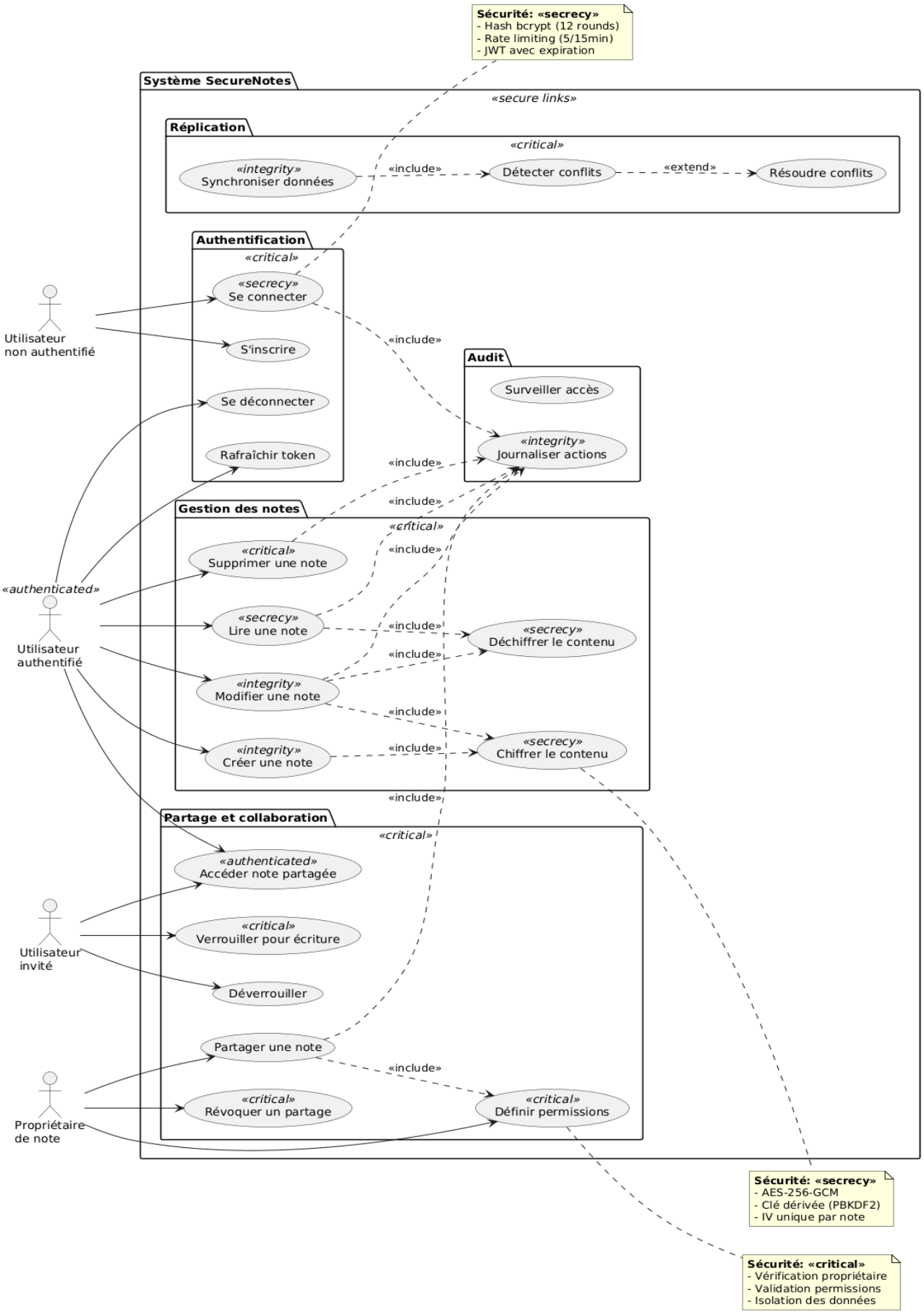
Diagrammes UML

Diagramme de cas d'utilisation UMLSec - SecureNotes



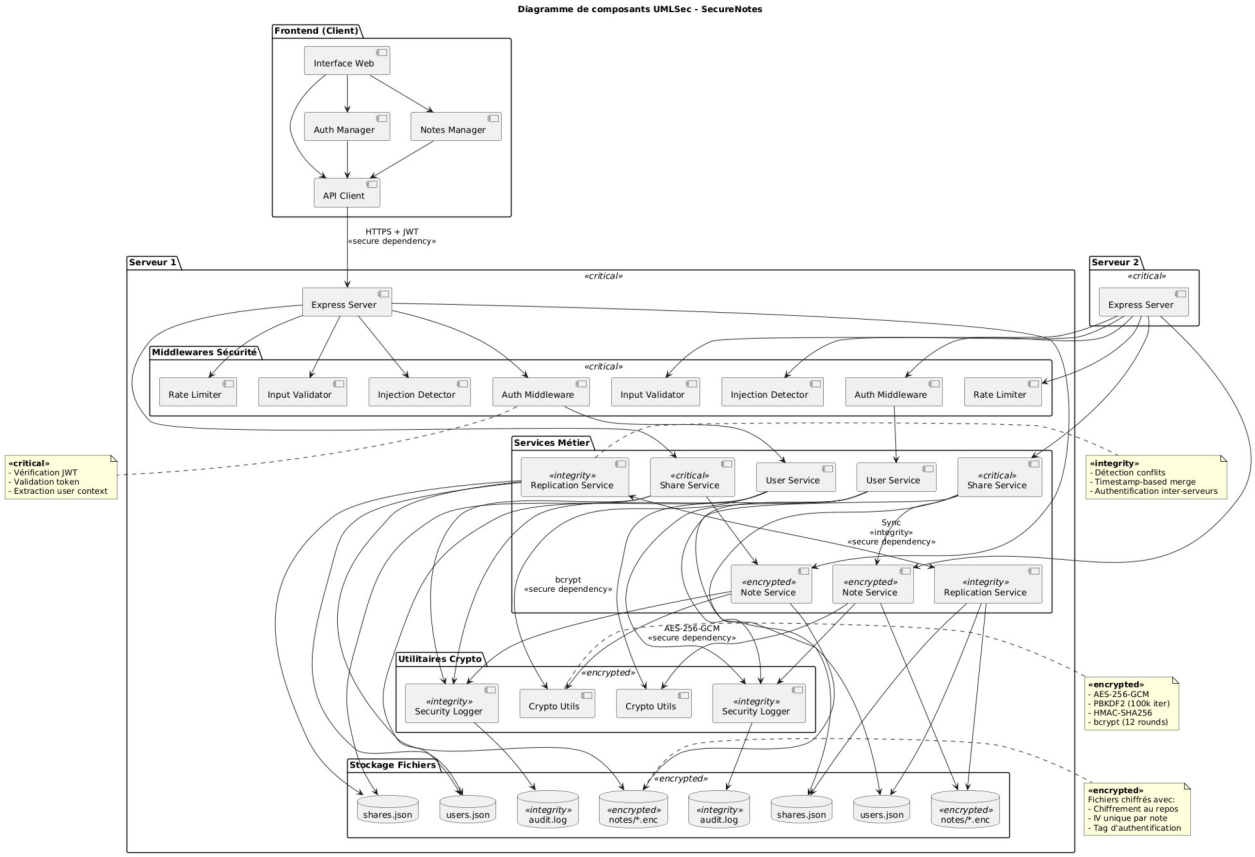
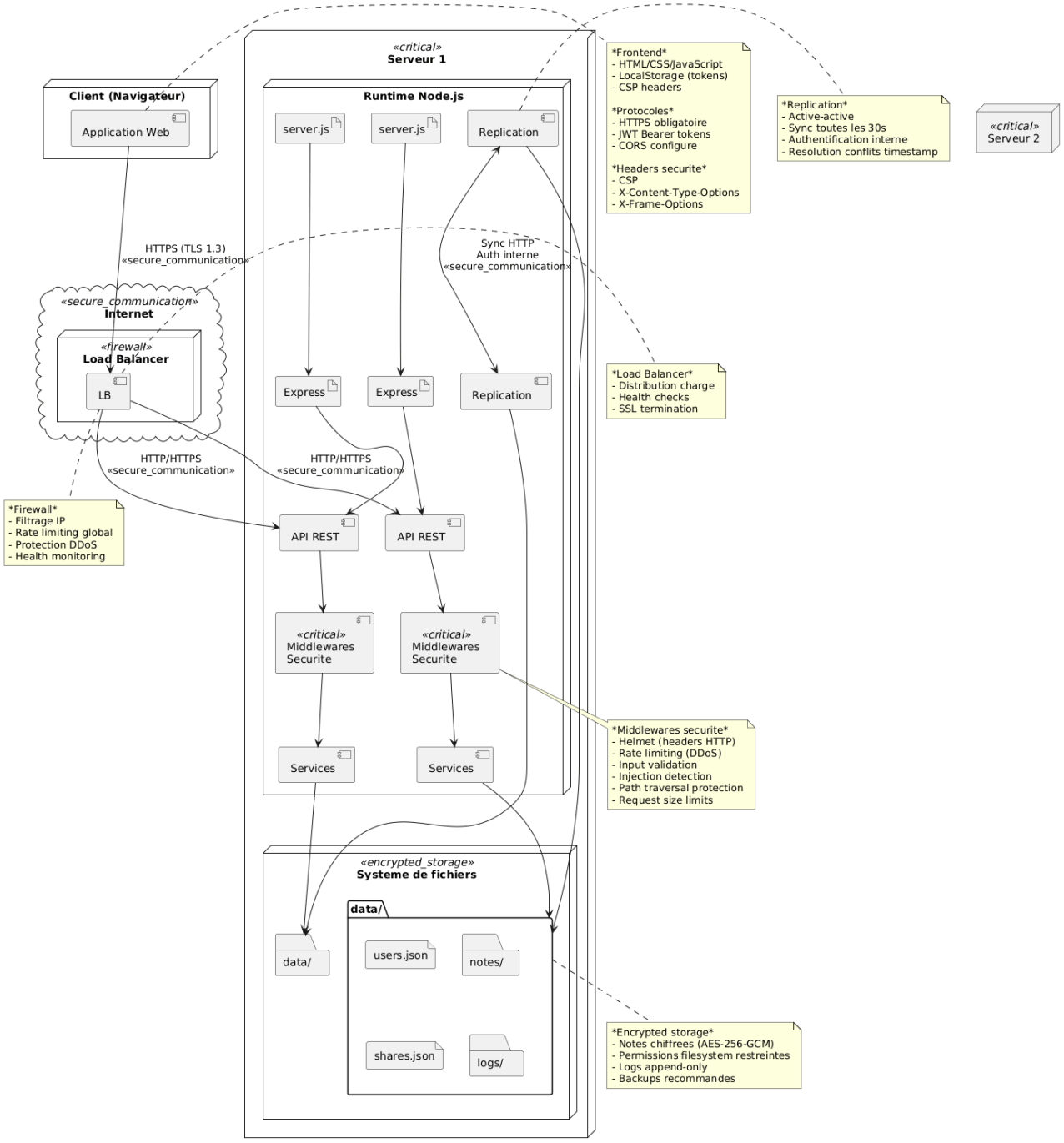
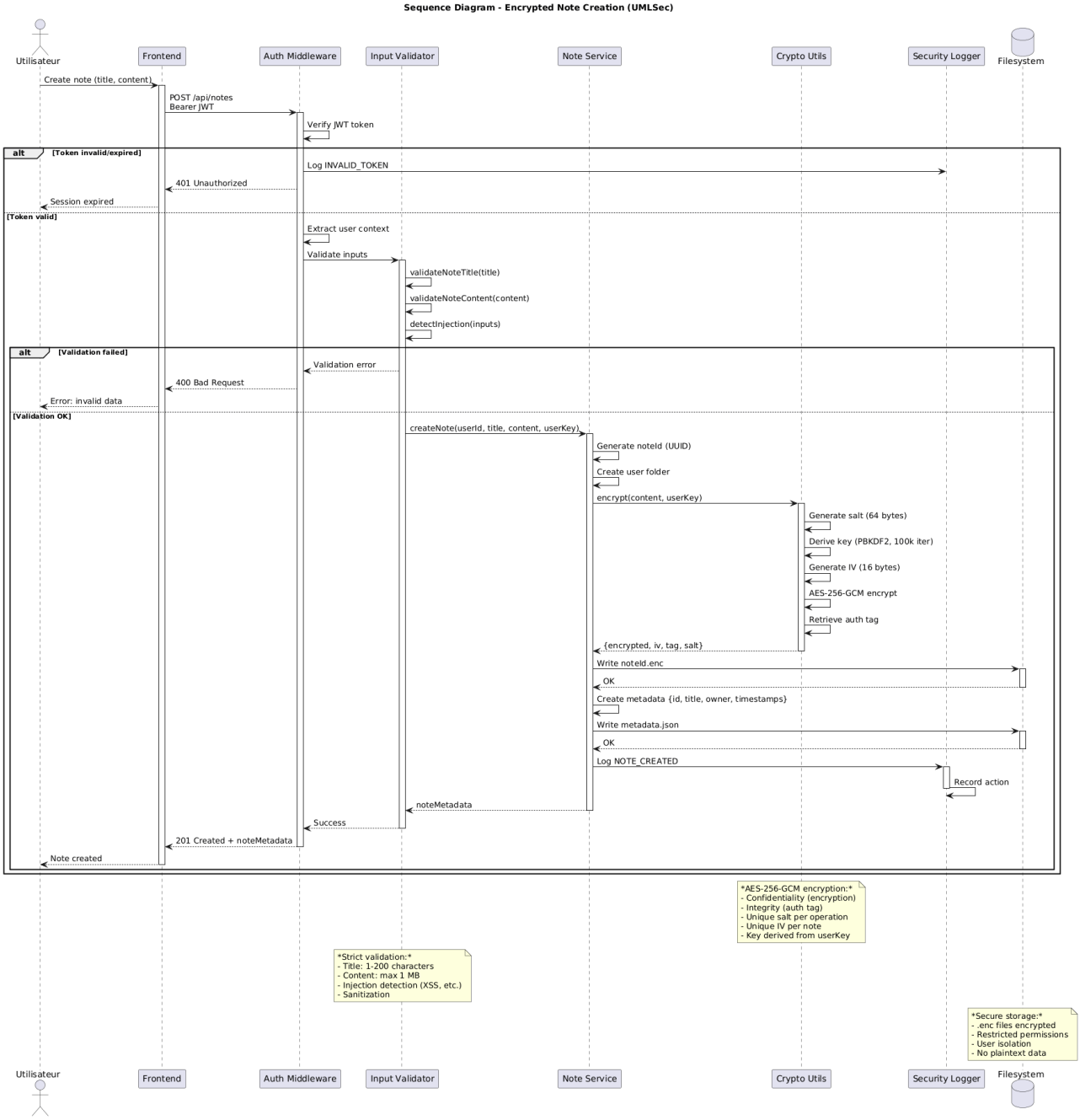
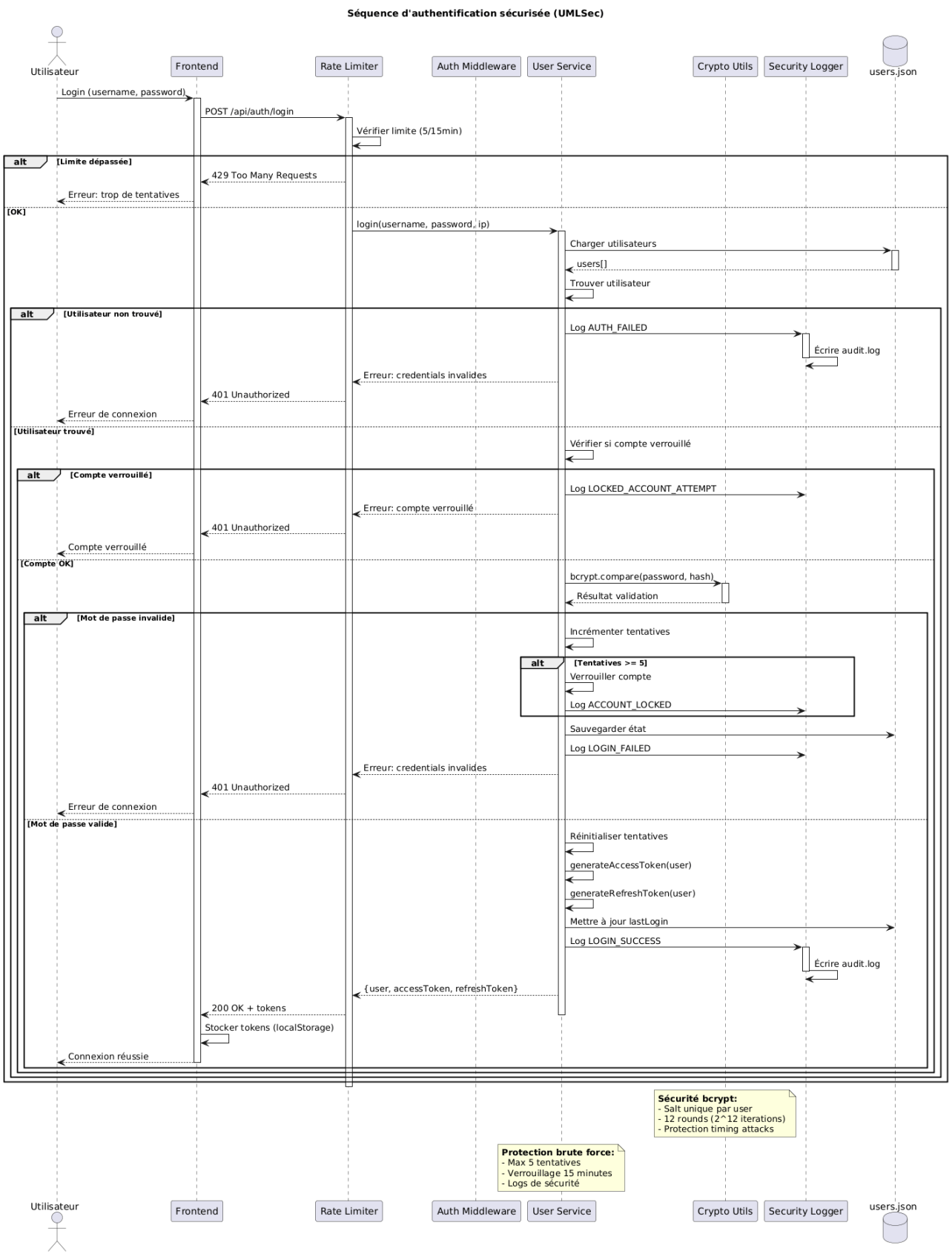


Diagramme de composants UMLSec - SecureNotes
Frontend (Client)
Interface Web
Auth Manager
Notes Manager
API Client
HTTPS + JWT
«secure dependency»
Serveur 1
«critical»
Express Server
Middlewares Sécurité
«critical»
Rate Limiter
Input Validator
Injection Detector
Auth Middleware
Input Validator
Injection Detector
Auth Middleware
Rate Limiter
Services Métier
«integrity»
Replication Service
«critical»
Share Service
User Service
User Service
«critical»
Share Service
Sync
«integrity»
«secure dependency»
bcrypt
«secure dependency»
«encrypted»
Note Service
«encrypted»
Note Service
«integrity»
Replication Service
AES-256-GCM
«secure dependency»
Utilitaires Crypto
«encrypted»
«integrity»
Security Logger
Crypto Utils
Crypto Utils
«integrity»
Security Logger
Stockage Fichiers
«encrypted»
shares.json
users.json
«integrity»
audit.log
«encrypted»
notes/*.enc
«integrity»
audit.log
shares.json
users.json
«encrypted»
notes/*.enc
Serveur 2
«critical»
Express Server
«critical»
- Vérification JWT
- Validation token
- Extraction user context
«integrity»
- Détection conflits
- Timestamp-based merge
- Authentification inter-serveurs
«encrypted»
- AES-256-GCM
- PBKDF2 (100k iter)
- HMAC-SHA256
- bcrypt (12 rounds)
«encrypted»
Fichiers chiffrés avec:
- Chiffrement au repos
- IV unique par note
- Tag d'authentification

Diagramme de déploiement UMLSec - SecureNotes




Sequence Diagram - Encrypted Note Creation (UMLSec)
Utilisateur
Frontend
Auth Middleware
Input Validator
Note Service
Crypto Utils
Security Logger
Filesystem
Create note (title, content)
POST /api/notes
Bearer JWT
Verify JWT token
alt
[Token invalid/expired]
Log INVALID_TOKEN
401 Unauthorized
Session expired
[Token valid]
Extract user context
Validate inputs
validateNoteTitle(title)
validateNoteContent(content)
detectInjection(inputs)
alt
[Validation failed]
Validation error
400 Bad Request
Error: invalid data
[Validation OK]
createNote(userId, title, content, userKey)
Generate noteId (UUID)
Create user folder
encrypt(content, userKey)
Generate salt (64 bytes)
Derive key (PBKDF2, 100k iter)
Generate IV (16 bytes)
AES-256-GCM encrypt
Retrieve auth tag
{encrypted, iv, tag, salt}
Write noteId.enc
OK
Create metadata {id, title, owner, timestamps}
Write metadata.json
OK
Log NOTE_CREATED
Record action
noteMetadata
Success
201 Created + noteMetadata
Note created
AES-256-GCM encryption:
- Confidentiality (encryption)
- Integrity (auth tag)
- Unique salt per operation
- Unique IV per note
- Key derived from userKey
Strict validation:
- Title: 1-200 characters
- Content: max 1 MB
- Injection detection (XSS, etc.)
- Sanitization
Secure storage:
- .enc files encrypted
- Restricted permissions
- User isolation
- No plaintext data


Séquence d'authentification sécurisée (UMLSec)
Utilisateur
Frontend
Rate Limiter
Auth Middleware
User Service
Crypto Utils
Security Logger
users.json
Login (username, password)
POST /api/auth/login
Vérifier limite (5/15min)
alt [Limite dépassée]
429 Too Many Requests
Erreur: trop de tentatives
[OK]
login(username, password, ip)
Charger utilisateurs
users[]
Trouver utilisateur
alt [Utilisateur non trouvé]
Log AUTH_FAILED
Écrire audit.log
Erreur: credentials invalides
401 Unauthorized
Erreur de connexion
[Utilisateur trouvé]
Vérifier si compte verrouillé
alt [Compte verrouillé]
Log LOCKED_ACCOUNT_ATTEMPT
Erreur: compte verrouillé
401 Unauthorized
Compte verrouillé
[Compte OK]
bcrypt.compare(password, hash)
Résultat validation
alt [Mot de passe invalide]
Incrémenter tentatives
alt [Tentatives >= 5]
Verrouiller compte
Log ACCOUNT_LOCKED
Sauvegarder état
Log LOGIN_FAILED
Erreur: credentials invalides
401 Unauthorized
Erreur de connexion
[Mot de passe valide]
Réinitialiser tentatives
generateAccessToken(user)
generateRefreshToken(user)
Mettre à jour lastLogin
Log LOGIN_SUCCESS
Écrire audit.log
{user, accessToken, refreshToken}
200 OK + tokens
Stocker tokens (localStorage)
Connexion réussie
Sécurité bcrypt:
- Salt unique par user
- 12 rounds (2^12 iterations)
- Protection timing attacks
Protection brute force:
- Max 5 tentatives
- Verrouillage 15 minutes
- Logs de sécurité