Politique de cryptographie et de gestion des clés

Neo Financia

RÉFÉRENCE	POL-CRYPTO-2025-V1.0
CLASSIFICATION	CONFIDENTIEL
VERSION	1.0
DATE D'APPROBATION	À définir
APPROBATION	Direction Sécurité & COMEX
PROPRIÉTAIRE	RSSI
PÉRIODICITÉ DE RÉVISION	Annuelle

Table des matières

1. Introduction et objectifs

1.1 Contexte

Neo Financia, en tant que néobanque européenne opérant exclusivement via des canaux numériques, dépend entièrement de la fiabilité et de la sécurité de ses mécanismes cryptographiques pour protéger les données sensibles, garantir l'intégrité des transactions financières et maintenir la confiance de ses 2 millions de clients.

La présente politique s'inscrit dans le cadre global de la Politique de Sécurité des Systèmes d'Information (PSSI) et définit les exigences spécifiques relatives aux services cryptographiques et à la gestion des clés au sein de Neo Financia.

Dans un contexte où les transactions financières et les documents clients constituent des données hautement sensibles, l'utilisation appropriée de la cryptographie représente un élément fondamental de notre stratégie de cybersécurité.

1.2 Objectifs de la politique

Cette politique vise à :

- Établir un cadre cohérent pour l'utilisation des services cryptographiques au sein de Neo Financia
- Définir les standards et exigences pour la protection des données et transactions par des moyens cryptographiques
- Garantir l'intégrité, la confidentialité et l'authenticité des transactions financières
- Préciser les rôles et responsabilités dans la gestion des clés cryptographiques
- Assurer la conformité aux exigences réglementaires et aux bonnes pratiques du secteur financier
- Maintenir une approche systématique pour le cycle de vie complet des clés cryptographiques
- Minimiser les risques liés à la compromission des clés ou à l'obsolescence des algorithmes

1.3 Portée et applicabilité

Cette politique s'applique à :

- L'ensemble des systèmes d'information de Neo Financia, qu'ils soient sur site ou dans le cloud (Azure, OVHcloud, AWS)
- Tous les cas d'usage des services cryptographiques (chiffrement, signature électronique, authentification, etc.)
- L'ensemble des données et transactions, avec une attention particulière aux données critiques (transactions financières, documents clients)
- Tous les collaborateurs, prestataires et partenaires impliqués dans le développement, l'exploitation ou l'utilisation des services cryptographiques
- Tous les environnements (développement, test, préproduction, production)
- Les données sensibles accessibles via les dispositifs BYOD dans le cadre du télétravail

1.4 Principes fondamentaux

La cryptographie au sein de Neo Financia repose sur les principes suivants :

- **Défense en profondeur** : Les mécanismes cryptographiques constituent une couche essentielle, mais non unique, de la sécurité
- **Conformité aux standards** : Utilisation d'algorithmes et protocoles publiquement reconnus et validés par la communauté
- **Séparation des fonctions** : Distribution des responsabilités pour réduire les risques d'usage inapproprié
- **Prévention de la non-répudiation** : Garantie de l'imputabilité des actions, notamment pour les transactions
- **Agilité cryptographique** : Capacité à faire évoluer les solutions en fonction des avancées technologiques et des menaces
- **Proportionnalité** : Niveau de protection adapté à la sensibilité des données et à leur contexte d'utilisation
- **Anticipation** : Préparation à la transition vers la cryptographie post-quantique

2. Gouvernance et responsabilités

2.1 Organisation et rôles

Fonction	Responsabilités
RSSI	- Propriétaire de la politique

	- Validation de la stratégie cryptographique - Arbitrage des exceptions - Reporting au COMEX et au Comité des Risques
Responsable Cryptographie	- Gestion opérationnelle de la PKI - Supervision du système de gestion des clés - Maintien des standards cryptographiques - Veille technologique et réglementaire
Administrateurs PKI	- Gestion des autorités de certification - Émission et révocation des certificats - Gestion des HSM - Exécution des procédures de gestion des clés
Équipe Sécurité Opérationnelle	- Surveillance de l'utilisation des services cryptographiques - Détection des anomalies et incidents - Application des contrôles cryptographiques
Équipes Infrastructure & Cloud	- Implémentation des mécanismes de chiffrement - Déploiement et configuration des solutions - Protection des infrastructures cryptographiques
Équipes Application	- Intégration des services cryptographiques dans les applications - Développement conforme aux standards - Test des fonctions cryptographiques
Auditeurs cryptographiques	- Évaluation périodique des systèmes cryptographiques - Vérification de la conformité - Recommandations d'amélioration
Key Custodians	- Détention de fragments de clés maîtres - Participation aux cérémonies de clés - Authentification lors des opérations critiques
Utilisateurs	- Utilisation conforme des mécanismes cryptographiques - Protection des éléments d'authentification personnels - Signalement des incidents

2.2 Comités et instances de gouvernance

Instance	Fréquence	Participants	Missions
Comité Cryptographique	Trimestrielle	RSSI, Responsable Crypto, Experts métier	- Définition de la stratégie cryptographique - Validation des évolutions majeures - Revue des incidents - Approbation des standards
Comité de Certification	Mensuelle	Responsable Crypto,	- Gestion opérationnelle de la PKI - Suivi des

		Administrateurs PKI	émissions/révocations - Planification des renouvellements
Cérémonie des clés	Selon besoin	Key Custodians, Responsable Crypto, Témoins	- Génération des clés maîtres - Création/destruction de matériel cryptographique critique
Comité de Sécurité (COSEC)	Mensuelle	RSSI, DSI, Responsables Sécurité	- Supervision globale - Validation des exceptions - Arbitrage des ressources

2.3 Séparation des fonctions

Neo Financia applique une stricte séparation des fonctions pour les opérations cryptographiques critiques :

- Aucun individu ne doit posséder seul le contrôle total sur les clés cryptographiques critiques
- Les administrateurs PKI n'ont pas accès aux HSM en dehors des procédures formelles
- Les développeurs ne doivent pas avoir accès aux clés de production
- Les Key Custodians sont désignés dans différentes directions pour éviter la collusion
- Un minimum de 3 personnes (quorum N sur M) est requis pour les opérations sur les clés maîtres
- Les fonctions d'audit sont strictement séparées des fonctions d'administration

2.4 Documentation et procédures

Neo Financia maintient une documentation complète et à jour concernant la cryptographie et la gestion des clés :

- Politique de cryptographie (présent document)
- Standards techniques détaillés
- Procédures opérationnelles pour chaque type d'opération
- Guides d'intégration pour les développeurs
- Procédures d'urgence et de reprise
- Schémas d'architecture des systèmes cryptographiques
- Journal des cérémonies de clés et des opérations sensibles
- Registre des exceptions accordées
- Résultats des audits et évaluations

La documentation est classifiée selon son niveau de sensibilité et accessible uniquement aux personnes autorisées.

3. Classification des données et exigences cryptographiques

3.1 Niveaux de classification

Neo Financia classe ses données selon les niveaux définis dans la PSSI, avec des exigences cryptographiques spécifiques pour chaque niveau :

Classification	Description	Types de données concernées	Exigences cryptographiques
P3 - Critique	Données hautement sensibles dont la divulgation ou l'altération pourrait avoir un impact majeur	- Transactions financières - Données d'authentification - Clés cryptographiques - Documents clients sensibles (KYC)	- Chiffrement fort obligatoire au repos et en transit - Signature électronique qualifiée - Protection par HSM pour les clés - Authentification multi-facteurs pour l'accès - Gestion stricte du cycle de vie
P2 - Confidentiel	Données sensibles à accès restreint	- Données personnelles clients - Configurations sensibles - Documents contractuels - Données financières agrégées	- Chiffrement au repos et en transit - Signature électronique avancée - Authentification forte pour l'accès - Protection renforcée des clés
P1 - Interne	Données à usage interne uniquement	- Communications internes - Documentation non sensible - Données opérationnelles	- Chiffrement en transit obligatoire - Chiffrement au repos recommandé - Authentification standard - Protection standard des clés
P0 - Public	Informations destinées au public	- Communications externes - Informations marketing	- Intégrité et authenticité garanties - Chiffrement en

		- Documents publics	transit pour l'accès administrateur

3.2 Exigences par cas d'usage

En complément de la classification des données, Neo Financia définit des exigences spécifiques par cas d'usage :

Cas d'usage	Objectifs de sécurité	Exigences cryptographiques
Authentification clients	Vérifier l'identité des clients	- Authentification multi-facteurs - Stockage sécurisé des credentials - Chiffrement des échanges - Protection contre le rejeu
Paiements et virements	Sécuriser les transactions financières	- Signature électronique des ordres - Chiffrement de bout en bout - Protection de l'intégrité - Non-répudiation
Communication client	Protéger les échanges avec les clients	- Chiffrement TLS 1.3 minimum - Authentification du serveur - Protection des sessions
API partenaires	Sécuriser les échanges avec Mangopay, Lemonway, etc.	- Authentification mutuelle - Signature des requêtes - Chiffrement des données sensibles - Contrôle de fraicheur
Stockage long terme	Protéger les archives et sauvegardes	- Chiffrement avec possibilité de déchiffrement futur - Protection des clés longue durée - Mécanismes d'intégrité
Signature de code	Garantir l'authenticité du code déployé	- Signature des packages et images - Vérification à chaque déploiement - Protection des clés de signature

3.3 Matrice de décision

Pour aider à la sélection des mécanismes cryptographiques appropriés, Neo Financia utilise la matrice de décision suivante :

Type de donnée	Classification	En transit	Au repos	Contrôles complémentaires

Codes d'authentification	P3	TLS 1.3 + Chiffrement application	AES-256 + Hachage salé	HSM, accès limité, audit
Transactions financières	P3	TLS 1.3 + Chiffrement E2E	AES-256	Signature, journalisation, contrôle d'accès
Documents clients (KYC)	P3	TLS 1.3	AES-256	Contrôle d'accès, DLP, watermarking
Données personnelles	P2	TLS 1.3	AES-256	Pseudonymisation, contrôle d'accès
Configuration système	P2	TLS 1.3 / SSH	AES-256	Contrôle d'accès, gestion des versions
Données opérationnelles	P1	TLS 1.2+	AES-256 recommandé	Contrôle d'accès
Contenu marketing	P0	TLS 1.2+	Non requis	Signature pour l'intégrité

4. Algorithmes et protocoles approuvés

4.1 Algorithmes approuvés

Neo Financia maintient une liste d'algorithmes cryptographiques approuvés, basée sur les recommandations des organismes de référence (ANSSI, NIST, BSI) et adaptée à ses besoins spécifiques :

Catégorie	Algorithmes approuvés	Force minimale	Usage privilégié	Obsolescence prévue
Chiffrement symétrique				
Recommandé	AES-GCM	256 bits	Données critiques, transactions	> 2040
Recommandé	AES-CBC avec HMAC	256 bits	Compatibilité systèmes existants	> 2035
Autorisé	ChaCha20-Poly1305	256 bits	Environnements à ressources limitées	> 2035
Toléré	AES-CBC	256 bits	Systèmes legacy uniquement	2027
Chiffrement asymétrique				
Recommandé	RSA-OAEP	4096 bits	Échange de clés, chiffrement	2030

Recommandé	ECIES (P-384, P-521)	384 bits min.	Échange de clés, chiffrement	> 2035
Recommandé	Courbes X25519	256 bits	Échange de clés rapide	> 2030
Toléré	RSA	3072 bits min.	Compatibilité systèmes existants	2028
Signature électronique				
Recommandé	RSA-PSS	4096 bits	Signature longue durée	2030
Recommandé	ECDSA (P-384, P-521)	384 bits min.	Signature standard	> 2035
Recommandé	Ed25519	256 bits	Signature haute performance	> 2030
Toléré	RSA-PKCS#1 v1.5	3072 bits min.	Compatibilité uniquement	2028
Fonctions de hachage				
Recommandé	SHA-384, SHA-512	384 bits min.	Usage général, stockage empreintes	> 2040
Recommandé	SHA-3 (384, 512)	384 bits min.	Applications critiques futures	> 2045
Autorisé	SHA-256	256 bits	Compatibilité, usages non critiques	> 2030
Toléré	SHA-1	160 bits	Validation intégrité interne uniquement	2025
Génération de nombres aléatoires				
Recommandé	HMACDRBG (SP800-90A)	N/A	Général	> 2040
Recommandé	CTR_DRBG (SP800-90A)	N/A	Général	> 2040
Requis	Sources d'entropie matérielles	N/A	Génération de clés maîtres	N/A

Cryptographie post-quantique				
En évaluation	CRYSTALS-Kyber	Selon NIST	Préparation future	N/A
En évaluation	CRYSTALS-Dilithium	Selon NIST	Préparation future	N/A

4.2 Protocoles approuvés

Catégorie	Protocoles approuvés	Version minimale	Usage privilégié	Obsolescence prévue
Sécurisation web				
Recommandé	TLS	1.3	Communications sensibles	> 2035
Autorisé	TLS	1.2	Compatibilité	2028
Interdit	SSL	Toutes	Aucun	Immédiate
API sécurisées				
Recommandé	OAuth 2.0 + OIDC	RFC 6749 + OIDC 1.0	Authentification API	> 2030
Recommandé	JWT signé (JWS)	RFC 7515	Tokens d'accès	> 2030
Recommandé	JWT chiffré (JWE)	RFC 7516	Données sensibles dans tokens	> 2030
Communications sécurisées				
Recommandé	SSH	v2 uniquement	Administration systèmes	> 2035
Recommandé	IPsec	IKEv2	Tunnels VPN	> 2030
Protocoles de paiement				
Requis	3-D Secure	2.0+	Authentification paiements	Selon évolutions
Requis	PCI P2PE	Version actuelle	Protection données cartes	Selon évolutions

4.3 Suites cryptographiques

Pour les protocoles configurables (comme TLS), Neo Financia définit les suites cryptographiques suivantes :

TLS 1.3 (préféré)

Suites autorisées, par ordre de préférence :

1. TLS_AES_256_GCM_SHA384
2. TLS_CHACHA20_POLY1305_SHA256
3. TLS_AES_128_GCM_SHA256

TLS 1.2 (compatibilité)

Suites autorisées, par ordre de préférence :

1. TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
2. TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
3. TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256
4. TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
5. TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
6. TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

4.4 Gestion de l'obsolescence

Neo Financia surveille l'évolution des standards cryptographiques et planifie la transition vers de nouveaux algorithmes :

1. **Processus de revue** :
    - Veille technologique et réglementaire continue
    - Revue annuelle formelle de tous les algorithmes et protocoles
    - Mise à jour du plan de transition
2. **Indicateurs d'obsolescence** :
    - Affaiblissement cryptographique théorique
    - Découverte de vulnérabilités
    - Évolution des recommandations officielles
    - Évolution des exigences réglementaires
    - Disponibilité d'alternatives plus robustes
3. **Plan de transition** :
    - Pour chaque algorithme obsolescent, définition d'une date limite d'utilisation
    - Identification des systèmes concernés
    - Définition des alternatives
    - Planification des migrations
    - Tests de compatibilité et d'impact
4. **Cryptographie hybride** :
    - Préparation à la transition post-quantique
    - Implémentation progressive de solutions hybrides pour les données critiques
    - Suivi des standards émergents

5. Infrastructure à clés publiques (PKI)

5.1 Architecture de la PKI

Neo Financia utilise une infrastructure à clés publiques (PKI) hiérarchique pour gérer les certificats, avec les niveaux suivants :

1. **Autorité de Certification Racine (AC Racine)**
    - Hors ligne, stockée dans un HSM dédié
    - Utilisée uniquement pour signer les AC intermédiaires
    - Cérémonie des clés formelle pour toute opération
    - Durée de validité : 20 ans
    - Stockage physique sécurisé
2. **Autorités de Certification Intermédiaires (AC Intermédiaires)**
    - AC Interne : pour les besoins internes (collaborateurs, systèmes)
    - AC Services : pour les services exposés aux clients
    - AC Partenaires : pour les communications avec les partenaires
    - Durée de validité : 10 ans
    - Protection par HSM
3. **Autorités de Certification Émettrices (AC Émettrices)**
    - AC Collaborateurs : certificats personnels
    - AC Serveurs : certificats serveurs internes
    - AC Applications : certificats d'applications
    - AC Clients : certificats clients
    - AC Code : signature de code
    - Durée de validité : 5 ans
    - Connectées aux systèmes d'émission automatisée
4. **Certificats d'entité finale**
    - Certificats personnels : authentification, signature, chiffrement
    - Certificats serveurs : authentification serveur
    - Certificats clients : authentification forte des clients
    - Certificats de signature de code : déploiements sécurisés
    - Certificats de signature de transactions : non-répudiation
    - Durée de validité : 1-3 ans selon l'usage

5.2 Profils de certificats

Neo Financia définit des profils de certificats standardisés selon les usages :

Type de certificat	Usage	Extensions critiques	Algorithme de signature	Durée de validité
Serveur TLS	Authentification serveur	Extended Key Usage: Server Authentication	ECDSA P-384	1 an
Client TLS	Authentification client	Extended Key Usage: Client Authentication	ECDSA P-384	2 ans
S/MIME	Email sécurisé	Key Usage: Digital Signature, Key Encipherment	RSA 3072	3 ans
Signature de code	Signature des déploiements	Extended Key Usage: Code Signing	RSA 4096	1 an

Signature de transactions	Non-répudiation	Key Usage: Non-Repudiation	ECDSA P-384	2 ans
Authentication collaborateur	SSO, VPN	Extended Key Usage: Client Authentication	ECDSA P-384	2 ans

5.3 Gestion des certificats

Neo Financia applique les principes suivants pour la gestion des certificats :

1. **Émission**
    - Vérification rigoureuse de l'identité du demandeur
    - Validation de l'autorisation par le propriétaire du domaine/système
    - Génération des clés privées sur le dispositif destinataire quand possible
    - Transmission sécurisée des certificats et clés
    - Documentation complète du processus d'émission
2. **Distribution**
    - Canaux sécurisés pour la distribution des certificats
    - Protection des clés privées pendant le transit
    - Confirmation de réception par le destinataire
    - Intégration avec les systèmes d'annuaire pour la publication
3. **Renouvellement**
    - Processus automatisé de notification avant expiration (90, 60, 30, 15, 7 jours)
    - Validation simplifiée pour le renouvellement standard
    - Nouvelle vérification complète tous les 6 ans ou en cas de changement significatif
    - Chevauchement des périodes de validité pour assurer la continuité
4. **Révocation**
    - Motifs de révocation définis (compromission, départ employé, etc.)
    - Processus d'urgence pour révocation immédiate
    - Publication des listes de révocation (CRL) toutes les 24h
    - Support OCSP pour vérification en temps réel
    - Délai maximum de 24h entre demande et publication de la révocation

5.4 Services OCSP et CRL

Neo Financia maintient des services de vérification de validité des certificats :

1. **Listes de révocation (CRL)**
    - Publication quotidienne des CRL complètes
    - Publication immédiate en cas de révocation d'urgence
    - Points de distribution redondants
    - Conservation de l'historique des CRL
    - Validité de 48h pour absorber les indisponibilités temporaires
2. **Service OCSP**

- Disponibilité 24/7 avec haute disponibilité
- Temps de réponse < 500ms
- Mise à jour en temps réel
- OCSP Stapling recommandé pour les serveurs
- Conservation des logs de requêtes pour audit

5.5 Contrôles opérationnels et physiques

Neo Financia met en place des contrôles stricts pour protéger l'intégrité de sa PKI :

1. **Contrôles physiques**
   - AC Racine dans un coffre-fort dédié avec contrôle d'accès biométrique
   - HSM dans des zones à accès hautement restreint
   - Surveillance vidéo et journalisation des accès
   - Systèmes de détection d'intrusion
2. **Contrôles opérationnels**
   - Principe de double contrôle pour toutes les opérations critiques
   - Séparation des rôles (administrateur, opérateur, auditeur)
   - Journalisation complète de toutes les actions
   - Audits internes trimestriels
   - Audit externe annuel par un organisme certifié
3. **Cérémonie des clés**
   - Procédure formelle documentée
   - Présence obligatoire de plusieurs témoins (quorum)
   - Enregistrement vidéo de la cérémonie
   - Conservation sécurisée du script et des logs
   - Vérification de l'intégrité des composants avant la cérémonie

6. Gestion du cycle de vie des clés

6.1 Génération des clés

Les exigences suivantes s'appliquent à la génération des clés cryptographiques :

1. **Source d'entropie**
   - Utilisation de générateurs de nombres aléatoires cryptographiquement sûrs (CSPRNG)
   - Sources d'entropie matérielles pour les clés critiques
   - Validation de la qualité de l'entropie avant génération
   - Combinaison de multiples sources pour les clés maîtres
2. **Environnement de génération**
   - Génération dans un environnement sécurisé
   - HSM certifié FIPS 140-2 niveau 3 minimum pour les clés critiques
   - Système isolé et durci pour les autres clés sensibles
   - Protection contre les fuites par canaux auxiliaires
3. **Paramètres des clés**
   - Longueur minimale selon les standards définis en section 4
   - Vérification de la qualité des paires de clés asymétriques

- Unicité garantie par des procédures appropriées
- Documentation des paramètres de génération

4. **Génération par cas d'usage**

Type de clé	Méthode de génération	Environnement	Contraintes spécifiques
Clés maîtres	Cérémonie formelle	HSM dédié hors ligne	Quorum obligatoire, témoins
Clés de chiffrement de données	Selon procédure standard	HSM ou module sécurisé	Double contrôle
Clés de chiffrement de session	Génération dynamique	Bibliothèque cryptographique validée	Unicité par session
Clés de signature de transactions	Selon procédure standard	HSM	Individuelle par signataire
Clés d'authentification	Sur le dispositif final quand possible	Selon contexte	Secrets partagés prohibés

6.2 Distribution et stockage des clés

Neo Financia applique des mesures strictes pour la distribution et le stockage des clés :

1. **Méthodes de distribution**

   - Utilisation de canaux chiffrés dédiés
   - Mécanismes de chiffrement à clé publique pour le transport
   - Séparation des composants pour les clés critiques
   - Transmission différée (temps et canaux) pour les composants
   - Vérification d'intégrité après transmission

2. **Stockage des clés**

Type de clé	Méthode de stockage	Contrôles d'accès	Durée de conservation
Clés maîtres	HSM certifié, composants séparés	Quorum, coffre physique	Durée de vie + période d'archivage
Clés de chiffrement longue durée	HSM ou stockage chiffré	Authentification forte, double contrôle	Durée de vie + période d'archivage
Clés privées de signature	HSM ou token personnel	Authentification du propriétaire	Durée de validité du certificat
Clés de session	Mémoire volatile	Isolation par	Durée de la

	uniquement	processus	session uniquement
Clés publiques	Stockage standard	Contrôle d'intégrité	Selon besoin

3. **Protection contre la divulgation**
    - Chiffrement des clés au repos systématique
    - Clés d'enveloppement (Key Wrapping) pour les clés sensibles
    - Hiérarchie de clés clairement définie
    - Journalisation des accès aux stockages de clés
    - Détection d'accès non autorisés

6.3 Utilisation des clés

Neo Financia définit des règles strictes pour l'utilisation des clés :

1. **Principes généraux**
    - Usage unique : une clé pour une seule fonction cryptographique
    - Séparation des contextes : clés distinctes par environnement
    - Limitation d'usage : respect des attributs et contraintes
    - Authentification préalable : contrôle d'accès à l'utilisation
    - Traçabilité : journalisation des opérations critiques
2. **Contrôles d'usage**
    - Vérification des droits avant toute opération
    - Limitation du nombre d'opérations par clé
    - Détection des usages anormaux ou abusifs
    - Protection contre les attaques par canal auxiliaire
    - Validation des paramètres d'entrée
3. **Durée de vie opérationnelle**

Type de clé	Durée d'utilisation maximale	Facteurs de renouvellement anticipé
Clés maîtres	10 ans	Avancées cryptographiques, suspicion de compromission
Clés de chiffrement de données	3 ans	Volume de données chiffrées, changements organisationnels
Clés de signature	2 ans	Volume de signatures, changements organisationnels
Certificats SSL/TLS	1 an	Exigences réglementaires, changements techniques
Clés de session	Durée de la session	Timeout, volume de données, détection d'anomalies

6.4 Rotation et renouvellement des clés

Neo Financia applique une politique de rotation régulière des clés :

1. **Planification**
    - Calendrier prédéfini de rotation pour chaque type de clé
    - Prise en compte des interdépendances entre clés
    - Synchronisation avec les fenêtres de maintenance
    - Communication préalable aux parties prenantes
2. **Procédure de rotation**
    - Génération de la nouvelle clé selon les standards
    - Période de transition avec double validité
    - Migration progressive des données ou services
    - Vérification complète après migration
    - Révocation ou désactivation de l'ancienne clé
    - Archivage sécurisé si nécessaire
3. **Événements déclencheurs de rotation extraordinaire**
    - Suspicion de compromission
    - Départ d'un détenteur de clé
    - Évolution majeure des standards cryptographiques
    - Incident de sécurité
    - Changement organisationnel significatif

6.5 Archivage et destruction des clés

Neo Financia définit des procédures strictes pour l'archivage et la destruction des clés :

1. **Archivage**
    - Évaluation de la nécessité d'archivage (déchiffrement futur)
    - Protection renforcée des clés archivées
    - Stockage hors ligne pour les clés les plus sensibles
    - Documentation détaillée des clés archivées
    - Tests périodiques de récupération
    - Durée de conservation alignée sur les obligations légales
2. **Méthodes de destruction**
    - Effacement sécurisé (multiple passes) pour les clés sur support logique
    - Destruction physique des HSM ou modules en fin de vie
    - Vérification de l'impossibilité de récupération
    - Documentation formelle de la destruction
    - Présence de témoins pour les clés critiques
3. **Matrice d'archivage par type de clé**

Type de clé	Archivage requis	Méthode d'archivage	Durée d'archivage
Clés de chiffrement de données	Oui	HSM dédié offline + backup sécurisé	Durée de vie des données + 10 ans
Clés de signature	Non	N/A	N/A (conserver les signatures uniquement)

Clés d'authentification	Non	N/A	N/A
Clés maîtres	Oui	Coffre physique, composants séparés	Durée de vie des clés dérivées + 5 ans
Clés de session	Non	N/A	N/A

7. Protection des clés cryptographiques

7.1 Dispositifs de stockage sécurisé

Neo Financia utilise différents dispositifs de stockage sécurisé selon la sensibilité des clés :

1. **Modules de sécurité matériels (HSM)**
    - Certification minimale FIPS 140-2 niveau 3
    - Utilisés pour toutes les clés critiques
    - Déploiement en cluster pour la haute disponibilité
    - Séparation des rôles administratifs
    - Audit trail complet de toutes les opérations
    - Surveillance physique et environnementale
2. **Tokens cryptographiques**
    - Dispositifs personnels pour les clés des utilisateurs
    - Protection par PIN ou biométrie
    - Certification minimale FIPS 140-2 niveau 2
    - Inventaire et suivi de tous les dispositifs
    - Procédure de révocation en cas de perte
3. **Modules logiciels**
    - Pour les clés de moindre sensibilité uniquement
    - Protection par chiffrement et contrôles d'accès renforcés
    - Stockage dans des zones mémoire protégées
    - Effacement sécurisé après utilisation
    - Surveillance des accès et modifications
4. **Stockage cloud**
    - Utilisation des services de gestion de clés cloud natifs
    - Azure Key Vault pour l'environnement Azure
    - AWS KMS pour l'environnement AWS
    - Solutions de chiffrement BYOK (Bring Your Own Key)
    - Contrôles d'accès IAM restrictifs

7.2 Protection des HSM

Les HSM étant au cœur de la sécurité cryptographique, Neo Financia applique des mesures de protection spécifiques :

1. **Sécurité physique**
    - Installation dans des zones à accès hautement restreint
    - Protections environnementales (alimentation, température)

- Surveillance vidéo et détection d'intrusion
- Maintenance sous surveillance
- Inventaire précis des composants

2. **Configuration sécurisée**

   - Durcissement selon les recommandations du fabricant
   - Désactivation des services non essentiels
   - Application des correctifs de sécurité
   - Mode FIPS obligatoire
   - Vérification régulière de la configuration

3. **Administration**

   - Principe de séparation des rôles
   - Quorum obligatoire pour les opérations sensibles (M of N)
   - Authentification forte des administrateurs
   - Journalisation détaillée de toutes les actions
   - Procédures formelles pour chaque type d'opération

4. **Surveillance et audit**

   - Monitoring en temps réel des événements de sécurité
   - Alertes sur les comportements anormaux
   - Conservation des journaux pour audit
   - Tests d'intrusion périodiques
   - Vérification de l'intégrité du firmware

7.3 Protection des clés dans les applications

La protection des clés au sein des applications suit les principes suivants :

1. **Conception sécurisée**

   - Pas de stockage de clés en clair dans le code
   - Utilisation d'APIs cryptographiques validées
   - Protection de la mémoire contenant les clés
   - Effacement sécurisé après utilisation
   - Limitation de la durée de vie en mémoire

2. **Technologies d'isolation**

   - Enclaves sécurisées lorsque disponibles
   - TEE (Trusted Execution Environment) pour les plateformes mobiles
   - Secure Elements pour les clés de plus haute sensibilité
   - Conteneurs sécurisés pour les applications cloud
   - Isolation des processus cryptographiques

3. **Bonnes pratiques de développement**

   - Revue de code spécifique aux aspects cryptographiques
   - Tests de pénétration ciblés
   - Obfuscation des implémentations critiques
   - Protection contre les attaques par canal auxiliaire
   - Formation spécifique des développeurs

7.4 Sauvegarde et restauration des clés

Neo Financia maintient des procédures de sauvegarde pour les clés critiques :

1. **Politique de sauvegarde**
    - Identification des clés nécessitant une sauvegarde
    - Fréquence adaptée à la criticité
    - Protection équivalente au stockage principal
    - Séparation des composants pour les clés les plus sensibles
    - Documentation précise des procédures
2. **Procédures de sauvegarde**
    - Sauvegarde chiffrée systématique
    - Validation de l'intégrité après sauvegarde
    - Stockage dans des lieux physiquement distincts
    - Inventaire et suivi des sauvegardes
    - Test périodique des sauvegardes
3. **Restauration**
    - Procédure formelle de demande
    - Validation par les autorités compétentes
    - Quorum pour les clés critiques
    - Documentation détaillée de chaque restauration
    - Vérification de la validité après restauration
4. **Matrice de sauvegarde par type de clé**

Type de clé	Stratégie de sauvegarde	Fréquence	Méthode	Sites de stockage
Clés maîtres	Composants séparés (M of N)	À la création uniquement	Backup HSM sécurisé	3 sites distincts
Clés de chiffrement données	Sauvegarde complète	Après chaque modification	Export sécurisé HSM	2 sites distincts
Clés PKI	Sauvegarde hiérarchique	Hebdomadaire	Export HSM chiffré	2 sites distincts
Clés personnelles	Recommandée à l'utilisateur	À la création	Selon dispositif	Selon politique utilisateur

8. Cryptographie pour les transactions financières

8.1 Exigences spécifiques aux transactions

Les transactions financières, étant au cœur de l'activité de Neo Financia, font l'objet d'exigences cryptographiques renforcées :

1. **Objectifs de sécurité**
    - Confidentialité des données financières
    - Intégrité des ordres et montants
    - Authentification forte des parties

- Non-répudiation des opérations
- Traçabilité complète
- Protection contre la rejouabilité

2. **Mécanismes cryptographiques requis**

- Signature électronique pour chaque transaction
- Chiffrement de bout en bout des données sensibles
- Authentification mutuelle des endpoints
- Horodatage qualifié pour les transactions critiques
- Numéros de séquence uniques
- Codes d'authentification de message (HMAC)

3. **Standards minimaux pour les transactions**

Élément de sécurité	Exigence pour transactions standard	Exigence pour transactions critiques (>10K€)
Chiffrement	TLS 1.3 + AES-256 applicatif	TLS 1.3 + chiffrement bout-en-bout + AES-256
Signature	ECDSA P-384	ECDSA P-384 ou RSA 4096 avec horodatage qualifié
Authentification client	SCA conforme DSP2	SCA + facteur supplémentaire
Protection anti-rejeu	Timestamp + nonce	Timestamp + nonce + séquence vérifiée
Journalisation	Signature des logs	Signature des logs + stockage immuable

8.2 Signature des transactions

Neo Financia met en place un système robuste de signature des transactions :

1. **Types de signatures**

- Signature client : preuve de consentement du client
- Signature système : validation technique par Neo Financia
- Signature partenaire : validation par les prestataires de paiement
- Signature d'audit : preuve d'intégrité pour les régulateurs

2. **Processus de signature**

- Création d'un objet de transaction normalisé
- Inclusion des métadonnées nécessaires (timestamps, identifiants)
- Calcul de l'empreinte sur l'ensemble des données
- Signature avec la clé privée appropriée
- Stockage sécurisé de la transaction signée
- Transmission sécurisée aux parties concernées

3. **Vérification des signatures**

- Validation systématique à chaque étape du traitement
- Vérification de l'authenticité du certificat signataire
- Contrôle de non-répudiation

- Validation des attributs du certificat
- Conservation des preuves de vérification

4. **Conservation des preuves**
   - Archivage à long terme des transactions signées
   - Protection de l'intégrité pendant toute la durée de conservation
   - Gestion de la durabilité cryptographique
   - Stockage dans un système d'archivage à vocation probatoire
   - Durée de conservation conforme aux obligations légales (minimum 10 ans)

8.3 Authentification des parties

Neo Financia implémente des mécanismes robustes pour l'authentification des parties impliquées dans les transactions financières :

1. **Authentification des clients**
   - Conformité aux exigences d'authentification forte (SCA) de la DSP2
   - Combinaison d'au moins deux facteurs parmi :
     - Connaissance (mot de passe, code PIN)
     - Possession (téléphone mobile, token)
     - Inhérence (biométrie)
   - Liage des facteurs d'authentification
   - Analyse de risque dynamique pour l'authentification adaptative
   - Support de la délégation d'authentification (OAuth 2.0, OIDC)

2. **Authentification des systèmes internes**
   - Certificats X.509 avec validation mutuelle
   - Rotation régulière des identifiants de service
   - Contrôle strict des autorisations
   - Journalisation des authentifications
   - Détection des anomalies comportementales

3. **Authentification des partenaires**
   - Tunnels sécurisés dédiés (mTLS)
   - Authentification basée sur des certificats
   - Validation des domaines et identités
   - Gestion stricte des révocations
   - Limitation des privilèges au minimum nécessaire

8.4 Protection des données de paiement

Neo Financia applique des mesures spécifiques pour la protection des données de paiement :

1. **Données de cartes bancaires**
   - Conformité PCI-DSS niveau 1
   - Tokenisation systématique des PAN
   - Non-conservation des données sensibles (CVV)
   - Masquage des numéros affichés (seuls les 4 derniers chiffres visibles)
   - Chiffrement point-à-point (P2PE) pour les transmissions
   - Déchiffrement uniquement dans des environnements dédiés et qualifiés

2. **Données de virements**
    - Chiffrement des coordonnées bancaires
    - Validation d'intégrité des montants et références
    - Contrôles anti-altération des bénéficiaires
    - Double validation pour les montants importants
    - Stockage chiffré des modèles de virement
3. **Données de paiement instantané**
    - Protection renforcée de bout en bout
    - Validation en temps réel des signatures
    - Mécanismes anti-rejeu stricts
    - Horodatage précis et sécurisé
    - Confirmation authentifiée de réception

8.5 Intégration avec les partenaires financiers

La sécurité des échanges avec les partenaires financiers (Mangopay, Lemonway) est assurée par :

1. **Sécurisation des API**
    - Authentification mutuelle par certificats (mTLS)
    - OAuth 2.0 avec jetons à courte durée de vie
    - Validation des signatures des requêtes (JWS)
    - Chiffrement des données sensibles dans les requêtes (JWE)
    - Validation stricte des formats et contenus
2. **Validation des transactions**
    - Signatures croisées des ordres
    - Contrôles de cohérence automatisés
    - Réconciliation cryptographique des flux
    - Non-répudiation garantie par signatures multiples
    - Archivage probatoire des échanges
3. **Surveillance dédiée**
    - Monitoring spécifique des flux partenaires
    - Alertes sur les patterns anormaux
    - Détection des désynchronisations
    - Traçabilité complète des échanges
    - Reporting sécurisé automatisé

9. Chiffrement des données au repos et en transit

9.1 Chiffrement des données au repos

Neo Financia implémente une stratégie de chiffrement au repos adaptée à la sensibilité des données :

1. **Approche par niveau de données**

Classification	Méthode de chiffrement	Gestion des clés	Contrôles supplémentaires
P3 - Critique	Chiffrement	HSM dédié	Contrôle d'accès,

	applicatif + stockage		audit renforcé
P2 - Confidentiel	Chiffrement au niveau stockage	HSM mutualisé	Contrôle d'accès, journalisation
P1 - Interne	Chiffrement au niveau volume	Key Management Service cloud	Contrôle d'accès standard
P0 - Public	Non requis	N/A	Contrôle d'intégrité

2. **Solutions par environnement**

Environnement	Technologies de chiffrement	Mode de gestion des clés
Base de données	TDE (Transparent Data Encryption) + chiffrement colonne	HSM pour TDE, KMS pour colonnes
Stockage de fichiers	Chiffrement au niveau fichier	Clés par dossier ou document
Stockage cloud Azure	Azure Storage Encryption, Azure Disk Encryption	Azure Key Vault avec BYOK
Stockage cloud AWS	S3 Encryption, EBS Encryption	AWS KMS avec rotation automatique
Stockage cloud OVHcloud	Chiffrement AES-256	Managed Keys avec rotation
Postes de travail	BitLocker, FileVault	Gestion centralisée des clés
Appareils mobiles	Chiffrement natif + conteneurisation	Gestion MDM avec effacement à distance

3. **Tokenisation et masquage**
    - Tokenisation des données sensibles répétitives
    - Masquage dynamique selon le profil utilisateur
    - Pseudonymisation des données pour les environnements non-production
    - Conservation des mappings dans un coffre-fort dédié
    - Rotation régulière des tables de tokenisation

9.2 Chiffrement des données en transit

Neo Financia protège toutes les communications avec des mécanismes adaptés à leur sensibilité :

1. **Exigences par type de flux**

Type de flux	Protocole minimum	Configuration	Validation
Internet → Application client	TLS 1.3	Forward Secrecy, HSTS, CT	Tests automatisés hebdomadaires
Application client → Backend	TLS 1.3 + chiffrement	Certificate Pinning, key attestation	Tests continus

	message		
Backend → Backend	TLS 1.3 ou IPsec	Authentification mutuelle	Validation automatisée
Intra-datacenter	TLS 1.2 minimum	Authentification	Scan réseau mensuel
Cloud privé	TLS 1.3 ou mTLS	Authentification forte	Validation CSPM
Sauvegarde	Chiffrement transport + contenu	Clés séparées	Vérification intégrité
Administration	SSH v2, RDP sur TLS	Clés ou MFA	Enregistrement sessions

2. **Sécurisation des endpoints**
    - Validation stricte des certificats
    - Certificate Transparency pour les certificats publics
    - DNSSEC et DNS over HTTPS/TLS
    - Mise en œuvre systématique du HSTS
    - CAA DNS pour contrôler l'émission de certificats
3. **Protection contre les attaques sur le chiffrement**
    - Désactivation des protocoles obsolètes
    - Configuration sécurisée des suites cryptographiques
    - Protection contre le downgrade
    - Renouvellement régulier des certificats
    - Surveillance des tentatives d'attaque

9.3 Chiffrement des sauvegardes

Neo Financia applique des mesures spécifiques pour la protection des sauvegardes :

1. **Principes de chiffrement**
    - Chiffrement systématique de toutes les sauvegardes
    - Chiffrement indépendant du système source
    - Clés dédiées distinctes des clés opérationnelles
    - Protection renforcée des clés de sauvegarde
    - Validation de l'intégrité avant et après restauration
2. **Gestion des clés de sauvegarde**
    - Hiérarchie de clés dédiée
    - Conservation sécurisée à long terme
    - Documentation précise des relations clés/sauvegardes
    - Test périodique de récupération
    - Procédure de restauration d'urgence
3. **Procédures opérationnelles**
    - Validation du chiffrement avant transfert
    - Contrôle d'intégrité à chaque étape

- Séparation des rôles pour sauvegarde et restauration
- Journalisation des opérations
- Audit régulier des procédures

9.4 Chiffrement dans les environnements cloud

Neo Financia applique une stratégie de chiffrement spécifique à ses environnements cloud :

1. **Principes généraux**
   - Approche BYOK (Bring Your Own Key) privilégiée
   - Séparation des clés par environnement et service
   - Rotation automatisée via les services natifs
   - Surveillance des opérations sur les clés
   - Audit régulier des configurations
2. **Solutions par fournisseur**

Fournisseur	Services de gestion de clés	Technologies de chiffrement	Contrôles spécifiques
Azure (70%)	Azure Key Vault	Storage Service Encryption, ADE, SQL TDE	Managed HSM, Access Policies, RBAC
OVHcloud (20%)	OVH Managed Keys	Object Storage Encryption, Instance Encryption	IAM, vRack isolation
AWS (10%)	AWS KMS, CloudHSM	S3 Encryption, EBS Encryption, RDS Encryption	IAM, CMKs, Policy Controls

3. **Contrôles supplémentaires**
   - CSPM (Cloud Security Posture Management) pour validation continue
   - Inventaire automatisé des ressources chiffrées
   - Validation de conformité des configurations
   - Détection des données non chiffrées
   - Tests d'intrusion spécifiques

10. Conformité réglementaire et audit

10.1 Exigences réglementaires

Neo Financia doit se conformer à plusieurs réglementations ayant des exigences spécifiques en matière de cryptographie :

1. **RGPD / UK GDPR**
   - Mise en œuvre de mesures techniques appropriées pour la protection des données
   - Chiffrement et pseudonymisation comme mesures de sécurité exemplaires
   - Documentation des choix cryptographiques
   - Analyses d'impact pour les traitements sensibles
2. **DSP2 / PSD2**

- Authentification forte du client (SCA)
- Sécurisation des canaux de communication
- Protection cryptographique des données de paiement
- Standards d'authentification et de signature

3. **DORA (Digital Operational Resilience Act)**
   - Résilience opérationnelle numérique
   - Protection cryptographique des systèmes critiques
   - Tests réguliers des mécanismes cryptographiques
   - Plans de continuité intégrant la cryptographie
4. **PCI-DSS**
   - Chiffrement des données de cartes
   - Gestion sécurisée des clés cryptographiques
   - Documentation des processus
   - Tests réguliers des mécanismes
5. **eIDAS**
   - Exigences pour les signatures électroniques
   - Standards pour les certificats qualifiés
   - Horodatage qualifié
   - Conservation des preuves

10.2 Documentation de conformité

Neo Financia maintient une documentation complète pour démontrer sa conformité :

1. **Documentation requise**
   - Politique cryptographique (présent document)
   - Standard de gestion des clés détaillé
   - Procédures opérationnelles
   - Résultats d'évaluation des risques
   - Rapports d'audit
   - Résultats des tests
   - Documentation des exceptions avec justifications
2. **Matrices de traçabilité**
   - Mappage des contrôles cryptographiques aux exigences réglementaires
   - Démonstration de couverture complète
   - Identification des interdépendances
   - Gestion des évolutions réglementaires
3. **Registres**
   - Inventaire des algorithmes et protocoles utilisés
   - Registre des HSM et dispositifs de stockage
   - Catalogue des certificats et autorités
   - Registre des exceptions avec durée de validité
   - Historique des incidents et résolutions

10.3 Évaluation et certification

Neo Financia procède à des évaluations régulières de ses mécanismes cryptographiques :

1. **Audits internes**
    - Audit annuel complet par l'équipe d'audit interne
    - Vérification trimestrielle par l'équipe sécurité
    - Tests de conformité automatisés
    - Revue de code ciblée sur les implémentations cryptographiques
    - Simulation d'incidents et tests de récupération
2. **Audits externes**
    - Audit annuel par un prestataire spécialisé
    - Test d'intrusion ciblé sur les mécanismes cryptographiques
    - Évaluation formelle tous les 2 ans
    - Certification PCI-DSS annuelle
    - Qualification RGS pour les fonctions critiques
3. **Certification et qualification**
    - Respect des standards ETSI pour les signatures avancées
    - Qualification des dispositifs selon les référentiels appropriés
    - Certification ANSSI pour les fonctions critiques
    - Conformité aux standards internationaux (NIST, ISO)

10.4 Veille réglementaire et technologique

Neo Financia maintient un processus actif de veille :

1. **Veille réglementaire**
    - Suivi des évolutions normatives (RGPD, DSP2, DORA, etc.)
    - Participation aux groupes de travail sectoriels
    - Relations avec les autorités de régulation
    - Mise à jour régulière des matrices de conformité
2. **Veille technologique**
    - Suivi des avancées en cryptographie
    - Surveillance des vulnérabilités et attaques
    - Évaluation des impacts sur les systèmes existants
    - Préparation aux évolutions (cryptographie post-quantique)
3. **Processus d'adaptation**
    - Évaluation d'impact pour chaque évolution significative
    - Planification des migrations et transitions
    - Tests préalables dans des environnements isolés
    - Documentation des décisions et justifications

11. Gestion des incidents liés aux clés

11.1 Types d'incidents

Neo Financia identifie plusieurs catégories d'incidents liés aux clés cryptographiques :

1. **Compromission de clés**
    - Divulgation non autorisée

- Vol de clés ou de matériel cryptographique
- Extraction par canal auxiliaire
- Exposition accidentelle

2. **Perte d'accès**

   - Perte de clés sans sauvegarde
   - Défaillance des dispositifs de stockage
   - Corruption des données cryptographiques
   - Oubli des éléments d'activation

3. **Défaillance cryptographique**

   - Découverte de vulnérabilités dans les algorithmes
   - Faiblesse dans la génération des clés
   - Implémentation incorrecte des protocoles
   - Échec des mécanismes de validation

4. **Problèmes opérationnels**

   - Expiration non anticipée de certificats
   - Échec de la rotation des clés
   - Désynchronisation des systèmes cryptographiques
   - Erreurs dans les procédures de gestion

11.2 Détection des incidents

Neo Financia met en œuvre plusieurs mécanismes pour détecter les incidents liés aux clés :

1. **Surveillance technique**

   - Détection des accès non autorisés aux systèmes de gestion des clés
   - Monitoring des opérations cryptographiques anormales
   - Alertes sur les échecs d'opérations
   - Surveillance des performances et comportements
   - Détection des modifications non autorisées

2. **Alertes préventives**

   - Notification anticipée d'expiration de certificats
   - Alerte sur les certificats révoqués
   - Surveillance des bulletins de sécurité cryptographique
   - Détection des tentatives d'attaque

3. **Canaux de remontée**

   - Signalement par les utilisateurs
   - Remontée par les équipes opérationnelles
   - Alertes automatisées des systèmes
   - Information par les partenaires ou fournisseurs

11.3 Réponse aux incidents

Neo Financia a défini des procédures spécifiques pour la gestion des incidents liés aux clés :

1. **Processus général**

- Détection et qualification initiale
- Évaluation de l'impact et de l'urgence
- Confinement et isolation des systèmes concernés
- Investigation technique approfondie
- Mise en œuvre des mesures correctrices
- Retour à la normale et validation
- Documentation et retour d'expérience

2. **Mesures spécifiques par type d'incident**

Type d'incident	Actions immédiates	Mesures de remédiation	Parties à informer
Compromission de clé	Révocation immédiate, isolation des systèmes concernés	Renouvellement des clés, analyse forensique	RSSI, COMEX, autorités si applicable
Perte d'accès	Activation des procédures de récupération	Restauration depuis sauvegarde, reconstruction si nécessaire	RSSI, responsables des systèmes affectés
Faiblesse cryptographique	Évaluation de l'exploitabilité, renforcement des contrôles	Migration vers des algorithmes sûrs	RSSI, équipes techniques
Expiration certificat	Déploiement d'urgence d'un nouveau certificat	Amélioration des procédures de surveillance	Équipes opérationnelles

3. **Niveaux d'escalade**
   - Niveau 1 : Gestion par l'équipe cryptographique
   - Niveau 2 : Escalade au RSSI et responsables concernés
   - Niveau 3 : Activation de la cellule de crise
   - Niveau 4 : Implication du COMEX et communication externe

11.4 Communication et notification

En cas d'incident lié aux clés cryptographiques, Neo Financia applique des règles précises de communication :

1. **Communication interne**

   - Information immédiate des équipes concernées
   - Escalade selon la gravité
   - Mise à jour régulière sur l'avancement
   - Coordination avec les autres équipes (juridique, communication)

2. **Notification externe**

   - Évaluation des obligations légales de notification
   - Information aux partenaires impactés
   - Communication aux clients si nécessaire
   - Notification aux autorités compétentes selon la réglementation

3. **Obligations spécifiques**
    - Notification CNIL/ICO pour les violations de données personnelles (72h)
    - Information à l'ANSSI/NCSC pour les incidents majeurs
    - Notification aux autorités financières selon les seuils définis
    - Communication aux schémas de paiement si applicable

11.5 Récupération et leçons apprises

Suite à un incident lié aux clés, Neo Financia applique un processus structuré de récupération et d'amélioration :

1. **Procédures de récupération**
    - Génération de nouvelles clés selon les procédures standards
    - Renouvellement des certificats affectés
    - Rechiffrement des données avec les nouvelles clés si nécessaire
    - Validation complète après récupération
    - Documentation détaillée des actions réalisées
2. **Analyse post-incident**
    - Investigation approfondie des causes racines
    - Évaluation de l'efficacité de la réponse
    - Identification des améliorations nécessaires
    - Documentation formelle et partage des enseignements
3. **Mise à jour des procédures**
    - Révision des politiques et procédures concernées
    - Renforcement des contrôles si nécessaire
    - Adaptation des mécanismes de détection
    - Formation complémentaire des équipes

12. Annexes techniques

12.1 Matrice RACI détaillée

Activité	RSSI	Resp. Crypto	Admin PKI	Key Custodians	Équipe Sécurité	Équipe Infra.	Équipe Dev.
Gouvernance							
Définition de la politique	A/R	R	C	I	C	C	C
Mise à jour standards	A	R	C	I	C	C	C
Revue annuelle	A	R	C	I	C	C	C
Gestion exceptions	A	R	C	I	C	C	C
Cycle de vie PKI							
Cérémonie AC	A	R	R	R	C	I	I

Racine							
Émission AC intermédiaires	A	R	R	R	C	I	I
Émission certificats	I	A	R	I	C	I	I
Révocation certificats	I	A	R	I	C	I	I
Cycle de vie des clés							
Génération clés critiques	A	R	R	R	C	I	I
Gestion clés applicatives	I	A	C	I	C	R	R
Rotation clés	I	A	R	C	C	R	R
Destruction clés	I	A	R	C	C	I	I
Opérations							
Surveillance quotidienne	I	A	R	I	R	C	I
Gestion HSM	I	A	R	C	C	C	I
Backup des clés	I	A	R	C	C	I	I
Audit des accès	I	C	C	I	A/R	I	I
Incidents							
Gestion incidents mineurs	I	A/R	R	I	R	C	C
Gestion incidents majeurs	A	R	R	C	R	R	C
Communication externe	A	C	I	I	C	I	I
Analyse post-incident	A	R	C	I	R	C	C
Évaluation et conformité							
Audit interne	I	C	C	I	C	C	C
Tests de	I	C	C	I	A/R	C	C

pénétration							
Évaluation réglementaire	A	R	C	I	C	I	I
Reporting conformité	A	R	I	I	C	I	I

Légende :

- R : Responsable (exécute l'action)
- A : Autorité (approuve et est responsable de l'action)
- C : Consulté (doit être consulté avant l'action)
- I : Informé (doit être informé du résultat)

12.2 Architecture détaillée de la PKI

[Diagramme d'architecture de la PKI avec tous les niveaux et composants]

La PKI de Neo Financia est organisée en quatre niveaux :

1. **AC Racine (Neo Financia Root CA)**
    - Certificat auto-signé de 20 ans
    - Clé RSA 8192 bits
    - Stockage dans un HSM dédié hors ligne
    - Cérémonie des clés avec 5 témoins minimum
    - Stockage physique dans un coffre-fort sécurisé
    - Activation nécessitant un quorum de 3 sur 5
    - Audit vidéo de toutes les opérations
2. **AC Intermédiaires (3)**
    - Neo Financia Internal CA
        - Pour les besoins internes
        - Clé RSA 4096 bits
        - Validité 10 ans
    - Neo Financia Services CA
        - Pour les services externes
        - Clé ECDSA P-384
        - Validité 10 ans
    - Neo Financia Partner CA
        - Pour l'émission de certificats partenaires
        - Clé ECDSA P-384
        - Validité 10 ans
3. **AC Émettrices (5)**
    - Neo Financia Employee CA
        - Certificats d'authentification et signature pour les collaborateurs
        - Clé ECDSA P-384
        - Validité 5 ans
    - Neo Financia Server CA
        - Certificats serveurs internes
        - Clé ECDSA P-384

        - Validité 5 ans
    - Neo Financia Application CA
        - Certificats pour les applications
        - Clé ECDSA P-384
        - Validité 5 ans
    - Neo Financia Client CA
        - Certificats client pour l'authentification forte
        - Clé ECDSA P-384
        - Validité 5 ans
    - Neo Financia Code Signing CA
        - Certificats pour la signature de code
        - Clé RSA 4096 bits
        - Validité 5 ans

4. **Certificats d'entité finale**
    - Multiples usages selon les besoins
    - Durée de validité limitée (1-3 ans)
    - Contraintes d'usage strictes

12.3 Procédure de cérémonie des clés

La génération des clés maîtres suit une procédure formelle de cérémonie des clés :

1. **Préparation**
    - Nomination des participants et définition des rôles
    - Préparation du script détaillé de la cérémonie
    - Vérification et préparation des équipements
    - Aménagement de la salle sécurisée
    - Test préalable des HSM et supports
2. **Déroulement**
    - Authentification de tous les participants
    - Vérification de l'intégrité des équipements
    - Génération des clés selon le script précis
    - Sauvegarde sécurisée des composants
    - Journalisation détaillée de toutes les opérations
    - Enregistrement vidéo complet
    - Signature du procès-verbal par tous les participants
3. **Post-cérémonie**
    - Sécurisation des composants dans les coffres-forts
    - Sauvegarde sécurisée de la documentation
    - Conservation des preuves
    - Audit indépendant du déroulement
    - Test de validation des clés générées

12.4 Procédures opérationnelles standards

Neo Financia maintient des procédures opérationnelles standards pour les principales opérations cryptographiques :

1. **Émission de certificat**

- Vérification de l'identité du demandeur
- Validation de la demande
- Génération sécurisée des clés
- Signature du certificat
- Publication dans l'annuaire
- Notification au demandeur
- Journalisation de l'opération

2. **Révocation de certificat**

- Vérification de l'autorité du demandeur
- Validation du motif de révocation
- Exécution de la révocation
- Mise à jour de la CRL et OCSP
- Notification aux parties concernées
- Journalisation de l'opération

3. **Rotation des clés de chiffrement**

- Préparation des nouvelles clés
- Validation technique et fonctionnelle
- Période de transition (double validité)
- Migration des données chiffrées
- Désactivation des anciennes clés
- Archivage sécurisé
- Vérification post-rotation

4. **Sauvegarde et restauration des HSM**

- Authentification des opérateurs autorisés
- Activation du mode backup/restore
- Exécution de la sauvegarde/restauration chiffrée
- Vérification de l'intégrité
- Stockage sécurisé des sauvegardes
- Journalisation détaillée
- Test de validation post-opération

12.5 Standards techniques détaillés

12.5.1 Configuration TLS

La configuration TLS des serveurs doit respecter les paramètres suivants :

```
# Exemple de configuration NGINX
ssl_protocols TLSv1.2 TLSv1.3;
ssl_prefer_server_ciphers on;
ssl_ciphers 'ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-
CHACHA20-POLY1305:ECDHE-RSA-CHACHA20-POLY1305:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-
AES128-GCM-SHA256';
ssl_ecdh_curve secp384r1;
ssl_session_timeout 10m;
ssl_session_cache shared:SSL:10m;
ssl_session_tickets off;
ssl_stapling on;
ssl_stapling_verify on;
add_header Strict-Transport-Security "max-age=63072000; includeSubDomains; preload";
```

12.5.2 Paramètres de génération des clés RSA

```
# Exemple de génération de clé RSA avec OpenSSL
openssl genpkey -algorithm RSA -pkeyopt rsa_keygen_bits:4096 -aes-256-cbc -out
private_key.pem
```

12.5.3 Paramètres de génération des clés ECDSA

```
# Exemple de génération de clé ECDSA avec OpenSSL
openssl genpkey -algorithm EC -pkeyopt ec_paramgen_curve:P-384 -aes-256-cbc -out
private_key.pem
```

12.5.4 Format de stockage des clés

- Clés privées : Format PKCS#8 chiffré
- Clés publiques : Format X.509 SubjectPublicKeyInfo
- Certificats : Format X.509 v3
- Archivage : Format PKCS#12 avec protection forte

12.5.5 Paramètres de l'algorithme AES

- Mode GCM privilégié
- Taille de clé : 256 bits
- IV unique pour chaque opération de chiffrement
- Tag d'authentification de 128 bits
- AAD (Additional Authenticated Data) systématique pour les données structurées

12.6 Spécifications des HSM

Neo Financia utilise différents modèles de HSM selon les besoins :

1. **HSM AC Racine**
    - Modèle : Thales Luna Network HSM 7
    - Certification : FIPS 140-2 niveau 3, Critères Communs EAL4+
    - Configuration : Standalone, déconnecté du réseau
    - Stockage : Dans un coffre-fort sécurisé
    - Activation : Cartes à puce avec quorum (3 sur 5)
    - Maintenance : Contrat de support premium
2. **HSM PKI et signature**
    - Modèle : Thales Luna Network HSM 7
    - Certification : FIPS 140-2 niveau 3
    - Configuration : Cluster hautement disponible
    - Stockage : Salle sécurisée avec contrôle d'accès
    - Activation : Authentification multifacteur
    - Maintenance : Contrat de support 24/7
3. **HSM transactions financières**
    - Modèle : Utimaco PaymentServer
    - Certification : PCI HSM, PCI-DSS
    - Configuration : Cluster actif-actif
    - Stockage : Datacenter principal et secondaire
    - Activation : Par système automatisé sécurisé
    - Maintenance : Contrat de support critique

4. **HSM cloud (Azure)**
    - Service : Azure Dedicated HSM
    - Certification : FIPS 140-2 niveau 3
    - Configuration : Déploiement redondant
    - Contrôle : Accès via Azure Key Vault avec RBAC strict
    - Utilisation : Protection des clés dans le cloud Azure

12.7 Glossaire technique

Terme	Définition
AES (Advanced Encryption Standard)	Algorithme de chiffrement symétrique standardisé par le NIST, utilisé par Neo Financia avec une clé de 256 bits.
Algorithme asymétrique	Méthode cryptographique utilisant une paire de clés (publique et privée) mathématiquement liées.
Algorithme symétrique	Méthode cryptographique utilisant la même clé pour le chiffrement et le déchiffrement.
Autorité de Certification (AC)	Entité émettant des certificats numériques qui lient une clé publique à une identité.
BYOK (Bring Your Own Key)	Approche permettant d'utiliser ses propres clés dans un service cloud tiers.
Certificat X.509	Format standard de certificat à clé publique, utilisé dans l'infrastructure PKI de Neo Financia.
Chiffrement de bout en bout	Protection des données qui restent chiffrées de leur point d'origine à leur destination finale.
Chiffrement homomorphe	Technique permettant d'effectuer des calculs sur des données chiffrées sans les déchiffrer.
CRL (Certificate Revocation List)	Liste des certificats révoqués avant leur date d'expiration.
Cryptographie post-quantique	Méthodes cryptographiques résistantes aux attaques d'un ordinateur quantique.
DSP2 (Directive sur les Services de Paiement 2)	Réglementation européenne imposant notamment l'authentification forte pour les paiements.
ECDSA (Elliptic Curve Digital Signature Algorithm)	Algorithme de signature numérique basé sur les courbes elliptiques.
FIPS 140-2/3	Norme gouvernementale américaine spécifiant les exigences de sécurité pour les modules cryptographiques.
HSM (Hardware Security Module)	Module matériel dédié à la protection des clés cryptographiques et à l'exécution d'opérations cryptographiques.

JWE (JSON Web Encryption)	Format standard pour représenter du contenu chiffré utilisant JSON.
JWS (JSON Web Signature)	Format standard pour représenter du contenu signé utilisant JSON.
KMS (Key Management System)	Système centralisé pour la gestion du cycle de vie des clés cryptographiques.
mTLS (mutual TLS)	Authentification TLS où les deux parties présentent des certificats, utilisée pour les API partenaires.
OCSP (Online Certificate Status Protocol)	Protocole permettant de vérifier en temps réel le statut de révocation d'un certificat.
PCI-DSS	Norme de sécurité pour les cartes de paiement, incluant des exigences cryptographiques.
PFS (Perfect Forward Secrecy)	Propriété garantissant que la compromission d'une clé à long terme ne compromet pas les clés de session passées.
PKI (Public Key Infrastructure)	Infrastructure à clés publiques permettant la création, gestion et révocation des certificats numériques.
RGPD (Règlement Général sur la Protection des Données)	Réglementation européenne sur la protection des données personnelles.
RSA	Algorithme cryptographique à clé publique utilisé pour le chiffrement et la signature.
SCA (Strong Customer Authentication)	Authentification forte du client requise par la DSP2, combinant au moins deux facteurs indépendants.
TDE (Transparent Data Encryption)	Technologie de chiffrement au niveau de la base de données.
TLS (Transport Layer Security)	Protocole cryptographique sécurisant les communications sur les réseaux, version 1.3 privilégiée par Neo Financia.
Tokenisation	Remplacement de données sensibles par des substituts non sensibles, utilisé notamment pour les données de cartes bancaires.