BANQUE DE LA REPUBLIQUE DU BURUNDI

TERMES DE REFERENCE POUR LE RECRUTEMENT D'UN FOURNISSEUR CHARGE DE L'IMPLEMENTATION D'UNE SOLUTION DE DIGITALISATION COMPLETE DU SECTEUR FINANCIER DU BURUNDI

Bujumbura, Mai 2024

TABLE DES MATIERES

i

I. CONTEXTE ET JUSTIFCATION

La digitalisation du secteur financier du Burundi est l'un des programmes de la vision du Gouvernement pour faire le Burundi un Pays émergent en 2040 et un pays développé en 2060. En effet, la digitalisation du secteur financier permettra d'améliorer l'efficacité des services publics, de renforcer la gouvernance et d'accroître l'inclusion financière.

Dans cette vision du Gouvernement du Burundi, la Banque de la République du Burundi compte renforcer le système national de paiement par la promotion des services financiers numériques malgré que le paysage financier actuel des paiements au Burundi présente un certain nombre de défis qui freinent le développement de cette économie numérique nationale.

Les principaux défis sont, entre autres, l'absence d'une identité numérique unique pour les utilisateurs des services financiers numériques et l'absence d'une interopérabilité effective intégrant tous les acteurs de l'écosystème des paiements du Burundi.

L'absence d'infrastructure centralisée orchestrant tous les flux financiers entraîne une fragmentation du marché et, par conséquent, différents types de risques, des coûts de transaction élevés, un manque de transparence des flux financiers, ce qui limite l'utilisation des moyens de paiement électroniques et l'inclusion financière.

Pour une digitalisation complète et effective du secteur financier du Burundi, il faut lever trois défis majeurs :

- L'intégration de tous les acteurs composant le secteur financier du Burundi dans l'écosystème numérique plus particulièrement ceux qui ne disposent pas d'infrastructure des systèmes de paiement ;
- L'interopérabilité de tous les systèmes et moyens de paiement existants et à venir au Burundi ;
- L'identification unique des utilisateurs des services financiers numériques au Burundi : L'absence d'une identité numérique unique des consommateurs des services financiers numériques est un défi majeur pour les services financiers numériques.

L'objectif de ce projet de digitalisation du secteur financier est le développement d'une économie numérique réduisant l'utilisation des espèces, mais également l'accroissement de l'inclusion financière, qui est le résultat de l'interopérabilité entre tous les acteurs du secteur financier (établissement de crédit, institutions de microfinance, établissements de paiement, etc.), à laquelle doit s'ajouter la capacité de

travailler en mode connecté (online) et déconnecté (offline) vu le taux de pénétration de l'Internet au Burundi (22%, données ARCT).

II. OBJECTIFS

La digitalisation du secteur financier du Burundi aura comme objectifs :

- Le développement de **l'utilisation des moyens de paiement électronique sans recourir au cash** qui est trop coûteux pour la Banque Centrale suite aux charges liées à l'impression des billets de banque ;
- La **réduction des coûts associés** aux paiements électroniques pour les parties prenantes et les clients finaux ;
- L'accroissement **du niveau d'inclusion financière du pays**, à travers la facilitation de l'utilisation des services bancaires sans agence sur tout le territoire du Burundi ;
- **L'interopérabilité** des différents systèmes et moyens de paiements au niveau national et régional ;
- L'identification des utilisateurs (Individus, Entreprises, Sociétés, Communauté, etc.) du secteur financier avec **un identifiant unique**.
- Automatisation des systèmes de compensation et règlements entre les différents acteurs de la place.

III. ACTIVITES A REALISER

1. Fourniture des équipements et déploiement de l'infrastructure matérielle et logicielle sur les sites primaire et secondaire de la BRB ainsi que les sites des institutions financières ;
2. Installation et mise en place des centres d'enrôlement des consommateurs des produits et services financiers ;
3. Délivrance d'un Identifiant Unique aux consommateurs des produits et services financiers enrôlés ;
4. Sécuriser le stockage de l'Identifiant Unique ainsi que les autres informations personnelles des utilisateurs afin de respecter le Règlement Général sur la Protection des Données ;
5. Mise à disposition des cartes aux clients des institutions financières ne disposant pas d'infrastructure monétique ;

6. Interopérabilité des cartes bancaires (existant) des institutions financières disposant de système monétique et celles des institutions financières qui n'en dispose pas ;
7. Certification des GAB/DAB et TPE par les émetteurs internationaux VISA, Mastercard, Amex, etc.
8. Acceptation des cartes bancaires internationales sur les GAB/DAB et TPE locaux ;
9. Possibilité d'effectuer des paiements internationaux ;
10. Fourniture d'une plateforme centralisée permettant l'interopérabilité des transactions effectuées sur carte bancaire, sur TPE, par internet et par téléphone mobile. La plateforme doit permettre également le paiement instantané ainsi que le routage de toutes les transactions ainsi que leur règlement en temps réel ;
11. Développement d'une passerelle de paiement qui facilitera le développement du commerce en ligne (e-commerce) au Burundi ;
12. Création d'un QR Code Unique et sécurisé qui rendra les paiements de proximité très flexibles dans les hôtels, les supermarchés, commerces de proximité, les restaurants, etc.
13. Mise en place d'un code unique USSD interfaçant et rendant interopérables tous les codes USSD déjà en usage au pays pour accroître considérablement l'inclusion financière dans les zones rurales les plus reculées ;
14. Permission des paiements transfrontaliers en intégrant un module de conversion instantanée de devises utilisées dans les différents pays conformément au taux du jour ;
15. Possibilité d'effectuer des paiements de détail et leur règlement avant de déverser les soldes nets dans le système RTGS de la Banque Centrale ;
16. Formation des formateurs pour le personnel de la BRB sur la solution de digitalisation mise en place à la BRB ;
17. Interfaçage du module de gestion des identifiants uniques avec les différents systèmes d'information (Core Banking) des institutions financières pour lier chaque identifiant unique aux différents comptes des clients ;
18. Formation sur le module d'enregistrement et d'émission des cartes aux agents chargés de l'enrôlement des consommateurs des produits et services financiers ;
19. Formation des formateurs du personnel des parties prenantes au projet de digitalisation du secteur financier sur la solution mise en place ;
20. Mettre en place un système de reporting destiné à la banque centrale ainsi qu'aux acteurs de l'écosystème ;

21. Le module doit permettre l'interfaçage avec les systèmes de GED (Gestion Electronique des Documents) disponibles ou qui seront disponibles durent la période de mise en place du projet.
22. Le fournisseur doit fournir un système Open Banking qui permettra à la banque de gérer ses livrets comptables.
23. Mettre à disposition un système d'Alias afin d'assurer une identité bancaire unique au niveau de la Banque Centrale du BURUNDI.

IV. DESCRIPTION DU SYSTEME CIBLE

Le système cible est la mise en place d'une plateforme centralisée permettant une interopérabilité de toutes les transactions effectuées dans l'écosystème des systèmes de paiement que ça soit sur carte bancaire, sur internet, sur téléphone mobile en vue d'une digitalisation complète et effective du secteur financier de la République du Burundi. Cette plateforme centrale sera composée par des modules distincts assurant les services ci-dessous :

1. Module d'identification unique de la population ;
2. Module d'interopérabilité :
    - Par des cartes bancaires ;
    - Via Téléphone Mobile ;
    - Via Internet.
3. Module d'inclusion financière.
4. Module de gestion des Litiges pour les opérations :
    - Par des cartes bancaires ;
    - Via Téléphone Mobile ;
    - Via Internet.
5. Module de compensation et règlement.

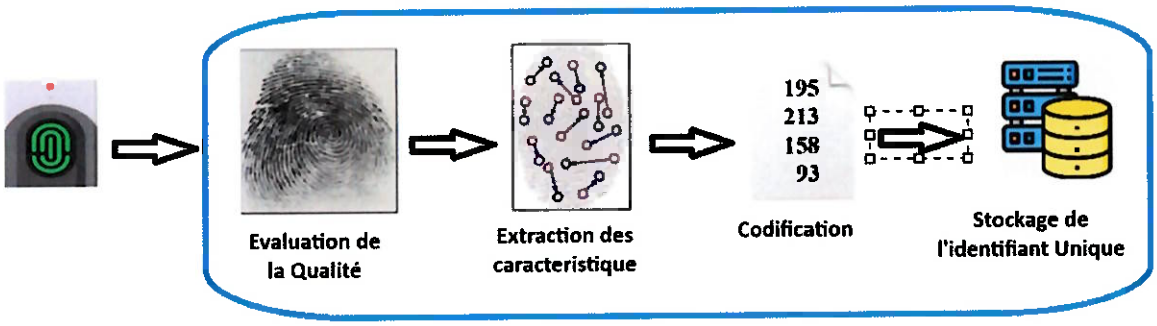
IV.1. Module d'Identification

La plateforme centralisée d'interopérabilité devra avoir un module d'enrôlement de tous les consommateurs des services financiers numériques afin de les identifier d'une manière unique. Ce module doit permettre à chaque consommateur ou clients des services financiers numériques d'avoir une identité numérique basée sur des paramètres **biométriques** qu'il utilisera pour toutes ses transactions électroniques. Chaque compte (bancaire, mobile, etc.) devra être lié à une seule identité numérique et

une identité numérique peut être lié à un ou plusieurs comptes.

Les Spécifications techniques et fonctionnelles de ce module d'identification sont les suivantes :

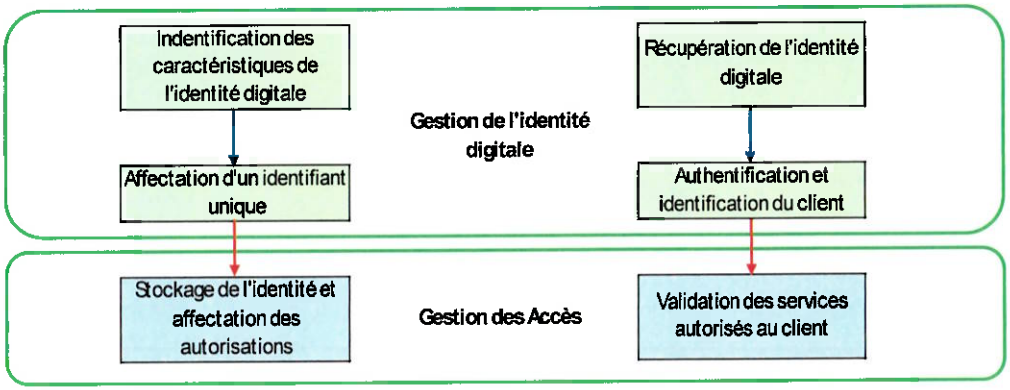
1. Le module d'identification doit fournir une identité numérique unique basée sur les paramètres biométriques ;



2. Le module d'identification doit prévenir le vol de l'identité ;
3. Le module d'identification doit être interfacé avec le module lutte contre le blanchiment des capitaux et le financement du terrorisme (AML et CFT) ;
4. Le module doit prendre en charge le système de versionnage des données KYC modifiés ;
5. Le module d'identification doit avoir la possibilité de charger ou télécharger les données des autres parties prenantes ;
6. Le module doit avoir une architecture multi-tiers (au moins 3 niveaux) ou micro-services ;
7. Chaque identifiant KYC créé doit avoir un code QR sécurisé associé ;
8. Le module doit avoir une possibilité de pouvoir croître pour traiter des volumes beaucoup plus importants (Scalabilité) ;
9. Le module ne doit pas dépendre d'une plateforme spécifique (Microsoft, Unix, Mac, Android, iOS, etc.). il devrait être indépendante de toute plateforme ;
10. Le module ne doit pas dépendre d'une base de données spécifique.
11. Le module doit disposer d'une capacité à assurer un service sans interruption, quelles que soient les conditions de fonctionnement des systèmes (migrations, panne de systèmes, changement de version, upgrade système, etc.…) : Haute disponibilité ;
12. Le module doit avoir une architecture d'équilibrage de charge (Load Balancing) ;
13. Le module doit avoir une architecture de réplication entière en temps réel du site primaire au site de secours ;

14. Le module doit être compatible avec plusieurs navigateurs pour prendre en charge de manière identique différents navigateurs Web ;
15. La solution doit être en conformité avec les directives de sécurité fournies par les Frameworks internationaux tels que NIST, ISO 27001, etc.
16. La solution doit être facilement paramétrable et personnalisable ;
17. Le module doit disposer d'une interface backoffice pour la gestion et la consultation.
18. La solution doit permettre la gestion des accès par profil (Super admin, Admin, Initiateur, Validateur) ;
19. La solution doit permettre la personnalisation et le paramétrage facile des différents profils créés (Super admin, Admin, Initiateur, Validateur) ;
20. La solution doit permettre la validation du numéro de téléphone par OTP (envoyé via SMS ou Email) ;
21. Le module doit permettre la gestion de l'utilisateur (créer, modifier, approuver, afficher, bloquer, débloquer, supprimer) ;
22. Le module doit avoir une interface ergonomique multilingue (Kirundi, Français et Anglais) ;
23. La solution doit avoir une fonction de capture et le traitement d'image du client ;
24. La solution doit avoir une fonction de vérification de la photo du client ;
25. Le module doit avoir une fonction de vérification de documents et détection de fraude sur les documents ;
26. Le module doit avoir de mécanisme de vérification KYC basé sur vidéo ;
27. Le module doit avoir de mécanismes de vérification des formulaires à l'aide des techniques OCR/ICR ;
28. Le module doit avoir de mécanismes de vérification du client à l'aide des empreintes digitales ;
29. Le fournisseur doit fournir le matériel nécessaire pour la récupération et identification des information client (empreintes, OCR, ...) ;
30. Le matériel fourni doit respecter les normes de sécurité internationales ;
31. Le fournisseur doit fournir le support nécessaire pour la maintenance du matériel fourni.
32. Le module doit avoir la possibilité de traiter des opérations groupées (créer, afficher, approuver, rejeter, annuler, supprimer) ;
33. Le module doit permettre la génération des dynamiques des rapports avec la fonctionnalité Business Intelligence ;

34. La solution doit être totalement APIsé, la documentation de l'API doit être détaillé est disponible (en français et anglais).
35. L'architecture technique détaillé de la solution doit être disponible ; l'installation de la solution doit impérativement être possible sur des environnements virtualisés.
36. Le module doit permettre l'enregistrement des logs d'audit relatifs à toute opération impactant le système.
37. Le fournisseur doit disposer d'un support 24/24 7/7 avec un système de ticketing électronique.
38. Le processus et les SLA de traitement des incidents doivent être décrits et détaillés.
39. La solution doit disposer de deux modules :



- Un module de gestion de l'identité digitale :

Le module permet la lecture, l'extraction et la création d'une identification digitale unique et sécurisée.
Le module permet l'identification d'un client à partir de son id unique.
Le module doit mettre à disposition à des systèmes tierces, la possibilité de vérifier l'identité unique et la récupération des informations du client, cette vérification doit être en temps réel.

- Un module de gestion des autorisations :

A sa création, chaque identifiant doit avoir un ensemble d'autorisation lui permettant d'accéder aux services des institutions de la place.
Le service d'autorisation doit être ineffaçable avec des systèmes tierces afin de à jour les autorisations affectées au client (interfaçages avec Système AML ou autres)

IV.2. Module d'interopérabilité

IV.2.1. Par cartes au niveau national et international

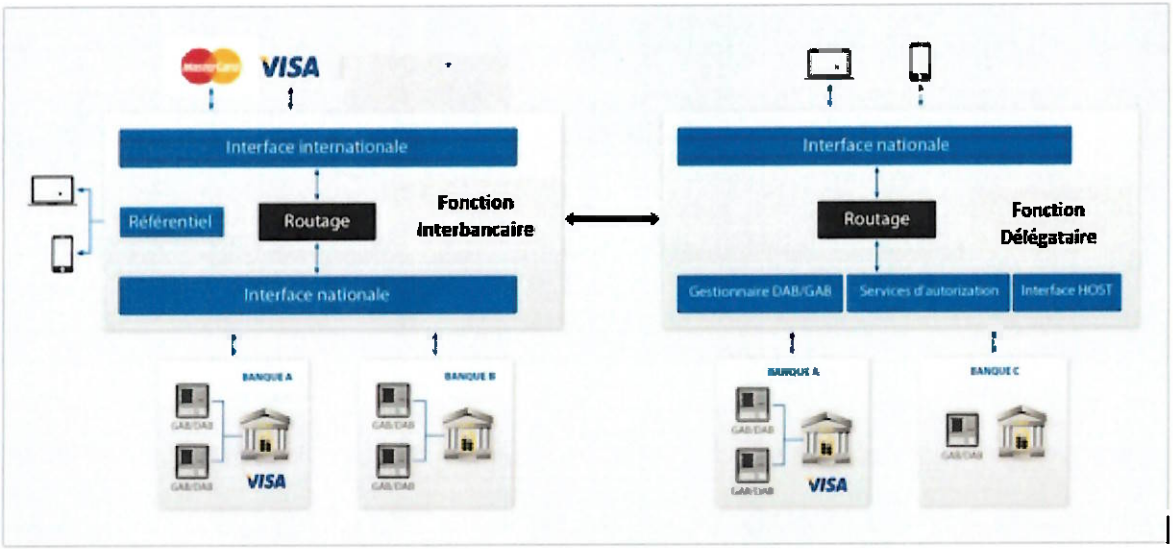
Ce module devra assurer les services monétiques interbancaires pour toutes les transactions nationales et internationales effectuées sur carte locale (ex : SESAME, etc.) ou carte EMV (exemple : Carte VISA) que ça soit au niveau des GAB, de l'Internet et des TPE. Ce module doit avoir une double fonction permettant d'assurer une fonction interbancaire et une fonction délégataire.

- Une fonction Interbancaire pour les services interbancaires sur carte entre les systèmes monétiques déjà existant (Carte bancaire, DAB/GAB et TPE existants) ;
- Une fonction délégataire qui fournit les services monétiques aux institutions financières ne disposant pas de systèmes monétiques. Cette fonction sera très bénéfique pour le secteur financier car elle intègrera tous les acteurs du système financier ne disposant pas d'infrastructure de paiement dans l'écosystème des paiements numériques.

En plus de ces deux fonctions, le module sera équipé de deux interfaces :

- Une interface nationale pour traiter toutes les transactions nationales ;
- Des interfaces internationales pour router les transactions internationales vers les émetteurs internationaux. Pour effectuer ces opérations internationales, le module devra être certifié par les émetteurs internationaux comme VISA, MasterCard, etc.

Le schéma ci-dessous montre l'architecture générale de ce module d'interopérabilité sur carte :



Les Spécifications techniques et fonctionnelles de ce module d'interopérabilité sur carte sont les suivantes :

1. Le module doit permettre l'interopérabilité des cartes tenant compte de tous les schémas existants et à venir au Burundi ;
2. L'interopérabilité locale des cartes locales sans faire recours au réseau VISA ou MasterCard ;
3. Le module doit prendre en charge toutes les cartes existantes et à venir ;
4. Le module doit supporter le protocole standard ISO 20022/8583.
5. Le module doit supporter la norme EMV.
6. Le module doit prendre en charge tous les DAB/GAB/TPE existants et à venir ;
7. Le module doit émettre des cartes pour les institutions financières qui ne disposent pas de système monétique ou celles désirant déléguer ce service ;
8. Les cartes émises pour les institutions financières ne disposant pas de service monétique doivent être opérationnelles sur les GAB/DAP/TPE existants et à venir ;
9. Le module d'interopérabilité sur carte doit permettre d'effectuer des paiements transfrontaliers avec conversion automatique de monnaies nationales ;
10. Le module d'interopérabilité sur carte doit être certifiée par les émetteurs internationaux pour effectuer des paiements internationaux ;
11. Retrait et dépôt sur n'importe GAB/TPE en utilisant n'importe quelle carte bancaire ;
12. Possibilité de transfert des fonds de la carte bancaire vers le portefeuille mobile et vice versa en utilisant la carte ;
13. Possibilité de transfert des fonds de la carte bancaire vers le compte bancaire et vice versa en utilisant la carte bancaire ;
14. Possibilité d'utiliser n'importe quelle carte bancaire sur n'importe quelle TPE/GAB/DAB en mode offline ;
15. Possibilité d'utiliser n'importe quelle carte bancaire pour payer les biens services sur les plateformes en ligne ;
16. Possibilité de faire des paiements P2P, P2G, et P2B en utilisant la carte bancaire ;
17. Possibilité de faire des paiements B2P, B2G, et B2B en utilisant la carte bancaire ;
18. Possibilité de faire des paiements G2P, G2G, et G2B en utilisant la carte bancaire ;
19. Intégration du module d'interopérabilité des cartes avec le système RTGS pour le règlement des soldes nettes résultant de la compensation des transactions sur carte ;
20. La mise en place d'un schéma local de carte ;
21. Le module doit permettre le paiement et règlement instantané via une carte bancaire.

22. La solution doit être totalement APIsé, la documentation de l'API doit être détaillé est disponible (en français et anglais).
23. L'architecture technique détaillé de la solution doit être disponible ; l'installation de la solution doit impérativement être possible sur des environnements virtualisés.
24. Le module doit disposer d'un système anti-fraude électronique.
25. Le module doit inclure un module de compensation entre les différents acteurs de la place ainsi que le règlement via les canaux de règlement en place.
26. Le fournisseur doit disposer d'un support 24/24 7/7 avec un système de ticketing électronique.
27. Le processus et les SLA de traitement des incidents doivent être décrits et détaillés.

IV.2.2. Par téléphonie mobile

Le module de paiement par téléphone mobile devra permettre aux clients ou consommateurs des services financiers numériques d'offrir des services de paiement à leurs clients en utilisant le téléphone portable en liaison avec ou non avec les comptes bancaires ainsi que les cartes bancaires.

1. Les Spécifications techniques et fonctionnelles de ce module sont les suivantes : Interopérabilité entre tous les portefeuilles mobiles existants et à venir ;
2. Interopérabilité de toutes les applications mobiles Banking développées dans les institutions financières ;
3. Acceptation d'un Unique USSD interfaçant toutes les applications mobiles ;
4. Mise en place d'un Unique QR Code pour les paiements de proximité ;
5. Transfert de fonds d'un portefeuille mobile vers un compte bancaire et vice versa (Bank to Wallet et Wallet to Bank) ;
6. Transfert de fonds d'un portefeuille mobile vers une carte bancaire et vice versa ;
7. Retrait et dépôt de fonds sur GAB/DAB via une application mobile, USSD et SMS ;
8. Retrait et dépôt de fonds sur TPE via une application mobile, USSD et SMS ;
9. Effectuer les paiements P2P, P2B, P2G via une application mobile, USSD et SMS ;
10. Effectuer les paiements B2P, B2B, B2G via une application mobile, USSD et SMS ;
11. Effectuer les paiements G2P, G2B, G2G via une application mobile, USSD et SMS ;
12. Effectuer les paiements via QR code ;
13. Possibilité d'effectuer des transactions régionales et internationales via des canaux mobiles ;
14. Intégration du module d'interopérabilité des cartes avec le système RTGS pour le règlement des soldes nettes résultant de la compensation des transactions sur téléphone mobile ;

15. Le module doit permettre le paiement et règlement instantané via des canaux mobiles.
16. La solution doit être totalement APIsé, la documentation de l'API doit être détaillé est disponible (en français et anglais).
17. L'architecture technique détaillé de la solution doit être disponible ; l'installation de la solution doit impérativement être possible sur des environnements virtualisés.
18. Le module doit disposer d'un système anti-fraude électronique.
19. Le module doit inclure un module de compensation entre les différents acteurs de la place ainsi que le règlement via les canaux de règlement en place.
20. Le fournisseur doit disposer d'un support 24/24 7/7 avec un système de ticketing électronique.
21. Le processus et les SLA de traitement des incidents doivent être décrits et détaillés.

IV.2.3. Par internet

Le module d'interopérabilité des paiements par Internet doit offrir aux utilisateurs une solution de paiement en ligne hautement sécurisé dotée des spécifications techniques et fonctionnelles suivantes :

1. Le module doit permettre à l'utilisateur d'accéder en ligne en une seule interface à tous ses comptes bancaires, tous ses portefeuilles et toutes ses cartes bancaires ;
2. Le module doit permettre à l'utilisateur d'effectuer en ligne les opérations de virements compte-à-compte, compte-à-portefeuille, portefeuille-à-portefeuille, compte-à-carte, portefeuille-à-carte, portefeuille-à-compte, carte-à-carte, carte-à- portefeuille, carte-à-compte ;
3. La mise en place d'une passerelle unique de paiement en ligne englobant tous les moyens de paiement disponibles au Burundi ;
4. Le module doit permettre d'effectuer des paiements en ligne de biens et services en utilisant un moyen de paiement de son choix (carte bancaire, compte bancaire, portefeuille) ;
5. L'intégration du module de paiement en ligne avec le module de lutte contre le blanchiment des capitaux et le financement du terrorisme (AML et CFT) ;
6. La possibilité d'effectuer des paiements P2P, P2G et P2B en ligne ;
7. La possibilité d'effectuer des paiements B2P, B2G et B2B en ligne ;
8. La possibilité d'effectuer des paiements G2P, G2G et G2B en ligne ;
9. Le module doit permettre l'interopérabilité de toutes les plateformes Web-Banking existantes et à venir ;
10. Le module doit permettre le paiement et règlement instantané en ligne.

11. L'intégration du module d'interopérabilité Internet avec le système RTGS pour le règlement des soldes nettes résultant de la compensation des transactions en ligne.
12. La solution doit être totalement APIsé, la documentation de l'API doit être détaillé est disponible (en français et anglais).
13. L'architecture technique détaillé de la solution doit être disponible ; l'installation de la solution doit impérativement être possible sur des environnements virtualisés.
14. Le module doit disposer d'un système anti-fraude électronique.
15. Le module doit inclure un module de compensation entre les différents acteurs de la place ainsi que le règlement via les canaux de règlement en place.
16. Le fournisseur doit disposer d'un support 24/24 7/7 avec un système de ticketing électronique.
17. Le processus et les SLA de traitement des incidents doivent être décrits et détaillés.

IV.2.4. Module de gestion backoffice, règlement et de prévention contre la fraude

1. Le module doit permettre en réconciliation en temps réel, quasi-temps réel et back-office entre les différents acteurs de la place.
2. Le module doit mettre à disposition une 360° de la clientèle de la banque.
3. Le module doit permettre la gestion des Alias comme moyen d'identification unique auprès de la BRB.
4. La réconciliation doit être disponible pour les différents types de transaction disponible :
    a. Par Carte.
    b. Par Mobile.
    c. Par Internet.
5. Le module doit être interfaçable avec les systèmes de règlements de la place.
6. Le module doit générer les états nécessaires pour permettre aux acteurs de la place de suivre leurs activités d'interopérabilité.
7. Le module doit mettre à disposition une interface pour la gestion des litiges pour les activités par carte, par mobile et par internet.
8. La solution doit mettre à disposition un module de gestion de la fraude par carte, par mobile et par internet.

IV.3. Plateforme de paiement délégataire

1. La plateforme doit permettre les échanges de flux transactionnels en temps réel, quasi-temps réel et back-office. La solution doit être modulaire et basée sur les technologies de développement

standards en vigueur.

2. La solution doit permettre la connexion avec la plateforme d'interopérabilité décrite dans le paragraphe ci-dessus.
3. La solution devra disposer d'une partie front office et d'une partie back office.
4. Le front office regroupera tous les services onlines afin de permettre aux clients d'échanger des flux en temps réel.
5. La partie backoffice doit permettre l'échange de fichiers et couvrir l'ensemble du cycle de la transaction (présentation, impayé, représentation, etc.)
6. La solution devra offrir des web services IN et OUT (quasi temps réel) financiers pour la prise en charge des flux de ces acteurs ;
7. Les spécifications techniques et fonctionnelles de la solution doivent être fournies en français et anglais ;
8. Trois (03) références similaires au contexte de cette consultation doivent être proposées ;
9. La solution devra être multi-institutions et de préférence multi-langues (Français, Anglais, ...)
10. La solution doit supporter toutes type de cartes (VISA, MasterCard, Local, CPA, Débit, Crédit et prépayé) ;
11. La solution doit supporter le standard de carte EMV.
12. La solution doit supporter le protocole ISO 20022/8583
13. Le fournisseur doit fournir les éléments nécessaires afin de permettre un transfert de connaissances garantissant une montée en compétences des équipes (documentation, formation et suivi lors de la mise en service, ...) ;
14. La fourniture d'un support efficient après la mise en production de la plateforme (période de garantie et de maintenance de la solution et des spécifications) ;
15. La formalisation des SLA sur la disponibilité des équipes support et la qualité de fonctionnement de la plateforme.
16. La solution doit certifier PCI-DSS afin de respecter les standards de sécurité monétique internationaux ;
17. La solution doit être certifiée VISA / Mastercard / UPI et autres réseaux internationaux, régionaux et nationaux ;
18. La solution doit être totalement APIsé, la documentation de l'API doit être détaillé est disponible (en français et anglais).

19. L'architecture technique détaillé de la solution doit être disponible ; l'installation de la solution doit impérativement être possible sur des environnements virtualisés.
20. Le fournisseur doit disposer d'un support 24/24 7/7 avec un système de ticketing électronique.
21. Le processus et les SLA de traitement des incidents doivent être décrits et détaillés.

IV.6. L'Inclusion Financière

Pour que l'inclusion financière soit améliorée, la solution recherchée doit permettre de :

- Travailler en mode connecté (online) et surtout en mode déconnecté (offline) vu le taux de pénétration de l'Internet au Burundi (22%, données ARCT) ;
- Assurer l'interopérabilité totale de tous les systèmes et moyens de paiements composant le secteur financier au Burundi ;
- Utiliser un code unique USSD pour les services financiers numériques ;
- Utiliser de simples SMS pour effectuer des transactions ;

NB : En plus des services mentionnés dans ce document, le soumissionnaire est invité à proposer d'autres services qui seraient actuellement disponibles au niveau de sa solution tout en étant éprouvés sur le marché

V. RESULTATS ATTENDUS

A la clôture du projet, la BRB devra jouir d'une plateforme centralisée clé en main complète, conviviale, modulaire et évolutive basée sur l'architecture trois tiers et « Service Oriented architecture, SOA ». Cette plateforme servira à atteindre l'objectif d'une digitalisation complète et effective du secteur financier comme développé dans les points ci-haut.

VI. METHODOLOGIE

La méthodologie devra s'appuyer en grande partie sur les bonnes pratiques internationales ou régionales en la matière et l'expérience du soumissionnaire dans des missions similaires. Pour mener à bien cette mission, le soumissionnaire doit fournir sa méthodologie complète qu'il compte utiliser ressortissant la compréhension de la mission, son plan de travail qui identifie en détail les méthodes et procédures à utiliser pour la réussite de la mission ainsi que le calendrier détaillé de réalisation chaque activité.

VII. PROFIL DU SOUMISSIONNAIRE

Le soumissionnaire doit être une firme ou un cabinet. Les groupements, les consultants individuels ne sont pas acceptés et sont exclus d'office de la compétition.

La Firme ou le cabinet doit avoir au moins sept (7) ans d'expérience dans le domaine et avoir réalisé des travaux similaires dans au moins trois (3) pays différents dans le domaine de digitalisation du secteur financier accompagnés d'attestations de bonne fin d'exécution démontrant la capacité du soumissionnaire à maîtriser l'ensemble des diverses technologies et services nécessaires pour la mise en œuvre du Projet.

Le personnel aligné devra justifier au moins de deux missions exécutées similaires à ce projet et doit parler couramment le Français.

VIII. PLANNING DES ACTIVITES

Le soumissionnaire devra spécifier dans son offre le planning détaillé des activités qu'il compte réaliser depuis l'initiation jusqu'à la clôture du projet.

IX. LIVRABLES ATTENDUS

Le soumissionnaire produira les livrables en langue française ci-après :

1. Un document des spécifications fonctionnelles et techniques détaillées de chaque module de sa solution ;
2. La structure de base de données de sa solution ;
3. Un plan d'installation du système, un plan de recette et d'intégration de chaque module de sa solution et un plan de migration des données ;
4. Un plan de formation avec précision des charges liées à la formation et à l'accompagnement des utilisateurs et des opérateurs ;
5. Un document précisant les informations qu'il compte transmettre aux exploitants techniques et opérationnels du système afin qu'ils assurent leurs activités en toute indépendance vis à vis du fournisseur ;
6. Un document précisant les modalités de transfert de compétences (formation dédiée, sur le tas au fil du projet…), le niveau de connaissance technique requis pour pouvoir acquérir lesdites compétences et le pré requis des administrateurs système ;
7. La liste des documents qu'il fournira dans le cadre du projet, en guise de documentation ;

8. Un plan de déploiement et de mise en service opérationnel de chaque module de sa solution.

NB : En guise d'assistance au démarrage, le soumissionnaire s'engage à déléguer le personnel technique adéquat, pour une période de trois mois, pour préparer le système au fonctionnement opérationnel, assister les équipes techniques et opérationnels chargé de la gestion de la plateforme centralisée située à la BRB et une assistance similaire aux participants chargés de la gestion de la plateforme participant.

X. CONTENU DES OFFRES

Les soumissionnaires intéressés devront produire les informations sur leurs capacités, qualifications et expériences démontrant qu'ils sont qualifiés pour la mission, en soumettant un dossier de manifestation d'intérêt comprenant une offre technique et une offre financière.

- **L'offre technique devra contenir les documents suivants :**

1. Une lettre de soumission signée par une personne ayant les pouvoirs d'engager la société soumissionnaire, accompagnée d'une procuration écrite authentifiée par le notaire en cas de délégation ;
2. L'adresse précise et exacte du soumissionnaire (adresse, numéro de téléphone, email, etc.) ;
3. Une preuve de l'existence légale de la société ;
4. Statuts notariés ;
5. Certificat d'immatriculation au registre de commerce ;
6. Attestation de non-redevabilité encore valide délivrée par une autorité fiscale ;
7. Comptes audités des 3 derniers exercices (2021, 2022, 2023) ;
8. Trois (3) références des marchés similaires exécutés avec preuve à l'appui pour chaque référence (attestation de bonne fin d'exécution) (l'absence de preuve engendre la note zéro) ;
9. CVs du personnel aligné pour le Projet signé à la fois par le personnel lui-même et par le représentant de la société soumissionnaire avec des diplômes/certificats valides attestant la qualification requise (académique et professionnelle).
10. Plan et Méthodologies de mise en œuvre du Projet d'une manière claire, concise et pertinente par rapport à la portée de l'appel d'offres (y compris les plans de travail, le calendrier, activités avec des critères de clôture clairs, des livrables du Projet, des tests d'acceptation, etc.).
11. Confirmation de la disponibilité du personnel aligné sur le Projet pour la durée complète du Projet, et le rôle de chaque personnel avec notes explicatives.
12. Une proposition détaillée de support et de maintenance clairement expliquée et soumise comme

une partie de la proposition technique dégageant toutes les exclusions le cas échéant.

13. Support 24/24, 7/7 doit être disponible preuve à l'appui.
14. Une proposition détaillée de formation et de transfert de connaissance clairement expliquée et soumise dans le cadre de la proposition technique dégageant toutes les exclusions le cas échéant.
15. Une garantie de soumission par message SWIFT d'avis de débit au profit du compte de la BRB de 150 000 USD pour les soumissionnaires étrangers, ou son équivalent en BIF pour les soumissionnaires locaux.
16. Tous les documents fournis par le soumissionnaire, à l'exception de la documentation imprimée non modifiable, doivent être paraphés, signés (et cachetés) par la personne autorisée.
17. Une proposition de visite sur Site pour des clients ayant une solution similaire à celle demandée par la BRB.

➢ **L'offre technique devra contenir les documents suivants** :

1. La lettre de soumission financière ;
2. Les bordereaux des prix pour chaque module, comprenant tous les droits et taxes payables au Burundi.

NB : L'absence ou la non-validité de l'un des documents énumérés ci-dessus constitue une cause de rejet d'office de l'offre.

XI. CRITERES D'EVALUATION DES OFFRES RETENUES A L'OUVERTURE

CRITERES D'EVALUATION DES OFFRES RETENUS			
I. OFFRE TECHNIQUE			
		Note obtenue	**Max**
I.1. Critères administratifs			**8**
1	Une lettre de soumission signée par une personne ayant les pouvoirs d'engager la société soumissionnaire, accompagnée d'une procuration écrite authentifiée par le notaire en cas de délégation.		0.5
2	L'adresse précise et exacte du soumissionnaire (adresse, numéro de téléphone, email, etc.).		0.5
3	Une preuve de l'existence légale de la société.		0.5
4	Statut notarié.		0.5

5	Certificat d'immatriculation au registre de commerce.		0.5
6	Attestation de non redevabilité encore valide délivrée par une autorité fiscale.		0.5
7	Trois (3) références des marchés similaires exécutés avec preuve à l'appui pour chaque référence (l'absence de preuve engendre la note zéro).		3
8	Une garantie de soumission par message SWIFT d'avis de débit au profit du compte de la BRB de 150 000 USD pour les soumissionnaires étrangers, ou son équivalent en BIF pour les soumissionnaires locaux		2
			Max
I.2. Module d'Identification (KYC)			**66**
1	Le module d'identification doit fournir une identité numérique unique basée sur les paramètres biométriques		4
2	Le module d'identification doit prévenir le vol de l'identité ;		2
3	Le module d'identification doit être interfacé avec le module lutte contre le blanchiment des capitaux et le financement du terrorisme (AML et CFT) ;		2
4	Le module doit prendre en charge le système de versionnage des données KYC modifiés ;		2
5	Le module d'identification doit avoir la possibilité de charger ou télécharger les données des autres parties prenantes ;		2
6	Le module doit avoir une architecture multi-tiers (au moins 3 niveaux) ou micro-services ;		2
7	Chaque identifiant KYC créé doit avoir un code QR sécurisé associé ;		1
8	Le module doit avoir une possibilité de pouvoir croître pour traiter des volumes beaucoup plus importants (Scalabilité) ;		2
9	Le module ne doit pas dépendre d'une plateforme spécifique (Microsoft, Unix, Mac, Android, iOS, etc.). il devrait être indépendante de toute plateforme ;		1
10	Le module ne doit pas dépendre d'une base de données spécifique.		1
11	Le module doit disposer d'une capacité à assurer un service sans interruption, quelles que soient les conditions de fonctionnement des systèmes (migrations, panne de systèmes, changement de version, upgrade système, etc....) : Haute disponibilité ;		2
12	Le module doit avoir une architecture d'équilibrage de charge (Load Balancing) ;		1
13	Le module doit avoir une architecture de réplication entière en temps réel du site primaire au site de secours ;		1
14	Le module doit être compatible avec plusieurs navigateurs pour prendre en charge de manière identique différents navigateurs Web ;		1
15	La solution doit être en conformité avec les directives de sécurité fournies par les Frameworks internationaux tels que NIST, ISO 27001, etc.		1
16	La solution doit être facilement paramétrable et personnalisable ;		2
17	Le module doit disposer d'une interface backoffice pour la gestion et la consultation.		2

18	La solution doit permettre la gestion des accès par profil (Super admin, Admin, Initiateur, Validateur) ;		2
19	La solution doit permettre la personnalisation et le paramétrage facile des différents profils créés (Super admin, Admin, Initiateur, Validateur) ;		2
20	La solution doit permettre la validation du numéro de téléphone par OTP (envoyé via SMS ou Email) ;		1
21	Le module doit permettre la gestion de l'utilisateur (créer, modifier, approuver, afficher, bloquer, débloquer, supprimer) ;		1
22	Le module doit avoir une interface ergonomique multilingue (Kirundi, Français et Anglais) ;		2
23	La solution doit avoir une fonction de capture et le traitement d'image du client ;		1
24	La solution doit avoir une fonction de vérification de la photo du client ;		1
25	Le module doit avoir une fonction de vérification de documents et détection de fraude sur les documents ;		2
26	Le module doit avoir de mécanisme de vérification KYC basé sur vidéo ;		2
27	Le module doit avoir de mécanismes de vérification des formulaires à l'aide des techniques OCR/ICR ;		1
28	Le module doit avoir de mécanismes de vérification du client à l'aide des empreintes digitales ;		2
29	Le fournisseur doit fournir le matériel nécessaire pour la récupération et identification des information client (empreintes, OCR , ...) ;		2
30	Le matériel fourni doit respecter les normes de sécurité internationales ;		2
31	Le fournisseur doit fournir le support nécessaire pour la maintenance du matériel fourni.		2
32	Le module doit avoir la possibilité de traiter des opérations groupées (créer, afficher, approuver, rejeter, annuler, supprimer) ;		1
33	Le module doit permettre la génération des dynamiques des rapports avec la fonctionnalité Business Intelligence ;		2
34	La solution doit être totalement APIsé, la documentation de l'API doit être détaillé est disponible (en français et anglais).		2
35	L'architecture technique détaillé de la solution doit être disponible ; l'installation de la solution doit impérativement être possible sur des environnements virtualisés.		2
36	Le module doit permettre l'enregistrement des logs d'audit relatifs à toute opération impactant le système.		2
37	Le fournisseur doit disposer d'un support 24/24 7/7 avec un système de ticketing électronique.		2
38	Le processus et les SLA de traitement des incidents doivent être décrits et détaillés.		2
39	La solution doit disposer de deux modules; un module de gestion de l'identité digitale d'affection de profile et gestion des autorisations relatives au profile.		1
			Max

I.3. Module d'interopérabilité par carte			**40**
1	Le module doit permettre l'interopérabilité des cartes tenant compte de tous les schémas existants et à venir au Burundi ;		2
2	L'interopérabilité locale des cartes locales sans faire recours au réseau VISA ou MasterCard ;		2
3	Le module doit prendre en charge toutes les cartes existantes et à venir ;		1
4	Le module doit supporter le protocole standard ISO 8583.		2
5	Le module doit supporter la norme EMV.		2
6	Le module doit prendre en charge tous les DAB/GAB/TPE existants et à venir ;		2
7	Le module d'interopérabilité sur carte doit permettre d'effectuer des paiements transfrontaliers avec conversion automatique de monnaies nationales ;		1
8	Le module d'interopérabilité sur carte doit être certifiée par les émetteurs internationaux pour effectuer des paiements internationaux ;		1
9	Retrait et dépôt sur n'importe GAB/TPE en utilisant n'importe quelle carte bancaire ;		2
10	Possibilité de transfert des fonds de la carte bancaire vers le portefeuille mobile et vice versa en utilisant la carte ;		1
11	Possibilité de transfert des fonds de la carte bancaire vers le compte bancaire et vice versa en utilisant la carte bancaire ;		1
12	Possibilité d'utiliser n'importe quelle carte bancaire sur n'importe quelle TPE/GAB/DAB en mode offline ;		1
13	Possibilité d'utiliser n'importe quelle carte bancaire pour payer les biens services sur les plateformes en ligne ;		1
14	Possibilité de faire des paiements P2P, P2G, et P2B en utilisant la carte bancaire ;		1
15	Possibilité de faire des paiements B2P, B2G, et B2B en utilisant la carte bancaire ;		1
16	Possibilité de faire des paiements G2P, G2G, et G2B en utilisant la carte bancaire ;		1
17	Intégration du module d'interopérabilité des cartes avec le système RTGS pour le règlement des soldes nettes résultant de la compensation des transactions sur carte ;		2
18	La mise en place d'un schéma local de carte ;		2
19	Le module doit permettre le paiement et règlement instantané via une carte bancaire.		2
20	La solution doit être totalement APIsé, la documentation de l'API doit être détaillé est disponible (en français et anglais).		2
21	L'architecture technique détaillé de la solution doit être disponible ; l'installation de la solution doit impérativement être possible sur des environnements virtualisés.		2
22	Le module doit disposer d'un système anti-fraude électronique.		2

23	Le module doit inclure un module de compensation entre les différents acteurs de la place ainsi que le règlement via les canaux de règlement en place.		2
24	Le fournisseur doit disposer d'un support 24/24 7/7 avec un système de ticketing électronique.		2
25	Le processus et les SLA de traitement des incidents doivent être décrits et détaillés.		2
			Max
I.4. Module d'interopérabilité par téléphone Mobile			**40**
1	Interopérabilité entre tous les portefeuilles mobiles existants et à venir ;		2
2	Interopérabilité de toutes les applications mobiles Banking développées dans les institutions financières ;		2
3	Acceptation d'un Unique USSD interfaçant toutes les applications mobiles ;		2
4	Mise en place d'un Unique QR Code pour les paiements de proximité ;		2
5	Transfert de fonds d'un portefeuille mobile vers un compte bancaire et vice versa (Bank to Wallet et Wallet to Bank) ;		2
6	Transfert de fonds d'un portefeuille mobile vers une carte bancaire et vice versa ;		2
7	Retrait et dépôt de fonds sur GAB/DAB via une application mobile, USSD et SMS ;		1
8	Retrait et dépôt de fonds sur TPE via une application mobile, USSD et SMS ;		1
9	Effectuer les paiements P2P, P2B, P2G via une application mobile, USSD et SMS ;		1
10	Effectuer les paiements B2P, B2B, B2G via une application mobile, USSD et SMS ;		1
11	Effectuer les paiements G2P, G2B, G2G via une application mobile, USSD et SMS ;		1
12	Effectuer les paiements via QR code ;		2
13	Possibilité d'effectuer des transactions régionales et internationales via des canaux mobiles ;		2
14	Intégration du module d'interopérabilité des cartes avec le système RTGS pour le règlement des soldes nettes résultant de la compensation des transactions sur téléphone mobile ;		2
15	Le module doit permettre le paiement et règlement instantané via des canaux mobiles.		2
16	La solution doit être totalement APIsé, la documentation de l'API doit être détaillé est disponible (en français et anglais).		2
17	L'architecture technique détaillé de la solution doit être disponible ; l'installation de la solution doit impérativement être possible sur des environnements virtualisés.		2
18	Le module doit disposer d'un système anti-fraude électronique.		2

19	Le module doit inclure un module de compensation entre les différents acteurs de la place ainsi que le règlement via les canaux de règlement en place.		2
20	Le fournisseur doit disposer d'un support 24/24 7/7 avec un système de ticketing électronique.		2
21	Le processus et les SLA de traitement des incidents doivent être décrits et détaillés.		2
			Max
I.5. Module d'interopérabilité par Internet			**31**
1	Le module doit permettre à l'utilisateur d'accéder en ligne en une seule interface à tous ses comptes bancaires, tous ses portefeuilles et toutes ses cartes bancaires ;		2
2	Le module doit permettre à l'utilisateur d'effectuer en ligne les opérations de virements compte-à-compte, compte-à-portefeuille, portefeuille-à-portefeuille, compte-à-carte, portefeuille-à-carte, portefeuille-à-compte, carte-à-carte, carte-à- portefeuille, carte-à-compte;		2
3	La mise en place d'une passerelle unique de paiement en ligne englobant tous les moyens de paiement disponibles au Burundi ;		2
4	Le module doit permettre d'effectuer des paiements en ligne de biens et services en utilisant un moyen de paiement de son choix (carte bancaire, compte bancaire, portefeuille) ;		2
5	L'intégration du module de paiement en ligne avec le module de lutte contre le blanchiment des capitaux et le financement du terrorisme (AML et CFT);		2
6	La possibilité d'effectuer des paiements P2P, P2G et P2B en ligne ;		1
7	La possibilité d'effectuer des paiements B2P, B2G et B2B en ligne ;		1
8	La possibilité d'effectuer des paiements G2P, G2G et G2B en ligne ;		1
9	Le module doit permettre l'interopérabilité de toutes les plateformes Web-Banking existantes et à venir ;		2
10	Le module doit permettre le paiement et règlement instantané en ligne.		2
11	L'intégration du module d'interopérabilité Internet avec le système RTGS pour le règlement des soldes nettes résultant de la compensation des transactions en ligne.		2
12	La solution doit être totalement APIsé, la documentation de l'API doit être détaillé est disponible (en français et anglais).		2
13	L'architecture technique détaillé de la solution doit être disponible ; l'installation de la solution doit impérativement être possible sur des environnements virtualisés.		2
14	Le module doit disposer d'un système anti-fraude électronique.		2
15	Le module doit inclure un module de compensation entre les différents acteurs de la place ainsi que le règlement via les canaux de règlement en place.		2
16	Le fournisseur doit disposer d'un support 24/24 7/7 avec un système de ticketing électronique.		2

17	Le processus et les SLA de traitement des incidents doivent être décrits et détaillés.		2
			Max
I.6. Module de gestion backoffice, règlement et de prévention contre la fraude			**23**
1	Le module doit permettre en réconciliation en temps réel, quasi-temps réel et back-office entre les différents acteurs de la place.		3
2	Le module doit mettre à disposition une 360° de la clientèle de la banque.		3
3	Le module doit permettre la gestion des Alias comme moyen d'identification unique auprès de la BRB.		2
4	La réconciliation doit être disponible pour les différents types de transaction disponible (Carte/Mobile/Internet).		3
5	Le module doit être interfaçable avec les systèmes de règlements de la place.		3
6	Le module doit générer les états nécessaires pour permettre aux acteurs de la place de suivre leurs activités d'interopérabilité.		3
7	Le module doit mettre à disposition une interface pour la gestion des litiges pour les activités par carte, par mobile et par internet.		3
8	La solution doit mettre à disposition un module de gestion de la fraude par carte, par mobile et par internet.		3
			Max
I.7. Platforme de Paiement délégataire			**42**
1	La plateforme doit permettre les échanges de flux transactionnels en temps réel, quasi-temps réel et back-office. La solution doit être modulaire et basée sur les technologies de développement standards en vigueur.		2
2	La solution doit permettre la connexion avec la plateforme d'interopérabilité décrite dans le paragraphe ci-dessus.		2
3	La solution devra disposer d'une partie front office et d'une partie back office.		2
4	Le front office regroupera tous les services onlines afin de permettre aux clients d'échanger des flux en temps réel.		2
5	La partie backoffice doit permettre l'échange de fichiers et couvrir l'ensemble du cycle de la transaction (présentation, impayé, représentation, etc.)		2
6	La solution devra offrir des web services IN et OUT (quasi temps réel) financiers pour la prise en charge des flux de ces acteurs ;		2
7	Les spécifications techniques et fonctionnelles de la solution doivent être fournies en français et anglais ;		2
8	Trois (03) références similaires au contexte de cette consultation doivent être proposées ;		2
9	La solution devra être multi-institutions et de préférence multi-langues (Français, Anglais, …)		2
10	La solution doit supporter toutes type de cartes (VISA , MasterCard , Local , CPA) (Debit, Credit et prepayé)		2
11	La solution doit supporter le standard de carte EMV.		2
12	La solution doit supporter le protocole ISO 8583		2

13	Le fournisseur doit fournir les éléments nécessaires afin de permettre un transfert de connaissances garantissant une montée en compétences des équipes (documentation, formation et suivi lors de la mise en service, …) ;		2
14	La fourniture d'un support efficient après la mise en production de la plateforme (période de garantie et de maintenance de la solution et des spécifications) ;		2
15	La formalisation des SLA sur la disponibilité des équipes support et la qualité de fonctionnement de la plateforme.		2
16	La solution doit certifier PCI-DSS afin de respecter les standards de sécurité monétique internationaux ;		2
17	La solution doit être certifiée VISA / Mastercard / UPI et autres réseaux internationaux, régionaux et nationaux ;		2
18	La solution doit être totalement APIsé, la documentation de l'API doit être détaillé est disponible (en français et anglais).		2
19	L'architecture technique détaillé de la solution doit être disponible ; l'installation de la solution doit impérativement être possible sur des environnements virtualisés.		2
20	Le fournisseur doit disposer d'un support 24/24 7/7 avec un système de ticketing électronique.		2
21	Le processus et les SLA de traitement des incidents doivent être décrits et détaillés.		2
I.8. Interopérabilité des Fintechs			**2**
1	La solution devra être équipe d'un module d'interopérabilité connectant toutes les fintechs existantes et à venir à toutes les infrastructures de paiement disponible dans le pays		2
			Max
1.9. Tableau de bord d'administration			**6**
1	Le soumissionnaire présente un outil, sous forme de tableau de bord de gestion, permettant, à l'administrateur, de suivre en temps réel, l'ensemble des activités fonctionnelles et techniques en cours de traitement par la solution.		3
2	Le soumissionnaire présente comment sa solution peut permettre une amélioration/modification des paramètres de suivi de chaque module		3
			Max
1.10. Production des rapports et des statistiques			**4**
1	Chaque module est doté d'un outil d'extraction de données à partir de sa propre base de données et de formatage de rapports, standards et par requête, que le participant utilisera librement pour produire des statistiques, dont les principales concernent les volumes d'échanges par contrepartie, par catégorie d'opérations et par devise, sur des périodes définies.		2

2	Chaque module est doté d'une fonctionnalité de rapport qui est à la fois standardisée et définie par l'utilisateur qui aura la possibilité d'interroger la base de données et de produire un rapport standard et/ou un rapport établi sur base des critères spécifiques choisis par l'utilisateur.		2
			Max
1.11. Facturation			**4**
1	Le soumissionnaire précise, dans son offre, les options possibles des services facturés pour chaque module.		2
2	Le système fournit un mode de calcul des frais ainsi que la possibilité, pour l'administrateur, de pouvoir configurer, par paramétrage, les différentes possibilités offertes par le système et convenues entre participants.		2
TOTAL			
ST	**ST = Score Technique**		**251**
II. OFFRE FINANCIERE			
SF	**SF = Score Financier**		**50**

XII. EVALUATION DES OFFRES RETENUES A L'OUVERTURE POUR LA SOLUTION DE DIGITALISATION

1. La spécification des besoins détaille les exigences techniques obligatoires. La conformité est déterminée par comparaison des spécifications proposées par le soumissionnaire aux exigences requises décrites dans ce document.

Critères	Note
Conformité aux exigences techniques obligatoires : Le soumissionnaire doit proposer un système qui couvre tous les aspects des exigences requises et doit expliquer clairement comment le système proposé répond aux exigences fonctionnelles et non-fonctionnelles mentionnées dans ce document. Le soumissionnaire doit renseigner la fiche d'exigence en annexe à ce document en faisant référence au chapitre couvrant le besoin dans la documentation. **Note = (Nbr de Point * 70) / 251** Le soumissionnaire se verra attribuer les Points comme suit (en fonction du % des exigences rencontrées) : a) Le soumissionnaire aura 100% des points si le besoin est totalement couvert ; b) Le soumissionnaire aura 50% des points si le besoin est partiellement couvert; c) Le soumissionnaire aura 0 (zéro) point si le besoin n'est pas couvert. d) Le fournisseur se verra attribuer des points bonus si des services à	70

valeurs ajoutés sont proposés dans son offre, le bonus global ne peut dépasser 30 Points. (Chaque service ne peux dépasser 3 points de bonus) ***Le soumissionnaire doit obtenir au moins une note de 65 pour valider cette section.***	

2. Le soumissionnaire doit démontrer qu'il a déjà fourni et mis en œuvre des Switch Nationaux de Paiement.

Critères	**Note**
Expérience pertinente du soumissionnaire : Preuve que le soumissionnaire a, au cours des 10 dernières années, fourni et implémenté avec succès au moins 3 Systèmes Nationaux de Paiement d'importance systémique qui sont actuellement en production, et dont 2 devraient être en Afrique. Cette preuve doit être constituée par des lettres de référence/recommandation des clients du soumissionnaire. La Banque vérifiera toutes les informations fournies. Le soumissionnaire se verra attribuer les notes comme suit : a) Si le soumissionnaire possède moins de 3 références pertinentes : attribuer la note 0 ; b) Si le soumissionnaire possède 3 références pertinentes et vérifiées : attribuer la note 25 ; c) Si le soumissionnaire possède plus de 3 références pertinentes et vérifiées : attribuer la note 30. Dans le cas d'un Consortium, toutes les sociétés membres du Consortium doivent témoigner d'une expérience pertinente. ***Le soumissionnaire doit obtenir au moins 25 points pour ce critère.***	30

3. Le soumissionnaire doit démontrer qu'il dispose du personnel possédant les compétences et l'expérience requises pour fournir, implémenter et assurer le support des Switch Nationaux de Paiement.

Critères	**Note**
Expérience et Qualification du Personnel Clé : Les ressources du soumissionnaire doivent avoir déjà travaillé sur au moins 3 projets de mise en œuvre de systèmes de paiement d'importance systémique avec des Banques Centrales et doivent avoir une expérience	20

professionnelle avérée dans la mise en œuvre de formats de messages ISO 20022. Il doit s'agir du personnel réel que le soumissionnaire compte déployer pendant toute la durée du projet.

1. **Chef de Projet (un)**

a) Diplôme de Master en Technologies de l'Information, Ingénierie, Commerce, Administration des Affaires ou Domaine d'études connexe (0.5 point) ;
b) Certification professionnelle en méthodologies de gestion de projets avec une institution de renommée internationale (Certification PRINCE2/PMP/Agile) (1 point) ;
c) Minimum de 5 ans d'expérience dans la gestion des projets informatiques complexes (2 points).

Le soumissionnaire doit obtenir au moins 3 points pour le Chef de Projet.

2. **Analyste Commercial (Un)**

a) Diplôme de Master en Technologies de l'Information, Ingénierie, Commerce, Administration des Affaires ou Domaine d'études connexe (0.5 point) ;
b) Certification professionnelle pertinente (telle que CBAP/CCBA) (0.5 point) ;
c) Minimum de 3 ans d'expérience dans les méthodologies et frameworks d'analyse commerciale spécifiques. Une vaste expérience dans la collecte des exigences, l'analyse des processus métiers et la traduction des besoins métiers dans les spécifications techniques. Le personnel doit posséder de solides capacités d'analyse et des compétences en communication pour collaborer efficacement avec les parties prenantes. (0.5 points).

Le soumissionnaire doit obtenir au moins 1 points pour l'Analyste Commercial.

3. **Architecte de Solutions (Un)**

a) Diplôme de Master en Technologies de l'Information, Ingénierie, Administration des Systèmes ou Domaine d'études connexe (0.5 point) ;
b) Certifications professionnelles liées aux architectures informatiques d'entreprise, telles que TOGAF, ou certifications spécifiques au fournisseur (0.5 point) ;
c) Minimum de 3 ans d'expérience approfondie en conception de systèmes. Le personnel doit posséder une compréhension approfondie des systèmes de paiement, modèles architecturaux, sécurité, évolutivité et intégration. (1 points).

Le soumissionnaire doit obtenir au moins 1.5 points pour l'Architecte de Solutions. **4. Développeur (Un)** a) Diplôme de Master en Technologies de l'Information, Ingénierie, Développement d'applications Desktop/Web/Mobiles (0.5 point) ; b) Certifications professionnelles en MCP, OCP ou certifications pertinentes liées à des langages (Java, PHP, C++, Python, React, Kotlin, Dart, etc.) ou à des frameworks de programmation spécifiques (Flutter, Laravel, Xamarin, etc.) utilisés dans le projet (0.5 point) ; c) Minimum de 3 ans d'expérience en systèmes de traitement de transactions/paiements. L'intégration des API et la connaissance des bonnes pratiques de sécurité sont essentielles. (0.5 point). ***Le soumissionnaire doit obtenir au moins 1.5 points pour le Développeur.*** **5. Spécialistes des Infrastructures/Réseau (Deux)** a) Diplôme de Master en Technologies de l'Information, Ingénierie, Réseaux ou Domaine d'études connexe (0.5 point) ; b) Certifications professionnelles liées aux infrastructures Réseau et Sécurité telles que CCNP, CCIE, CISSP ou CEH (0.5 point) ; c) Minimum de 3 ans d'expérience dans la conception, la mise en œuvre et la gestion des infrastructures réseau pour les systèmes critiques. Connaissance des protocoles réseau, des mesures de sécurité, configurations de la Haute Disponibilité et les pratiques de reprise après sinistre. (1 point). ***Le soumissionnaire doit obtenir au moins 3 points pour les Spécialistes des Infrastructures/Réseau (1.5 points maximum pour chacun des 2).*** **6. Administrateur de base de données (Un)** a) Diplôme de Master en Technologies de l'Information, Ingénierie, Bases de données ou Domaine d'études connexe (0.5 point) ; b) Certifications professionnelles pour les plateformes de bases de données utilisées dans le Projet comme Oracle, Microsoft SQL Server, SQLite, Firebase, Firestore ou Room Database, etc. (1 point) ; c) Minimum de 5 ans d'expérience dans les systèmes de gestion de bases de données (SGBD) et dans la gestion des bases de données transactionnelles en temps réel et à grande échelle. Connaissance de la conception, l'optimisation, la sécurité, les procédures de sauvegarde et de récupération des bases de données. Expérience relative aux nouvelles bases de données mobiles comme Firebase et Firestore (1 point).	

Le soumissionnaire doit obtenir au moins 1.5 points pour l'Administrateur de base de données.

7. **Spécialiste de la sécurité (Un)**

a) Diplôme de Master en Technologies de l'Information, Ingénierie, Sécurité ou Domaine d'études connexe (0.5 point) ;
b) Certifications professionnelles en sécurité de l'information telles que CompTIA Security+, CISA, CEH, CISSP, etc. (0.5 point) ;
c) Minimum de 5 ans d'expérience dans la sécurité de l'information des entreprises. Connaissances approfondies des frameworks et standards de sécurité pertinents pour le Projet (1 point).

Le soumissionnaire doit obtenir au moins 1 points pour le Spécialiste de la sécurité.

8. **Equipe de Déploiement et Support (Deux)**

d) Diplôme de Master en Technologies de l'Information, Ingénierie, ou Domaine d'études connexe (0.5 point) ;
e) Certifications professionnelles liées à ITIL pour la gestion des services informatiques ou des certifications spécifiques au fournisseur pour les technologies utilisées dans le déploiement et le support. (0.5 point) ;
f) Minimum de 5 ans d'expérience dans la configuration et le déploiement des systèmes, de préférence avec une expertise dans la gestion des systèmes à tâches critiques. Connaissances approfondies dans le troubleshooting, les pratiques ITIL, la gestion du changement, le monitoring des systèmes et la gestion des incidents. (1 point).

Le soumissionnaire doit obtenir au moins 3 points pour l'Equipe de Déploiement et Support (Maximum 1.5 points pour chacun des 2 membres de l'Equipe).

Les soumissionnaires doivent fournir les éléments de preuve suivants pour le personnel ci-dessus :

- *CVs au format fourni dans ce document signé par le personnel proposé et par le soumissionnaire.*
- *Copies des Diplômes académiques et des Certificats Professionnels.*
- *Copies des Passeports ou des Cartes Nationales d'Identité du personnel proposé.*
- *Veuillez noter que le soumissionnaire ne sera pas autorisé à remplacer un personnel par un autre qui ne faisait pas partie de la proposition sans l'approbation préalable de la Banque.*
- *Un soumissionnaire qui ne parvient pas à fournir toutes les resources*

clés indiquées ci-dessus sera disqualifié immédiatement. ***Le soumissionnaire qui obtient moins de 15 points pour ce critère sera disqualifié immédiatement.***	

4. Le soumissionnaire doit soumettre un plan détaillé de mise en œuvre du Projet comprenant des plans de travail, des graphiques et tableaux des délais d'exécution, toutes les activités avec des critères de clôture clairs, livrables du projet, tests d'acceptation, etc.

Critères	**Note**
Plan d'implémentation du Projet : Le soumissionnaire doit couvrir en détail tous les éléments relatifs à la mise en œuvre du Projet et les méthodologies d'une manière claire, concise, et pertinente par rapport à la portée de l'offre. N.B. : Le soumissionnaire sera évalué sur la base d'une documentation adéquate de chacun des domaines suivants : a) Graphique chronologique basé sur GCC 20.1 (0.5 point) ; b) Liste détaillée des activités avec des critères de clôture clairs. (0.5 point) c) Liste des livrables du projet y compris la documentation et les procédures opérationnelles standard. (0.5 point) d) Calendrier détaillé du personnel pendant la mise en œuvre du Projet montrant les délais et les périodes pendant lesquels chaque ressource/personnel/consultant doit être déployé sur site et à distance. (0.5 point) e) Tests d'acceptation. (0.5 point) f) Activités Go-Live. (0.5 point) ***Le soumissionnaire doit obtenir au moins 2 points pour ce critère.***	3

5. Le soumissionnaire doit soumettre une Proposition de Support et de Maintenance.

Critères	**Note**
Support et Maintenance : a) Proposition détaillée pour le Support et la Maintenance après-vente, et détails du Support qui sera fourni après la mise en service et après la garantie, pour une durée de 3 ans. Une proposition de Support détaillée doit être clairement étiquetée et soumise dans le cadre de la proposition technique. Cela devrait montrer toutes les exclusions, le	4

cas échéant. Cependant, le prix du Support doit être inclus dans une enveloppe séparée de la proposition financière, et clairement décomposée pour chaque année. (2.5 points) ; b) Expérience du personnel de Support. Le personnel de Support doit avoir au moins 5 années d'expérience pratique avec le système particulier proposé par le soumissionnaire et certifications professionnelles pertinentes du fabricant. Veuillez vous référer aux exigences relatives à l'Equipe de Déploiement et de Support. (1.5 point) ***Le soumissionnaire doit obtenir au moins 3 points pour ce critère.***	

6. Le soumissionnaire doit soumettre un Plan des services de formation et de transfert de connaissances.

Critères	**Note**
Plan de services de formation et de transfert de connaissances : Le soumissionnaire doit s'engager à assurer la formation et le transfert de connaissances à la Banque et aux parties prenantes pour renforcer les capacités dans la gestion, le support et la maintenance des Systèmes de Paiement Nationaux en fournissant une proposition sur mesure qui sera convenue d'un commun accord par les deux parties. Cependant le prix des services de formation et de transfert de connaissance doit être inclus dans un enveloppe séparée de proposition financière et doit être clairement divisée (par article de formation) et détaillée en conséquence. ***Le soumissionnaire doit obtenir au moins 2 points pour ce critère.***	3

7. Le soumissionnaire doit effectuer une démonstration du produit proposé pour présenter ses caractéristiques, ses fonctionnalités et ses avantages.

Critères	**Note**
Démonstration du produit : Sur invitation de la Banque, les soumissionnaires éligibles devront démontrer tous les aspects de la solution proposée pour présenter ses caractéristiques, ses fonctionnalités et ses avantages. Les critères de démonstration du produit doivent couvrir les éléments suivants : a) Cas d'utilisation (3 points) ;	10

b) Exigences fonctionnelles (4 points) ; c) Exigences non-fonctionnelles (3points). Tous les coûts liés à la démonstration du produit seront à la charge du soumissionnaire. ***Le soumissionnaire doit obtenir au moins 9 points pour ce critère.***	

8. Le soumissionnaire doit soumettre un Plan des services de formation et de transfert de connaissances.

Critères	**Note**
Vérification des informations et Diligence raisonnable : Sur invitation du fournisseur la Banque effectuera des visites chez les clients indiqués comme références dans leurs offres pour vérifier les informations incluses dans le dossier d'appel d'offre et confirmer la capacité du soumissionnaire pour exécuter le Projet. Les visites de sites seront axées sur l'expérience des utilisateurs des services fournis et des fonctionnalités du système mis en œuvre sur ces sites, et dans toute zone d'opération que la Banque peut juger nécessaire pour faire preuve de diligence raisonnable dans le processus d'évaluation. Le soumissionnaire organisera également une visite de la Banque à ces locaux afin de constater la capacité et le processus de support mis en place par le fournisseur. Les visites sur place doivent faire partie du processus d'évaluation. Les frais de ces visites seront à la charge du soumissionnaire. Seuls les clients des soumissionnaires qui auront démontré l'expérience et les capacités requises et qui auront satisfait à toutes les exigences fonctionnelles et non-fonctionnelles seront visités. ***Le soumissionnaire doit obtenir au moins 9 points pour ce critère***	10

Le résumé des scores techniques se présente comme suit :

CRITERES	**NOTE MAXIMALE**	**NOTE MINIMALE**
Conformité aux exigences techniques obligatoires	**70 points**	**65 points**
Expérience pertinente du soumissionnaire	**30 points**	**25 points**
Expérience et Qualification du Personnel Clé	**20 points**	**15 points**
Plan d'Implémentation du Projet	**3 points**	**2 points**
Support et Maintenance	4 points	**3 points**
Services de Formation et de Transfert de Connaissances	**3 points**	**2 points**

Démonstration du produit	**10 points**	**9 points**
Vérification des Informations et Diligence Raisonnable	**10 points**	**9 points**
TOTAL EVALUATION TECHNIQUE	**150 points**	**130 points**

*** Le score Minimum pour se qualifier à l'analyse financière doit être de 130 points.**

- **L'offre financière devra contenir les documents suivants :**

3. La lettre de soumission financière ;
4. Les bordereaux des prix pour chaque module, comprenant tous les droits et taxes payables au Burundi ;

NB : L'absence ou la non validité de l'un des documents énumérés ci-dessus constitue une cause de rejet d'office de l'offre.

XIII. PRESENTATION DES OFFRES

Les offres rédigées en Français seront envoyées en **un (1) original en version papier** et en **une (1) version électronique sur une clé USB**. En cas de divergence entre l'original et la version numérique, seul l'original fera foi. Les offres (techniques et financières) seront présentées dans deux (2) enveloppes fermées et séparées, comportant respectivement les mentions « **OFFRE TECHNIQUE** » et « **OFFRE FINANCIERE** ».

Les deux (2) enveloppes seront glissées dans une enveloppe extérieure fermée portant la mention « **Offre pour le recrutement d'une firme (cabinet) chargée de l'implémentation d'une solution de digitalisation complète du secteur financier du Burundi** ».

Les enveloppes contenant les offres seront envoyées à l'adresse ci-après :

Monsieur le Gouverneur de la Banque de la République du Burundi

1, Avenue du Gouvernement

B.P. 705 Bujumbura

Tél. (+0257) 22 40 00 00 / Fax. (+257) 22 22 31 28

E-mail : brb@brb.bi

Outre cette adresse, l'enveloppe extérieure portera les inscriptions : « **A n'ouvrir qu'en séance d'ouverture des offres** ».

L'enveloppe extérieure ne doit comporter aucun signe distinctif du soumissionnaire.

Toute enveloppe ouverte ou ne respectant pas la formalisation ci-dessus mentionnée ne pourra pas être

acceptée.

XIV. DEPOT ET OUVERTURE DES OFFRES

Les propositions seront adressées au Gouverneur de la Banque de la République du Burundi et déposées au Secrétariat de la Direction de la Banque situé au 5eme étage, au plus tard le 21/6/2024 à 10h00.L'ouverture aura lieu au même jour à 10h30 minutes dans une des salles de réunion du Siège de la BRB en présence des concourants qui le souhaitent.

Les offres financières seront ouvertes plus tard après l'évaluation des offres techniques pour les seuls candidats techniquement qualifiés.

XV. MONNAIE DE SOUMISSION

La monnaie de soumission est l'USD ou EURO pour les soumissionnaires étrangers, le Franc Burundi pour les soumissionnaires locaux.

XVI. GARANTIE DE SOUMISSION

L'offre est accompagnée d'une garantie bancaire de soumission par message SWIFT au profit du compte de la BRB pour un montant de cent cinquante mille dollars américains (150 000 USD) pour les soumissionnaires étrangers, ou équivalent en franc Burundi pour les soumissionnaires locaux.
La garantie de soumission sera restituée au soumissionnaire non gagnant après notification du marché. Elle ne sera pas restituée au soumissionnaire retenu qui se désistera.

XVII. MODALITES DE MISE EN ŒUVRE

Le soumissionnaire sera recruté selon les termes et conditions de la BRB et entreprendra les tâches et responsabilités assignées sous la supervision directe de la BRB.
La planification des différentes réunions entre la firme et les différentes institutions de microfinance, établissements de crédit et les établissements de paiement mobile sont sous la coordination de la BRB.

XVIII. VISITE AU COURS DE LA PHASE D'EVALUATION

Une visite sur site, d'au moins deux références présentées dans l'offre du Soumissionnaire sera organisée à la seule discrétion de la BRB pendant le processus d'évaluation et avant la **notification du marché**.

XIX. LANGUE DU MARCHE

La langue du présent marché est le Français. Les soumissions, le contrat, les rapports et toute autre correspondance sont rédigés en Français.

XX. MODALITES DE PAIEMENT

Les paiements seront effectués sur présentation des factures détaillées comme suit :

- 20% du montant total du marché dès la signature du contrat, sur production d'une garantie bancaire (par message SWIFT pour les soumissionnaires étrangers) du même montant et présentation de la facture y relative.
- 20% à la réception de chaque module (Identification, Interopérabilité sur carte et TPE, paiement par téléphone mobile et paiement par internet).

XXI. DROIT APPLICABLE

Le présent marché est régi par le droit burundais, spécialement le règlement de Passation des Marchés de la Banque de la République du Burundi disponible sur www.brb.bi.

XXII. DEMANDE D'INFORMATIONS COMPLEMENTAIRES

Toutes questions ou demandes d'informations additionnelles concernant les présents TDRs seront envoyées à l'adresse e-mail : brb@brb.bi, au plus tard quinze (15) jours calendrier avant la date limite de dépôt des offres. Les réponses aux questions de clarification des soumissionnaires seront communiquées simultanément par courrier électronique à tous les candidats soumissionnaires au plus tard (10) jours avant la date butoir de dépôt des offres.

BANQUE DE LA REPUBLIQUE DU BURUNDI

Alexis NKUNZIMANA
Conseiller de Direction

BANQUE DE LA REPUBLIQUE BRB DIRECTION DU BURUNDI

Irène KABURA MURIHANO
1er Vice-Gouverneur