

I. Objectif et champs d'application

Cette procédure a pour objet de définir les règles, les rôles et les modalités opérationnelles de gestion des clés cryptographiques au sein de la Banque de l'Union – Côte d'Ivoire (BDU-CI). Elle vise à garantir une gestion sécurisée, traçable et conforme des clés utilisées pour le chiffrement des données sensibles, notamment dans les environnements critiques tels que la monétique, les bases de données, les échanges interbancaires ou les systèmes d'authentification.

Elle s'inscrit dans une démarche globale de renforcement de la sécurité de l'information, en conformité avec les exigences de la norme PCI-DSS et les bonnes pratiques en matière de cryptographie, afin d'assurer la confidentialité, l'intégrité et la disponibilité des données bancaires.

Cette procédure s'applique à l'ensemble des entités techniques et fonctionnelles impliquées dans la génération, la distribution, le stockage, la rotation et la révocation des clés cryptographiques, et concerne les cas suivants :

- Gestion des clés de chiffrement utilisées dans les bases de données, les fichiers et les systèmes applicatifs (**Swift** et autres application) ;
- Gestion des clés au sein des modules de sécurité matériels (HSM) ;
- Partage, protection et renouvellement des clés maîtresses (LMK, TMK, etc...) ;
- Répartition des responsabilités entre les différentes parties prenantes (DSI, Exploitation, Sécurité, Réseau, Directeur du contrôle permanent et de la conformité, etc.) ;
- Conformité aux règles d'audit, de traçabilité et de conservation des preuves.

II. Objectifs de la procédure

L'objectif de cette procédure est de définir les rôles, responsabilités et mécanismes opérationnels encadrant la gestion sécurisée du cycle de vie des clés cryptographiques utilisées au sein de la Banque de l'Union – Côte d'Ivoire (BDU-CI). Elle vise à garantir la génération, la distribution, le stockage, l'usage, la rotation et la révocation des clés dans le respect des normes de sécurité les plus strictes, notamment celles relatives à la confidentialité, à l'intégrité et à l'authenticité des données sensibles.

Elle s'inscrit dans une démarche proactive de réduction des risques liés à la compromission de clés, à l'utilisation inadéquate de la cryptographie, ou à la non-conformité avec les exigences réglementaires (PCI-DSS, ISO 27001, ANSSI), et permet :

- De protéger les clés et données critiques contre tout accès, usage ou divulgation non autorisés ;
- De garantir une séparation stricte des rôles et une traçabilité complète des manipulations cryptographiques ;
- D'assurer la continuité et la fiabilité des opérations bancaires impliquant le chiffrement ou la signature électronique ;
- De prévenir les pertes de données ou interruptions de services liés à une mauvaise gestion des clés ;
- De faciliter les audits internes et externes en centralisant les enregistrements et preuves de conformité.

Cette procédure couvre les domaines suivants :

- Génération et stockage des clés (symétriques, asymétriques, maîtresses, de session) ;
- Distribution, injection et activation des clés dans les équipements ou applications ;
- Rotation périodique ou en cas d'incident, et révocation des clés obsolètes ;
- Sécurisation des environnements matériels et logiciels de gestion des clés (HSM, coffres-forts, etc.) ;
- Journalisation, supervision et conservation des événements liés aux clés.

III. Rôles et responsabilités

RÔLE	RESPONSABILITÉ
DSI	Superviser l'environnement technique et garantir la mise en œuvre sécurisée des outils de gestion des clés cryptographique.
RSSI	Valider les règles de gestion des clés, superviser l'ensemble du cycle de vie des clés, assurer la conformité aux normes (ISO 27001, PCI-DSS, ANSSI, etc.).
Directeur du contrôle permanent et de la conformité (DCPC)	Conserve les clés physiques LMK dans un coffre-fort installé dans son bureau. Le DCPC possède les clés avec un second désigné.
SSI	Mettre en œuvre les opérations de génération, d'injection, de rotation et de révocation des clés ; assurer la traçabilité et la séparation des rôles.
Exploitant HSM	Administrer les HSM et coffres-forts cryptographiques, assurer la disponibilité et la sécurité des plateformes de gestion des clés.
Manager Métier / Responsable applicatif	Coordonner avec la SSI les besoins applicatifs nécessitant l'utilisation de clés, s'assurer que les accès soient limités aux usages autorisés.
Utilisateur habilité	Respecter les procédures de manipulation des clés, ne jamais stocker ni transmettre de clé sans chiffrement ou en dehors des canaux sécurisés.

IV. Sigles et Définitions

➤ Définitions

Clé cryptographique : Élément numérique utilisé dans un algorithme de chiffrement ou de signature électronique pour sécuriser des données ou des transactions.

Cycle de vie des clés : Ensemble des étapes liées à la gestion d'une clé cryptographique, depuis sa génération jusqu'à sa révocation ou destruction.

Injection de clé : Processus d'introduction sécurisée d'une clé dans un équipement (HSM, serveur, terminal...).

Coffre-fort cryptographique : Environnement logiciel ou matériel utilisé pour stocker et protéger les clés de manière sécurisée.

Séparation des rôles : Principe de sécurité consistant à attribuer des fonctions distinctes à différentes personnes afin d'éviter qu'un seul individu puisse compromettre la sécurité du système.

Rotation de clé : Remplacement périodique d'une clé par une nouvelle pour renforcer la sécurité des données chiffrées.

Compromission de clé : Situation dans laquelle une clé cryptographique a pu être exposée ou interceptée, nécessitant sa révocation immédiate.

➤ **Sigles**

HSM : Host Security Module : module matériel sécurisé pour la gestion des clés.

TMK : Terminal Master Key : clé maître utilisée pour un terminal de paiement.

LMK : Local Master Key : clé maître locale d'un HSM.

KCV : Key Check Value : valeur de contrôle utilisée pour vérifier une clé.

PKI : Public Key Infrastructure : infrastructure de gestion de certificats et clés.

ATM : Automated Teller Machine : Distributeur automatique de billets.

AWK : Aquirer Working Key ; Clé de travail de l'acquéreur.

CDE : Card holder Data Environment : Détenteur de la carte Données Environnement.

CHD : Card Holder Data : Données du titulaire de la carte.

CV : Card Verification Value : Valeur de vérification de la carte.

DAB : Distributeur Automatique de Billets.

DPC : Données de porteurs de cartes.

IPS : Intrusion Prevention System : Système de prévention des intrusions.

IWK : Issuer Working Key : Clé de travail de l'émetteur.

PGP : Pretty Good Privacy.

PVV : Pin Verification Value : Valeur de vérification des pins.

SAD : Sensitive Authentication Data : Données d'authentification sensibles.

TPK : Terminal Pin Key ;

Sommaire de la procédure

I. Objectif et champs d'application	1
II. Objectifs de la procédure.....	2
III. Rôles et responsabilités	3
IV. Sigles et Définitions.....	3
V. Références / Règles de gestion.....	5
VI. Narratif de la procédure	12

V. Références / Règles de gestion

❖ Documents de références

- Norme ISO/IEC 27001 : 2022 ;
- Politique de sécurité des systèmes d'information de la BDU-CI ;

❖ Règles de gestion (Processus de gestion des clés cryptographiques)

➤ Règles générales

- Protéger les clés de cryptage utilisées pour le cryptage des données des titulaires de cartes contre la divulgation et l'utilisation illicite.
- Restreindre l'accès aux clés cryptographiques au plus petit nombre d'opérateurs possible.
- Stocker les clés cryptographiques de manière sécurisée peu d'emplacements et formes que possible.

- Documenter en détail et déployer les processus et les procédures de gestion des clés cryptographiques servant au cryptage des données des titulaires de cartes, notamment ce qui suit :
 - Génération de clés cryptographiques robustes : longueur de 256 bits minimum pour les clés de protocoles de chiffrement symétriques.
 - Sécuriser la distribution des clés cryptographiques.
 - Sécuriser le stockage des clés cryptographiques.
 - Modifier périodiquement les clés cryptographiques au moins une fois par an.
 - Retrait ou remplacement des clés cryptographiques obsolètes ou soupçonnées d'avoir été compromises.
 - Fractionner les connaissances et l'établissement d'un double contrôle des clés cryptographiques.
 - Empêcher la substitution non autorisée des clés cryptographiques.
 - Exiger aux opérateurs chargés de la gestion de clés cryptographiques de signer l'engagement de protection des clés de cryptage, reconnaissant qu'ils comprennent et acceptent leurs responsabilités.

➤ **Description de la procédure**

Cette partie présente les procédures opérationnelles liées à la mise en place des règles de gestion des clés de cryptage de BDU-CI. Ces procédures concernent :

- Les clés de cryptage des bases de données
- Les clés de cryptage des fichiers
- Les clés de cryptages des applications (cas de SWIFT)
- Les clés de cryptage HSM

➤ **Chiffrement des bases de données**

Description de la solution de chiffrement : Les colonnes contenant des données sensibles telles que le numéro de carte (PAN), le nom du porteur, la date d'expiration et le

code service doivent être chiffrées à l'aide d'un mécanisme de chiffrement transparent intégré au moteur de base de données. Ce chiffrement s'appuie sur l'algorithme AES avec une clé de 256 bits, conformément aux meilleures pratiques de sécurité et aux exigences des normes telles que PCI-DSS.

ID	RESPONSABLE / INTERVENANTS	DESCRIPTION	DOCUMENTS PRODUIT
1	Service Exploitation et Production	Génération de la clé de chiffrement, création du conteneur sécurisé (coffre/keystore), sauvegarde de la première partie du mot de passe.	1 - PV de génération de la clé ; 2 - Signature d'un engagement de confidentialité.
2	Service Sécurité des SI	Sauvegarde de la seconde partie du mot de passe du conteneur sécurisé.	Signature d'un engagement de confidentialité

Génération des clés : Les clés de chiffrement sont générées à l'aide d'un module de chiffrement conforme aux standards internationaux. La génération est effectuée par un administrateur habilité, suivant une procédure documentée validée par le RSSI et conformément au processus de gestion des changements.

Distribution des clés : Les clés sont stockées exclusivement sur les environnements autorisés (ex : cluster de bases de données) dans un conteneur sécurisé (keystore ou coffre-fort cryptographique). En cas de site de secours, la réplication des clés est assurée via un mécanisme sécurisé de synchronisation ou de réplication de disques, garantissant l'intégrité et la confidentialité.

Stockage des clés : Les clés sont stockées dans un conteneur chiffré protégé par un mot de passe réparti entre plusieurs entités afin de garantir la séparation des rôles.

- Les premiers caractères du mot de passe sont conservés par le Service Exploitation et Production ;

- Les derniers caractères sont détenus par le Service Sécurité des Systèmes d'Information.

La détention de ces éléments est conditionnée à la signature d'un engagement formel de confidentialité et de protection des clés.

Rotation et changement des clés : Les clés de chiffrement et les mots de passe associés doivent être renouvelés au moins une fois par an ou à chaque changement de contexte critique (changement d'infrastructure, compromission suspectée, audit majeur...). Le processus de changement suit une procédure formalisée et validée par la Direction des Systèmes d'Information et la Sécurité des SI. Après chaque changement, les parties prenantes renouvellent leur engagement écrit de protection des clés.

➤ **Chiffrement des fichiers**

Description de la solution de cryptage. La solution de chiffrement mise en place au sein de la Banque permet de protéger les données sensibles contre tout accès non autorisé, aussi bien pendant leur stockage, utilisation que durant leur transfert.

Deux niveaux de chiffrement sont appliqués :

- Le chiffrement complet de disque, utilisé pour sécuriser l'ensemble des données stockées sur les ordinateurs portables, postes de travail, serveurs ou périphériques mobiles ;
- Le chiffrement de fichiers et de dossiers spécifiques, permettant de cibler précisément les informations à sécuriser, de manière granulaire.

Dans les deux cas, le chiffrement est effectué de manière transparente et automatique, sans intervention particulière de l'utilisateur, et avec un impact minimal sur les performances du système.

L'algorithme utilisé est AES (Advanced Encryption Standard), avec une clé de 256 bits, conformément aux standards de sécurité reconnus (ISO/IEC 27001, PCI-DSS, recommandations ANSSI).

Le chiffrement est géré via une infrastructure centralisée, permettant l'administration des politiques de sécurité, la gestion des groupes d'utilisateurs et la répartition des droits de chiffrement/déchiffrement. Les clés sont générées, distribuées, utilisées, stockées et renouvelées de manière contrôlée et traçable par l'équipe infrastructure.

ID	RESPONSABLE / INTERVENANTS	DESCRIPTION	DOCUMENTS PRODUIT
1	Service Infrastructure Systèmes et Réseaux	Génération des clés, gestion des groupes d'utilisateurs, suivi des accès et renouvellement des clés.	1 - PV de génération des clés. 2 - Engagement de confidentialité

Génération des clés : L'administrateur en charge procède à la génération des clés de chiffrement pour chaque groupe d'utilisateurs ou équipement, selon les politiques de sécurité définies.

Distribution des clés : Les clés sont distribuées de façon sécurisée aux utilisateurs ou aux équipements en fonction de leur appartenance à un groupe prédéfini, et selon des mécanismes de provisioning automatique.

Stockage des clés : Les clés sont stockées à la fois sur un serveur central sécurisé et, si nécessaire, sur les postes clients concernés. Leur protection repose sur un mécanisme de chiffrement complémentaire, ainsi qu'un contrôle strict des accès.

Changement et rotation des clés : La rotation des clés de chiffrement est configurée pour intervenir au moins une fois par an, ou plus fréquemment en cas d'évolution du risque, de

compromission ou de changement de contexte. L'ensemble du processus est documenté et suivi par l'équipe en charge.

➤ **Procédures de gestion des clés LMK**

Description de la solution : La gestion des clés de chiffrement applicatif (en particulier pour le cas de Swift) devrait idéalement être assurée par un module matériel de sécurité (HSM), conformément aux bonnes pratiques en matière de sécurité cryptographique. Dans un environnement bancaire, il serait recommandé de déployer au moins deux HSM dans le site de production : un en mode actif pour traiter les opérations en temps réel, et un second en mode passif servant de système de secours. Ce HSM secondaire pourrait ainsi prendre automatiquement le relais en cas de défaillance du HSM principal, assurant ainsi la résilience et la disponibilité continue des services critiques.

Génération des clés : L'administrateur du HSM générera les clés LMK selon les meilleures pratiques recommandées par le fournisseur.

Distribution des clés, Les trois clés LMK, composant la clé maîtresse LMK, sont générées par le HSM de production ainsi que les mots de passe correspondants. Ils sont détenus par les trois personnes suivantes : (Chacun des titulaires devra désigner un suppléant distinct, lequel connaîtra uniquement la portion du mot de passe correspondant au titulaire qu'il remplace, afin de pallier toute éventuelle indisponibilité de ce dernier.) :

- Chef de division d'exploitation informatique ;
- Chef de Service Sécurité SI (RSSI) ;
- Responsable conformité et réglementaire.

Ces personnes (titulaires + suppléants) doivent s'engager à reconnaître, comprendre et accepter leurs responsabilités, relative à la possession des clés citées ci-dessus en signant l'engagement de protection des clés de cryptage.

Stockage des clés : Les trois clés physiques LMK sont conservées dans un coffre-fort situé dans le bureau du DCPC. L'accès à ce coffre-fort est exclusivement connu du DCPC, ainsi que d'un suppléant désigné pour pallier tout éventuelle indisponibilité. Mais les codes permettant l'utilisation des clés physiques LMK à l'intérieur du coffre-fort ne sont connus que des trois personnes précédemment mentionnées et leurs suppléants au besoin.

Utilisation des clés : Dès qu'un besoin d'utilisation des clés physiques LMK est identifié, une demande formelle (par courriel ou via un formulaire dédié) doit être adressée au DCPC par l'entité requérante. Après validation par les personnes habilitées, le DCPC (ou son suppléant) remet les trois clés physiques LMK à leurs détenteurs respectifs pour utilisation. Ces derniers procèdent alors, de manière conjointe, à l'activation du processus d'utilisation de la clé maîtresse LMK pour l'opération demandée.

Changement des clés : Une procédure de passation est exécutée en cas de changement des détenteurs des clés HSM. Cette procédure de passation prévoit notamment un changement du mot de passe associé au moment de la récupération de la carte à puce.

VI. Narratif de la procédure

PRO-RSSI-SSI-10	Procédure de gestion des clés cryptographiques	RSSI, DSI, Comité Sécurité, users, Direction générale.
-----------------	------------------------------------------------	--------------------------------------------------------

Acteurs	Descriptions des tâches	Outils et interfaces
I. Génération des clés		
Service Infrastructure Systèmes & Réseaux, Administrateur HSM, Administrateur Base de données.	<ul style="list-style-type: none"> – Génération des clés (bases de données, fichiers, HSM) selon les standards définis. – Lancement des commandes de génération LMK (LMK1, LMK2, LMK3). – Participation au double contrôle de génération LMK. 	Console HSM, Outil de gestion des configurations, Procédure interne validée
Service Exploitation & Production Administrateur Base de données.	<ul style="list-style-type: none"> – Génération de la première partie de mot de passe (conteneur sécurisé, coffre). – Participation à la génération et au stockage des LMK. 	Console HSM, coffre-fort physique ou numérique
Service Sécurité des SI	<ul style="list-style-type: none"> – Génération de la seconde partie de mot de passe (coffre, wallet, keystore). – Supervision des processus de génération selon les standards de sécurité. 	Console HSM, documentation de sécurité, engagements signés
II. Distribution et sauvegarde des clés		
Service Infrastructure Systèmes	<ul style="list-style-type: none"> – Transfert sécurisé des clés vers les environnements cibles (bases, serveurs, équipements). – Mise en œuvre de la réPLICATION sécurisée des HSM (actif/passif). – Archivage des anciennes clés dans des zones sécurisées. 	Console HSM, tunnel chiffré (SCP, SFTP), documentation de transfert, procédures de sauvegarde
Service Exploitation & Production	<ul style="list-style-type: none"> – Sauvegarde de la première partie du mot de passe ou des composants de clés dans un coffre sécurisé. – Mise à jour du référentiel d'inventaire des clés. 	Coffre-fort physique/numérique (Thycotic, CyberArk), base de données de suivi interne, manuel opératoire

Acteurs	Descriptions des tâches	Outils et interfaces
Service Sécurité des SI	<ul style="list-style-type: none"> - Sauvegarde de la seconde partie du mot de passe ou des clés décomposées. - Vérification du respect des exigences de redondance, de séparation des rôles et de conservation des logs. 	Coffre-fort numérique, registre de journalisation, procédure d'audit interne
III. Rotation, révocation et suppression des clés		
Service Infrastructure Systèmes & Réseaux, Administrateur HSM	<ul style="list-style-type: none"> - Planification et exécution de la rotation périodique des clés (bases, fichiers, HSM). - Remplacement des LMK en cas de changement de membre ou d'incident. 	Console HSM, scripts automatisés, calendrier de rotation
Service Exploitation & Production	<ul style="list-style-type: none"> - Sauvegarde des nouvelles clés et archivage sécurisé des anciennes. - Mise à jour des configurations applicatives et systèmes. 	Coffre numérique, outil de gestion de configuration, procédure de déploiement
Service Sécurité des SI	<ul style="list-style-type: none"> - Révocation des clés compromises ou obsolètes. - Suivi des incidents liés aux clés et élaboration des rapports post-événements 	SIEM, registre de gestion des incidents, rapports de contrôle

Annexes / Enregistrements

Liste des ampliations

N°	Structures	Date	Visa	Observations
01				
02				

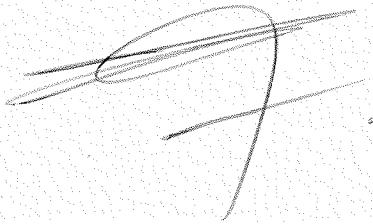
Liste des modifications

N°	Nature de la modification	Date	Chapitre ou page concerné (e)	Observations
01				
02				

Rédigé par : RESPONSABLE
DE LA SECURITE DES
SYSTEMES D'INFORMATION

Date : 06/01/2025

Signature :



Validé par : COMITE
PROCEDURES

Date : 06/01/2025

Signature :



Approuvé par : DIRECTION
GENERALE

Date :

Signature :

