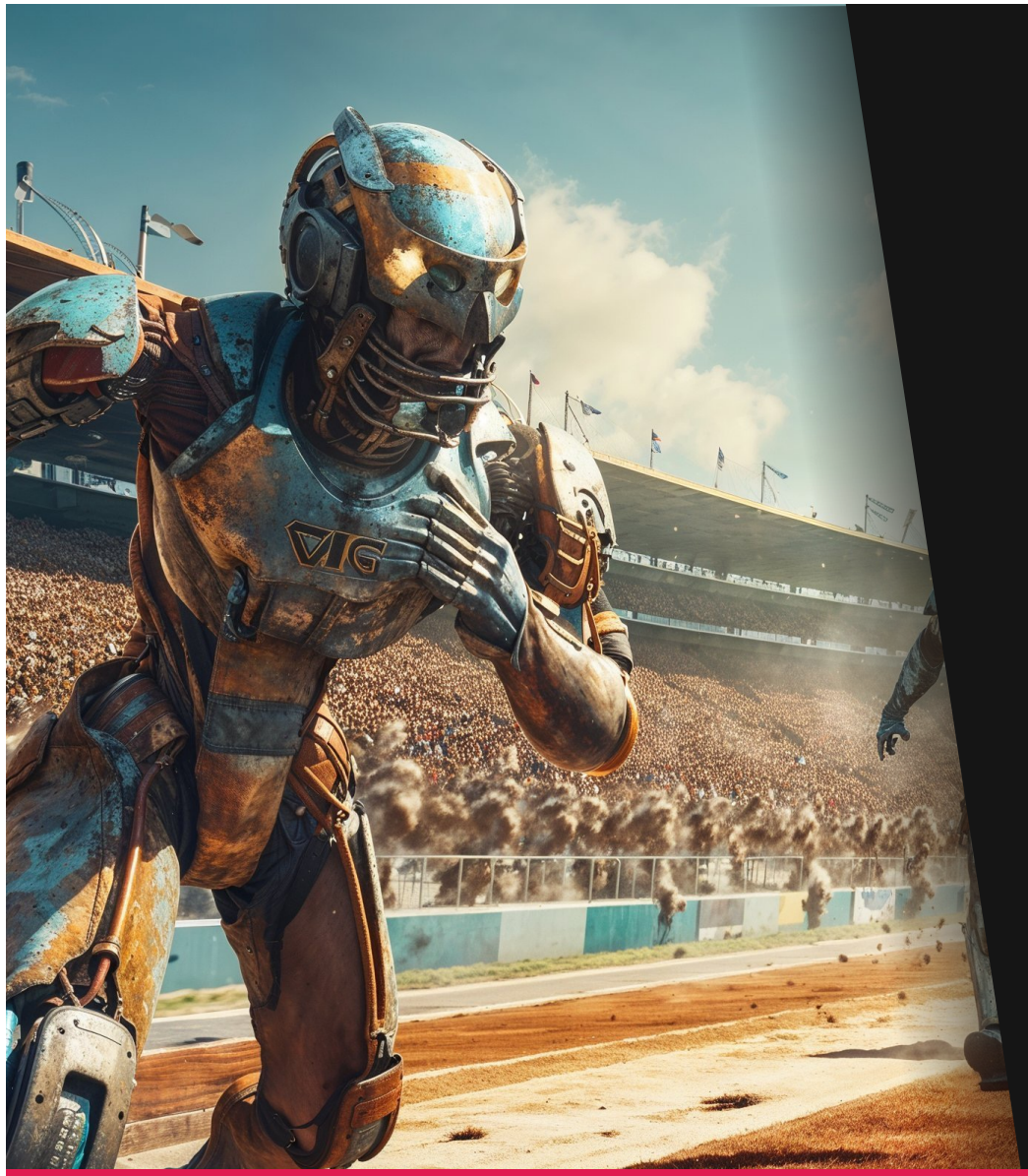


DEVOXX FRANCE 2024

Thematic

SECURITY

WARMUP

CONFIDENTIALITÉ DES DONNÉES SUR LES OFFRES SAAS KAFKA OU PULSAR

/ CHIFFREMENT DE BOUT EN BOUT

Guillaume DUFRÊNE

SUMMARY

/ SUMMARY

1. EDA & CONTEXTE
   projet cloud AXA
2. PRINCIPE GÉNÉRAL
   démos avec spring-kafka
3. VAULT CENTRALISÉ
   principe et démo spring-kafka
4. AVEC PULSAR
   et avec un vault centralisé

ABOUT ME

Guillaume Dufrêne

/ Staff Engineer @ AXA France

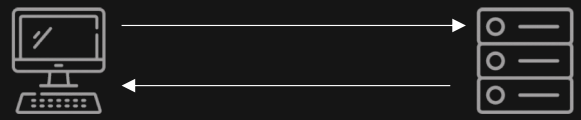
Développeur
Enseignant

Pilote planeur
Instructeur

Board Game Geek

/ EDA

CONTEXTE



client

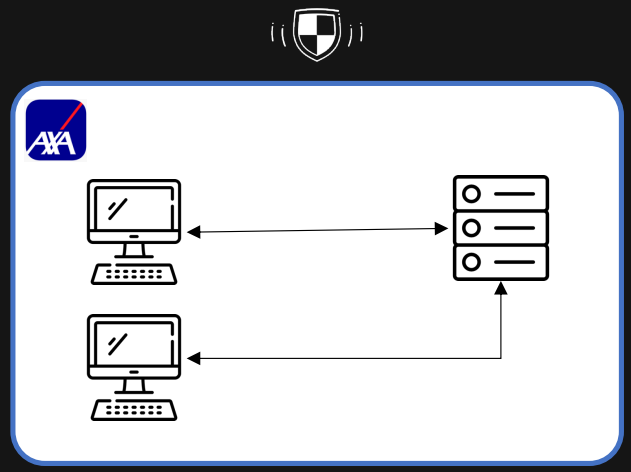
server

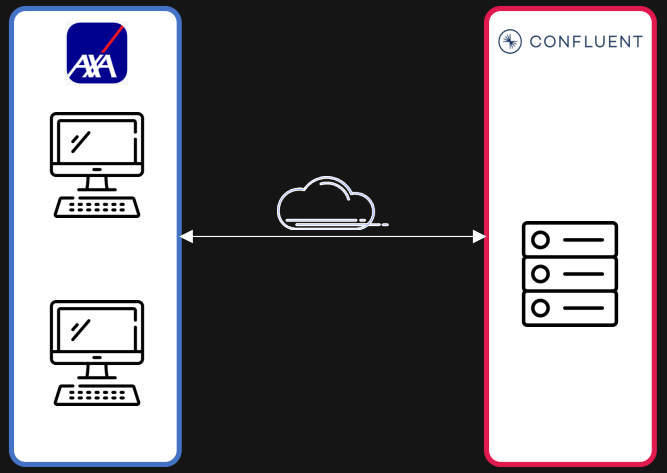
producer

consumer

CONTEXTE

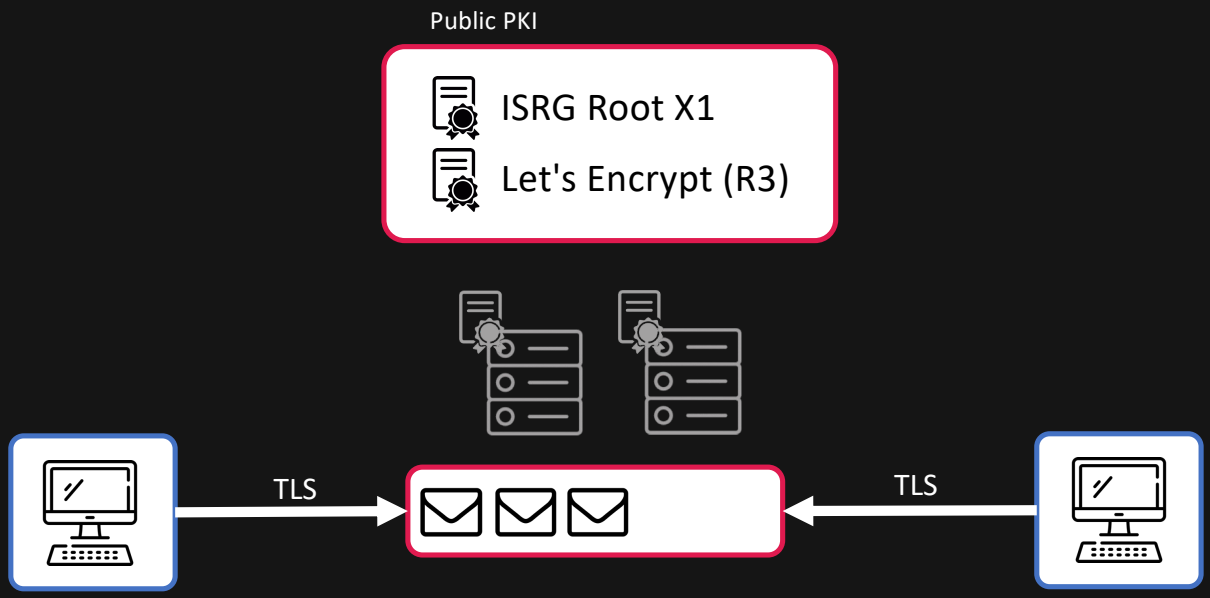
/ TO THE CLOUD





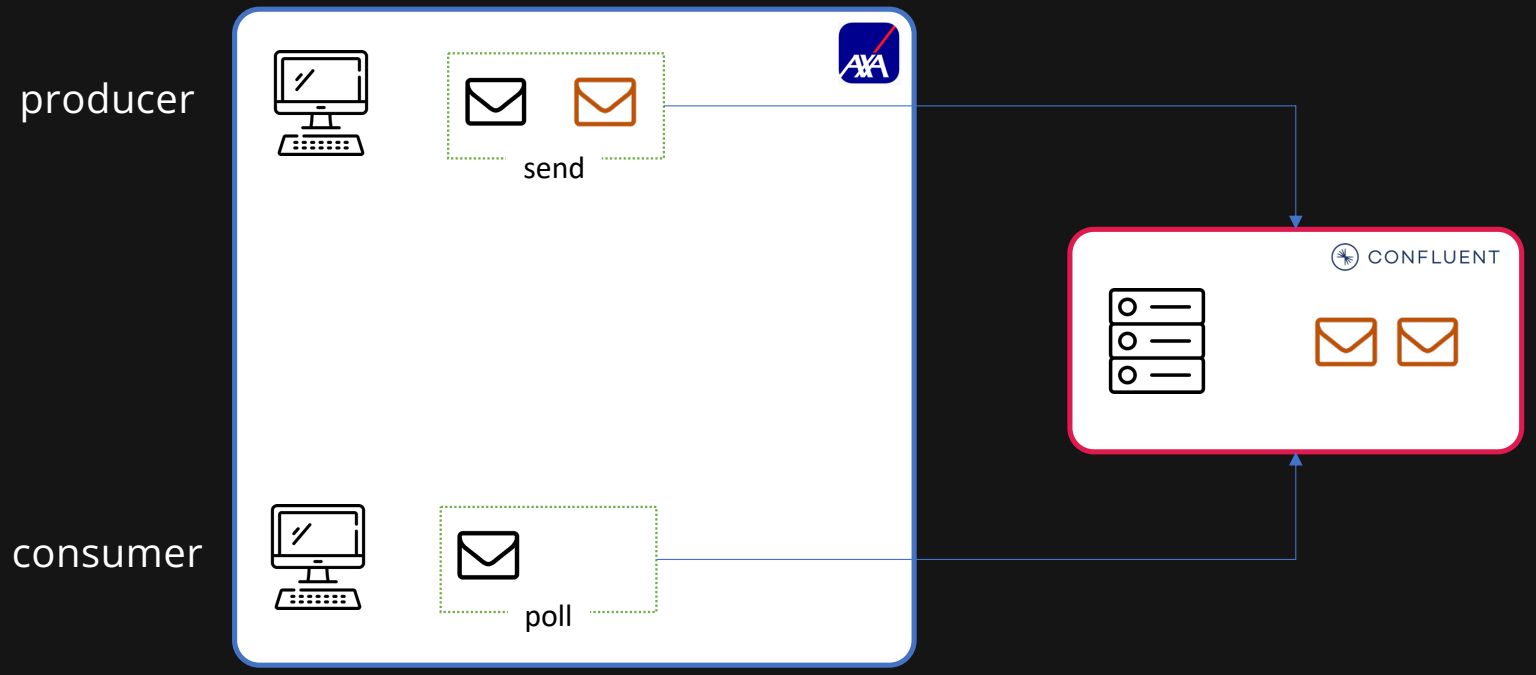
/ TLS

PRINCIPE



/ CHIFFREMENT

PRINCIPE



/ AES ?

PRINCIPE

[AES Explained (Advanced Encryption Standard)]

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

[@Computerphile]

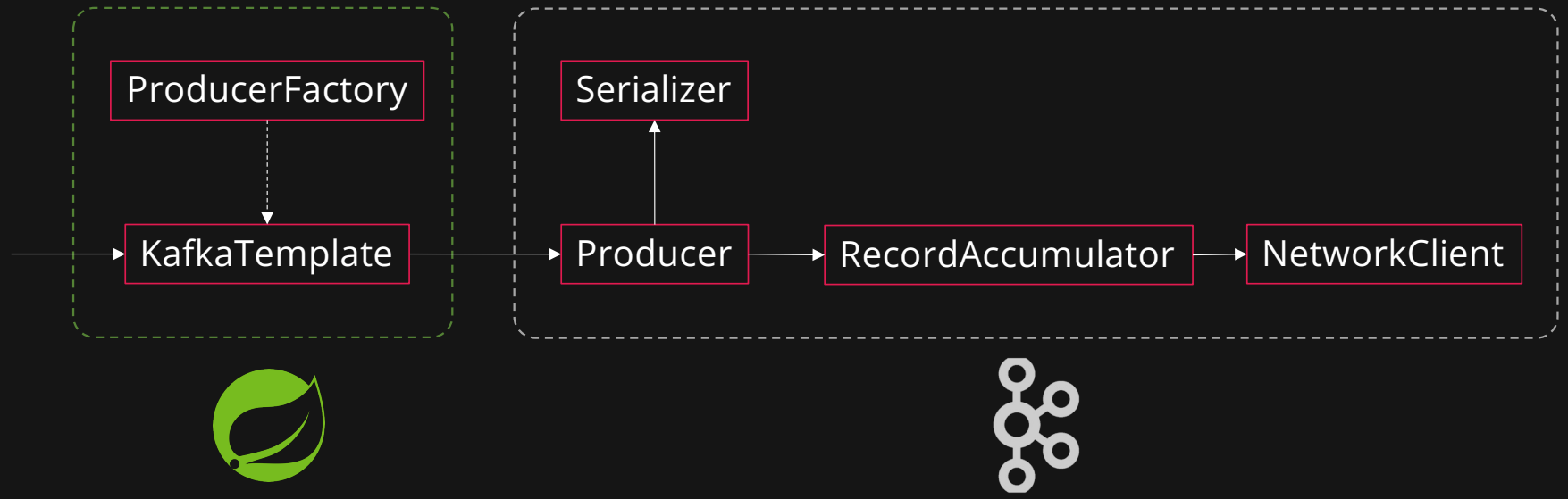
/ DEMO 1

- Implémentation naïve avec spring-kafka

PRINCIPE

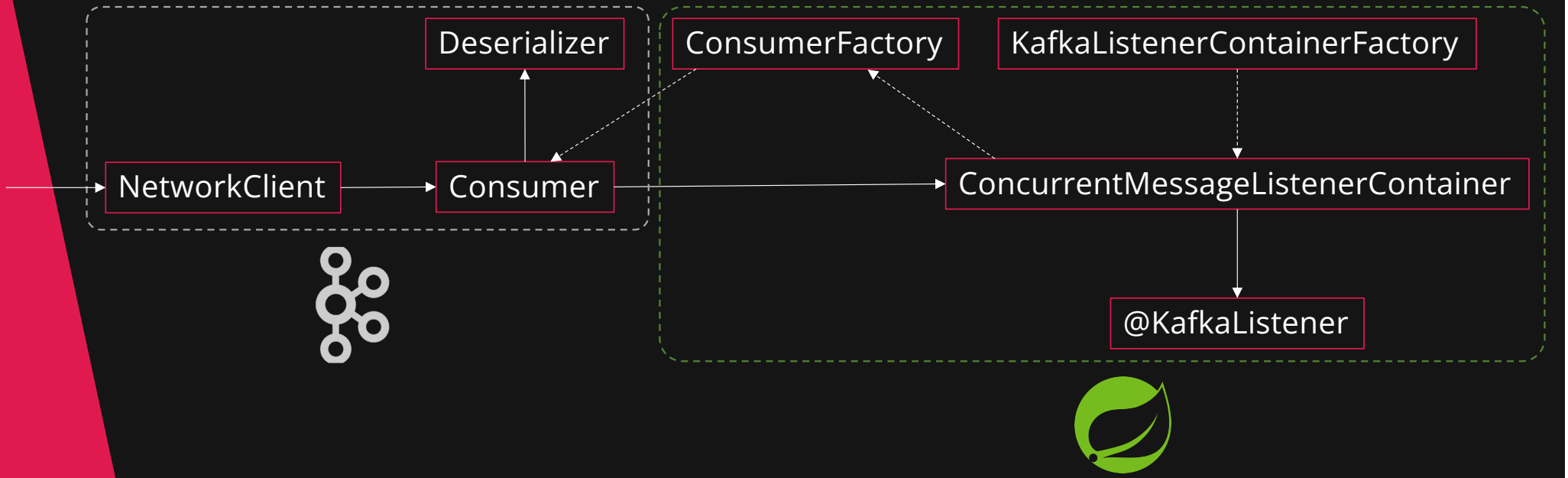
/ PRODUCTION KAFKA

PRINCIPE



/ CONSOMMATION KAFKA

PRINCIPE



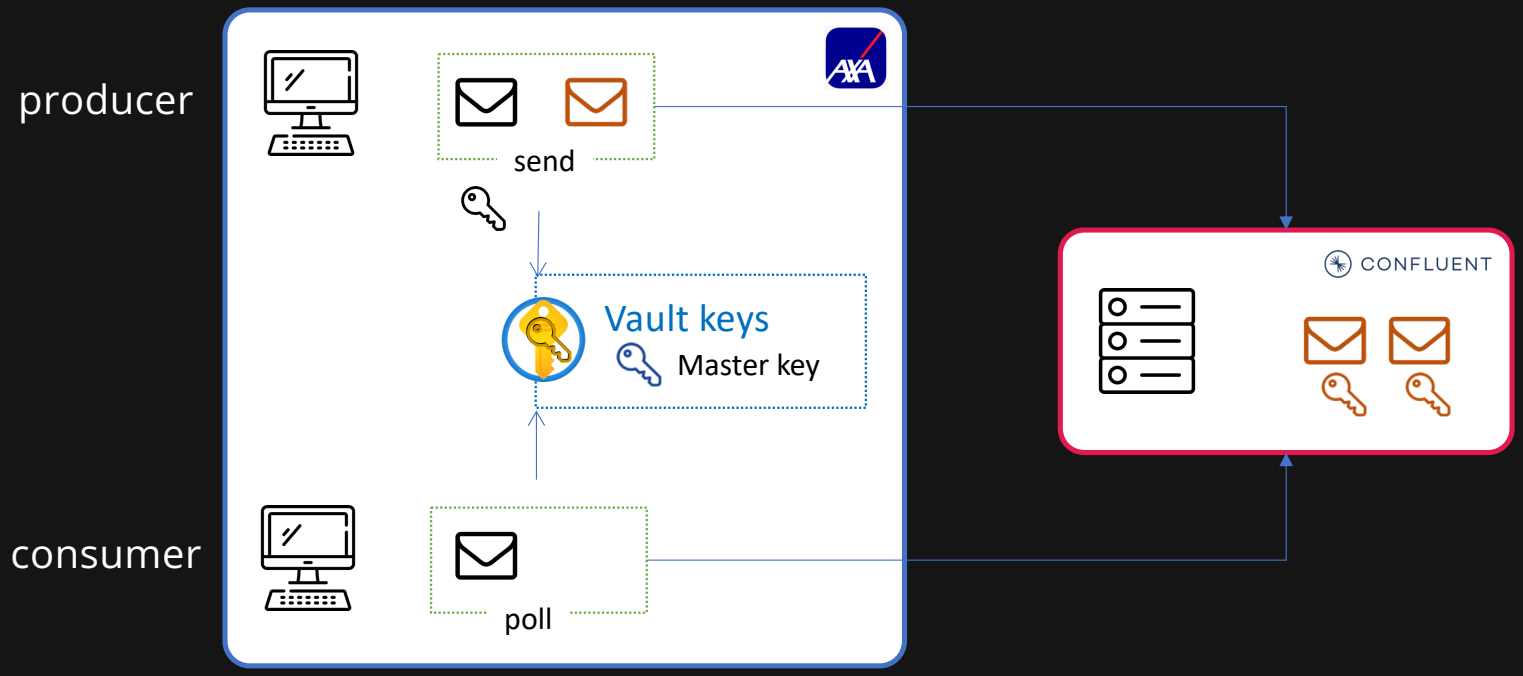
/ DEMO 2

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

PRINCIPE

/ PORTE CLÉ CENTRALISÉ

VAULT CENTRALISÉ



/ DEMO 3

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

VAULT CENTRALISÉ

/ APACHE PULSAR

Cloud-Native, Distributed Messaging and Streaming

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

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

AVEC PULSAR

/ APACHE PULSAR

DEVOXX FRANCE

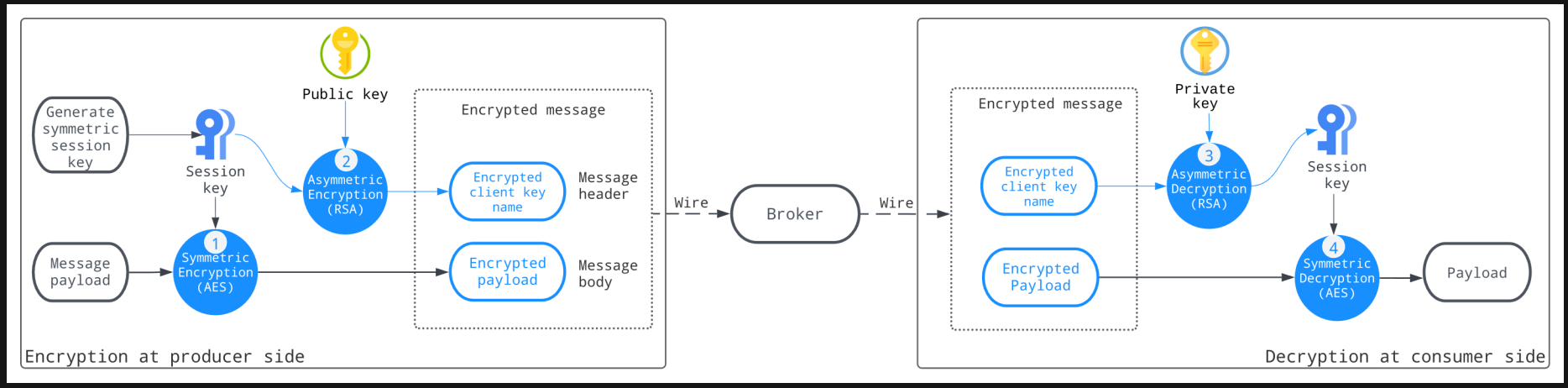
Apache Pulsar : enfin une alternative à Kafka ?

Julien Jakubowski

Thursday 10:30 - 11:15
Neuilly 252AB

AVEC PULSAR

/ E2E ENCRYPTION



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

AVEC PULSAR

/ E2E ENCRYPTION

CryptoKeyReader

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

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

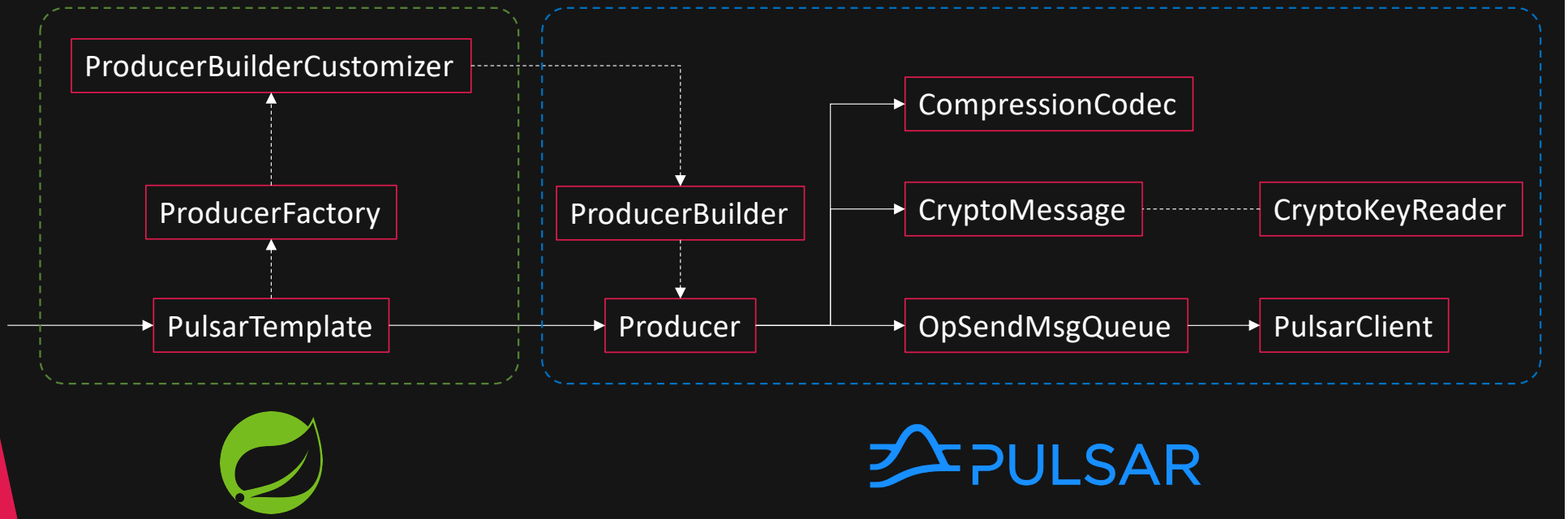
EncryptionKeyInfo

```
public class EncryptionKeyInfo {


    private Map<String, String> metadata;
    private byte[] key;
    // …
```

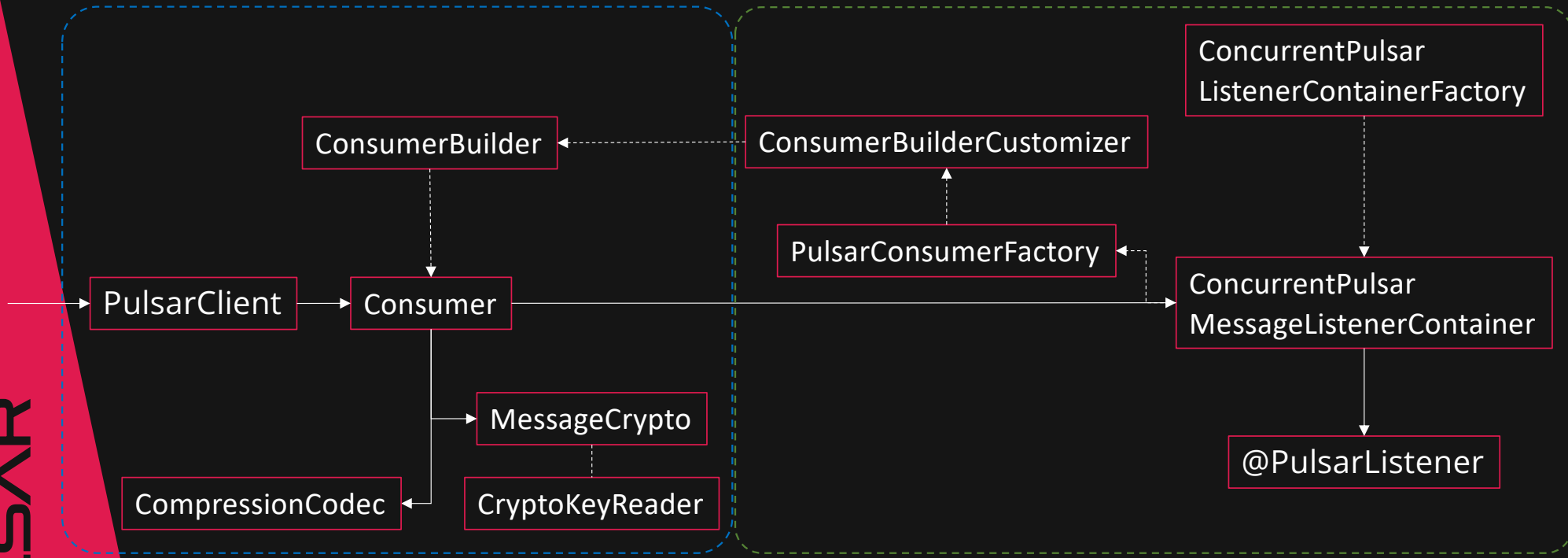
AVEC PULSAR

/ PRODUCTION PULSAR



AVEC PULSAR

/ CONSOMMATION PULSAR



AVEC PULSAR

PULSAR

/ DEMO 4

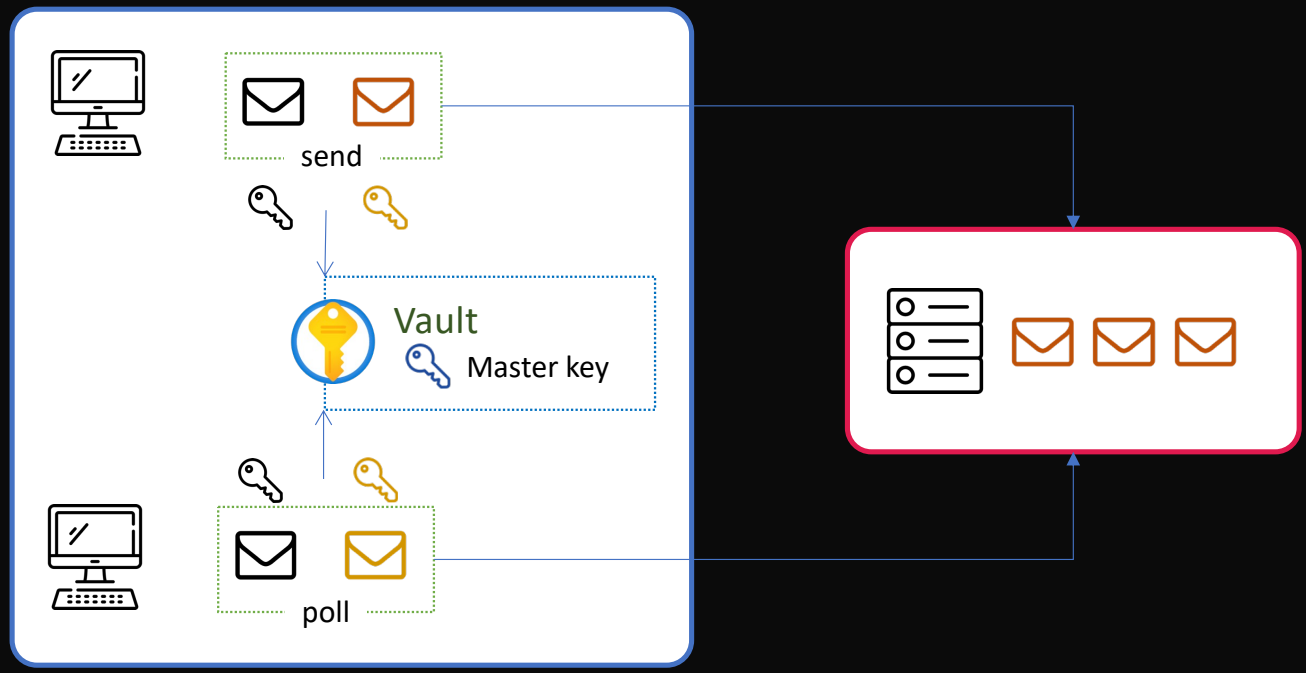
- Chiffrement bout en bout avec spring-pulsar

VAULT CENTRALISÉ

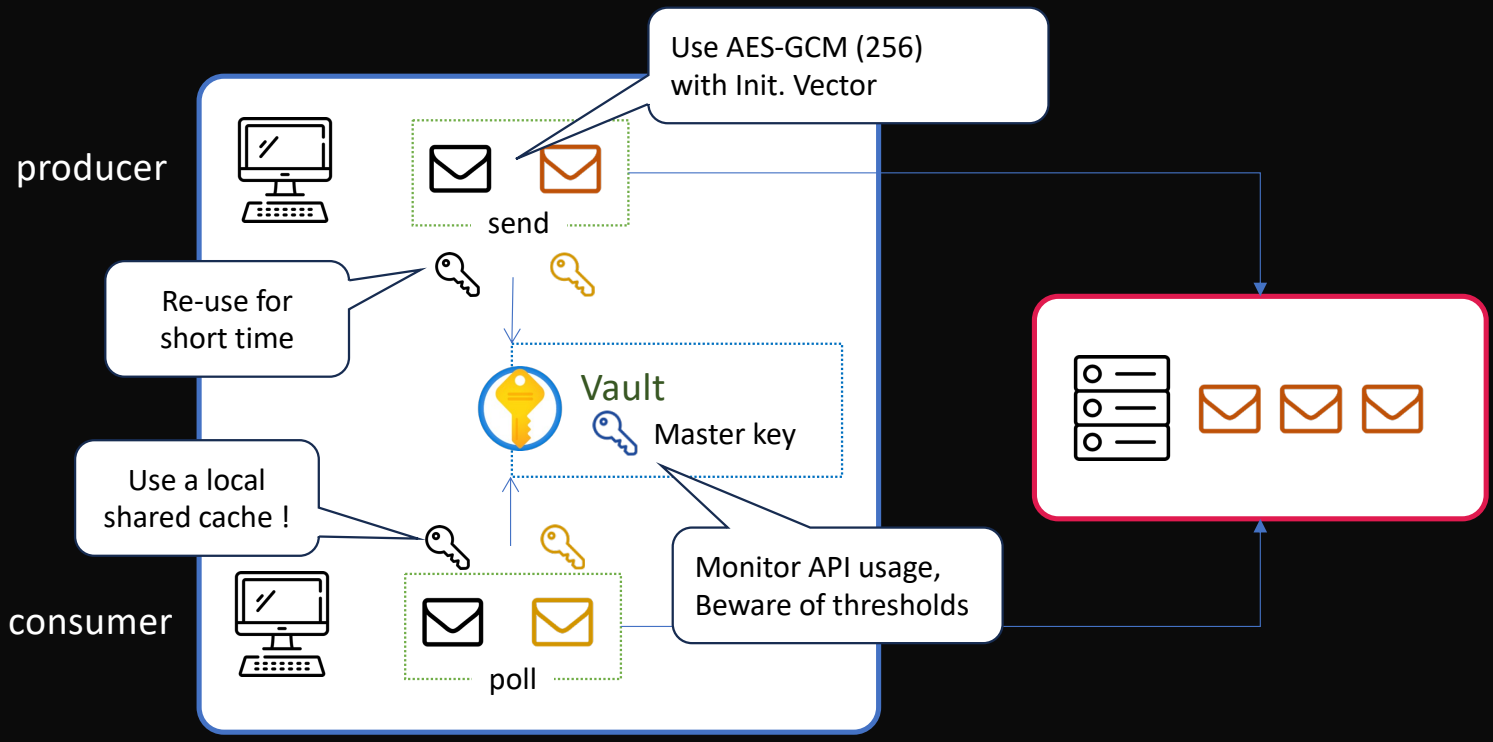
DEVOXX FRANCE 2024

SUMMARY GUIDE

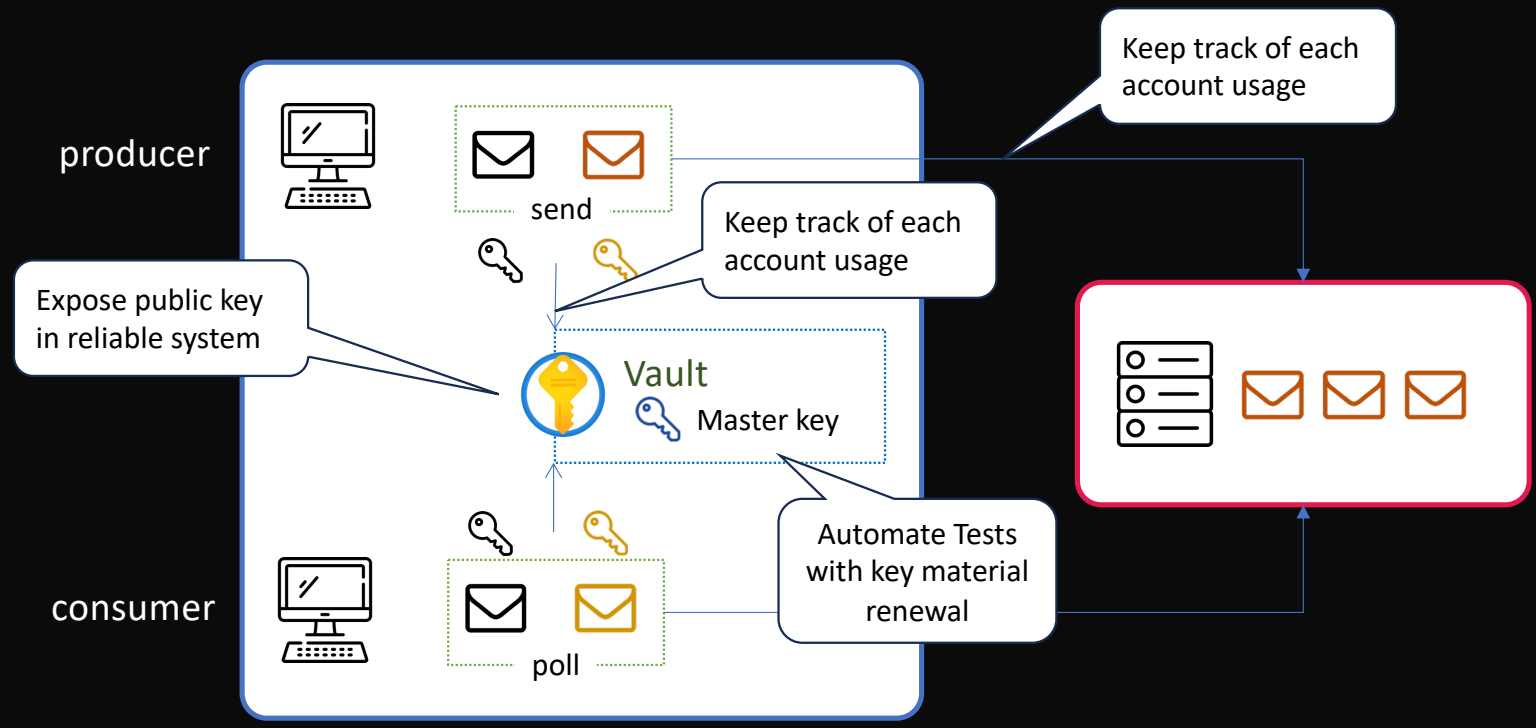
/ RÉSUMÉ



/ CONSEILS


Use AES-GCM (256)
with Init. Vector
producer
send
Re-use for
short time
Vault
Master key
Use a local
shared cache !
Monitor API usage,
Beware of thresholds
consumer
poll

/ CONSEILS


producer
send
Keep track of each account usage
Keep track of each account usage
Expose public key in reliable system
Vault
Master key
Automate Tests with key material renewal
consumer
poll

THANKS FOR WATCHING

DEVOXX FRANCE 2024

Confidentialité des données
sur les offres SaaS Kafka ou Pulsar

https://github.com/gdufrene/devoxx2024


THANKS
FOR WATCHING
DEVOXX FRANCE 2024
Confidentialité des données
sur les offres SaaS Kafka ou Pulsar
https://github.com/gdufrene/devoxx2024
AXA