MOUSTASS VIDÉO

Messagerie vidéo ultra-sécurisée pour le secteur financier à Maurice.

Conception QAW (Quality Architecture Workshop)

Cette QAW définit les qualités attendues en scénarios mesurables, puis relie ces scénarios aux choix architecturaux et aux tests.

1- Objectif du QAW

Le QAW a pour but d'identifier, formaliser et prioriser les attributs de qualité critiques du système Moustass Vidéo afin de guider les décisions d'architecture (C4, ADR, sécurité, DevSecOps).

Dans ce projet, le QAW permet de :

- Répondre aux risques d'écoutes illégales
- Garantir la conformité réglementaire (RGPD, DPA)
- Justifier les choix cryptographiques et microservices

2- Parties prenantes (Stakeholders)

Stakeholder	**Attentes clés**
Expéditeur	Confidentialités, preuve d'envoi
Destinataire	Authenticité, intégrité du message
Equipe sécurité	Zero Trust, E2EE, audit
Admin sécurité	Audit, supervision, alertes
Équipe DevSecOps	Automatisation, Maintenabilité
Régulateurs	RGPD, traçabilité, rétention

3- Attributs de qualités priorisés

Sécurité: Confidentialité, intégrité, authentification forte, non-répudiation, Zero Trust.
Conformité: RGPD (droits, rétention, traçabilité), droit à l'effacement.
Disponibilité: 99,5% mensuel, résilience DoS, quotas.
Performance: Latence lecture < 2s (P 95), upload 100 Mo < 5 s.
Maintenabilité: Isolation des microservices, ADR explicites, tests TDD critiques.
Observabilité: Logs, traces corrélées et signées pour audit.

4- Scénarios QAW

Scénario 1 – Confidentialité (E2EE)

- *Source* : Attaquant externe
- *Stimulus* : Interception du trafic ou accès au stockage
- *Environment* : Système en production
- *Réponse attendue*:
    - Vidéo chiffrée en transit (TLS 1.3)
    - Vidéo chiffrée au repos
    - Clés jamais stockées en clair
    - Aucune donnée lisible sans clé
    - Accès refusé si non autorisé
    - KMS/Vault isolé

Impact architectural

- Chiffrement côté client (E2EE)
- Clés par message
- mTLS inter-services

Scénario 2 - Intégrité et authenticité

- *Source* : Utilisateur malveillant
- *Stimulus* : Modification du contenu vidéo
- *Réponse attendue* :
    - Détection automatique de toute altération
    - Rejet du message à la lecture

- *Mesure*:
    - Signature RSA-PSS valide
    - Vérification SHA-256

Impact architectural

- Manifeste JSON signé
- Vérification avant lecture
- KMS / Vault

Scénario 3 - Non-répudiation

- *Source* : Expéditeur
- *Stimulus* : Contestation d'un envoi vidéo
- *Réponse attendue* :
    - Preuve cryptographique de l'envoi
- *Mesure*:
    - Signature liée à l'identité
    - Horodatage fiable (NTP)

Impact architectural

- Signature RSA-PSS
- Logs d'audit signés
- Stockage des clés publiques

Scénario 4 - Traçabilité et audit

- *Source* : Admin sécurité / Auditeur
- *Stimulus* : Demande d'audit RGPD
- *Réponse attendue* :
    - Journal complet des actions
    - Horodatage précis
- *Mesure*:
    - 100% des actions critiques journalisées

Impact architectural

- Service d'audit dédié
- Logs signés
- MySQL pour métadonnées

Scénario 5 - Performance – Lecture Vidéo

- *Source* : Utilisateur
- *Stimulus* : Lecture d'une vidéo
- *Réponse attendue*:
    - Lecture démarre rapidement
- *Mesure*:
    - lecture < 2 secondes pour 95% des requêtes

Impact architectural

- Stockage objet (MinIO/S3)
- Segmentation upload
- Observabilité et SLO

Priorisation des attributs (résumé)

Attribut	**Priorité**
Confidentialité	Critique
Intégrité	Critique
Authenticité	Critique
Non-répudiation	Critique
Traçabilité	Elevée

Disponibilité	Elevée
Scalabilité	Moyenne

« Le QAW nous a permis d’identifier que la confidentialité, l’intégrité et la non-répudiation sont des exigences architecturales critiques, ce qui a directement guidé nos choix de chiffrement, de signature numérique et d’architecture microservices. »