بنك المغرب
BANK AL-MAGHRIB

Département Surveillance des Systèmes et Moyens de Paiement et Inclusion Financière

LC/BKAM/2018/70 Rabat, le 12 novembre 2018

LETTRE CIRCULAIRE RELATIVE AU PAIEMENT MOBILE DOMESTIQUE

Considérant les dispositions de la Décision n°392/W/18 du 12 novembre 2018 relative au paiement mobile domestique ;

Il est décidé ce qui suit :

Article 1

La présente Lettre Circulaire a pour objet de fixer les conditions et modalités d'offre du paiement mobile « m-wallet », entre les émetteurs, acquéreurs et switch mobile.

Elle englobe les règles de place techniques et de sécurité adoptées applicables à l'ensemble des acteurs, ainsi que les règles relatives aux traitements des réclamations, incidents et litiges.

I. Règles Techniques et de Sécurité :

Article 2

Les Principes directeurs régissant le « m-wallet » sont fixés comme suit :

- Chaque « m-wallet » dispose d'un identifiant transactionnel unique qui est le numéro de téléphone de son titulaire et d'un identifiant technique unique, conformément aux modalités fixées par le switch mobile ;

- Pour les transactions interopérées, la correspondance entre cet identifiant et le « m-wallet » se fait grâce à la table de correspondance, visée à l'article 4 ci-dessous, et opérée par le switch mobile. De ce fait, chaque « m-wallet » émis doit être déclaré à sa création au switch mobile et l'inscription des « m-wallet par défaut » à la table de correspondance est obligatoire lors de l'enrôlement du client.

- Les transactions une fois validées sont irréversibles pour l'émetteur ;

- Les flux d'échange se font en Single message ;

- Les fichiers de fin de journée sont transmis par le switch à des fins de reporting et pour faciliter la réconciliation comptable des banques et EdP ;

- Chaque établissement est responsable de la gestion des flux entre ses utilisateurs et sa plateforme de paiement « flux On-Us ». On entend par « flux On-Us », les opérations réalisées entre un « m-wallet » et un autre « m-wallet » domicilié au sein

d'un même établissement (Réception des flux sur le « m-wallet » par défaut). En cas de multiplicité de « m-wallet » du destinataire des fonds, le « m-wallet » à considérer est celui qui a été désigné par le client en tant que « m-wallet par défaut», comme indiqué plus bas ;

- Les cinématiques « On Us » sont librement gérées par les établissements ;

- Les canaux et outils technologiques sont laissés au libre choix des établissements qui peuvent choisir un ou plusieurs des canaux spécifiés ou innover en déployant de nouveaux canaux / technologies ;

- Il est recommandé d'avoir des interfaces utilisateurs et des étapes de cinématiques identiques pour les transactions « On Us » et « Off Us » pour offrir une expérience utilisateur transparente.

Article 3

L'architecture globale du paiement mobile est articulée autour d'un switch mobile chargé d'assurer les fonctions suivantes :

- Routage des transactions, basé sur la table de correspondance ;
- Suivi des soldes et fourniture des données permettant la compensation ;
- Gestion et tenue à jour de la table de correspondance ;
- Notification à l'ensemble des établissements en temps réel de tout changement du « m-wallet par défaut »;
- Déversement des soldes issus de la compensation des transactions 'paiement mobile' au niveau du SRBM.

Les protocoles adoptés pour assurer ses fonctions sont les suivants :

- Le protocole « SID dérivé ISO8583 » actuel mis à jour pour les besoins du paiement mobile. Ses nouvelles spécifications SID sont disponibles au niveau du switch mobile : Ce protocole gère nativement les besoins de crédit/débit en temps réel.
- Le protocole de compensation « fichiers LIS » actuel mis à jour pour les besoins du paiement mobile notamment par la création d'un fichier logique dans le LIS pour le reporting sur Transactions relatives au paiement mobile ;

Article 4

Le routage des transactions inter-opérées se fait sur la base de la table de correspondance. Elle permet de déterminer l'établissement détenteur du « m-wallet par défaut» du client bénéficiaire identifié par son numéro de téléphone.

La structure de cette table de correspondance ainsi que ces modalités de gestion sont présentées à l'annexe 1.

Article 5

Les établissements émetteurs et acquéreurs ont pour responsabilité de se conformer, au minimum, aux règles ci-après :

1. **RS1 :** les transactions ne peuvent être initiées qu'après les étapes préalables d'authentification du client ;
2. **RS2 :** la saisie à plusieurs reprises d'informations d'authentification erronées déclenche un mécanisme d'authentification complémentaire ou un blocage du « m-wallet » ;
3. **RS3 :** le profil de risque des clients et de leurs transactions doit être contrôlé et maitrisé pour réduire les risques de fraude ;
4. **RS4 :** les agents qui sont également commerçant acceptant ne peuvent pas utiliser leur compte de paiement 'Agent' pour l'acceptation des paiements commerçant.

Article 6

Le format du QR Code Place pour effectuer des transferts & paiements inter-établissements de paiement est basé sur le format QR-Code défini dans le document [**EMV_QRCPS**] (Cf. Annexe 2). Comme spécifié dans [EMV_QRCPS], le contenu du QR-Code doit être au format texte UTF-8 et avoir une taille maximale de 512 caractères.

II. Règles de Gestion des Exceptions :

Article 7

Les clients peuvent détenir plusieurs « m-wallet », que ce soit auprès de plusieurs établissements (banques/établissements de paiement) ou auprès du même établissement.

En cas de détention de plusieurs « m-wallet », les règles de gestion suivantes doivent être appliquées :

- La sélection du «m-wallet par défaut » est faite obligatoirement par le client ;
- La demande de sélection du «m-wallet par défaut » est systématique à chaque ajout d'un « m-wallet ». Elle est vérifiée par l'envoi d'un OTP au client par le switch mobile.
- Le « m-wallet par défaut» est utilisé pour la réception des flux ;
- Le client peut changer à tout moment son « m-wallet par défaut » ;
- Le Switch assure la centralisation et la diffusion des informations sur le « m-wallet par défaut » auprès des émetteurs concernés :
  - L'établissement domiciliataire dont le « m-wallet» a été sélectionné comme « m-wallet par défaut » est notifié ;
  - L'établissement auprès duquel le client avait précédemment son « m-wallet par défaut » est également notifié de ce changement.

Article 8

Dans le cas de figure où le Destinataire ne dispose pas de « m-wallet », l'annulation de l'opération est automatique avec envoi d'une notification à l'émetteur ainsi qu'au numéro du destinataire pour information sur la raison de l'annulation.

بنك المغرب
BANK AL-MAGHRIB

III. Règles de Gestion des Réclamations, Incidents et Litiges :

Article 9

Les mécanismes de Gestion des réclamations et de Gestion des incidents doivent respecter, au minimum, les principes ci-dessous :

- La gestion des annulations est automatique et se fait en temps réel ;
- Les requêtes et réclamations émises par un utilisateur sont toujours instruites et traitées par l'établissement détenteur du « m-wallet » ;
- le délai maximal de gestion des réclamations, et spécifiquement pour les transactions de paiement et de retrait GAB, ne peut excéder un délai maximum de 5 jours ouvrables ;
- Le client doit disposer d'un délai suffisant, qui ne peut être inférieur à 7 jours, pour pouvoir faire une contestation, liée notamment à une erreur d'exécution de paiement ou à un prélèvement indu des commissions ;
- En cas de litiges, la plateforme du switch mobile fait office de base de référence de l'ensemble des transactions « Off Us ».

IV. Autres dispositions

Article 10

Les acteurs de l'écosystème mobile s'engagent à mettre en place une Veille technologique place autour du « Paiement Mobile » pour améliorer les fonctionnalités du « m-wallet ».

Les acteurs de l'écosystème mobile s'engagent à instaurer une veille continuelle sur les normes de sécurité afférentes au paiement mobile et ce, en complément des normes édictées par Bank Al-Maghrib.

Article 11

Les dispositions de la présente lettre circulaire entrent en vigueur à la date de sa signature.

Signé : Mme Hakima EL ALAMI

Signé : A. BENNANI

بنك المغرب
BANK AL-MAGHRIB

Annexe 1

Structure de la table de correspondance

La structure de la table de correspondance est conçue de façon à pouvoir remplir les objectifs qui lui sont fixés, à savoir le routage des transactions inter-opérées. Par ailleurs, elle permet également de traiter les processus suivants :

- Gestion des types de comptes;
- Gestion du multi-wallet ;
- Gestion de la sécurisation des modifications de la table.

Numéro de téléphone	Type de compte	Code EdP	Identifiant du wallet dans le SI de l'EdP	Statut	Clé pour modification	Date et heure de création	Date et heure de modification

➢ *Elément N°1 : Numéro de téléphone*

Ce champ contient le numéro de téléphone du client et est utilisé, entre autre, pour la gestion du multi-wallet.

➢ *Elément N°2 : Type de compte*

Ce champ optionnel contient le type de compte du client pour la gestion du niveau du compte et des règles associées :

1 – Type de compte 1 limité à 200 MAD
2 – Type de compte 2 limité à 5 000 MAD
3 – Type de compte 3 limité à 20 000 MAD
4 – Autre type de compte, sans limite (compte bancaire, compte agent).

➢ *Elément N°3 : Code Etablissement de paiement / banque*

Ce champ contient le code établissement permettant d'identifier l'établissement de paiement/banque émetteur du m-wallet par défaut.

Le code EdP/banque est attribué par Bank Al-Maghrib une fois l'établissement agréé.

➢ *Elément N°4 : Identifiant technique du wallet*

Ce champ contient le numéro d'identification technique du m-wallet qui est géré par le switch mobile selon les spécifications techniques fixées par ce dernier.

➢ *Elément N°5 : Statut*

Ce champ informe sur le statut du « m-wallet » : Actif, Suspendu, Résilié.

- *Elément N°6 : Clé pour modification*

Ce champ sert d'Identifiant permettant la modification des informations liées à un numéro de téléphone, afin de sécuriser la maintenance de chaque enregistrement.

- *Elément N°7: Date et heure de création*

Ce champ sert à enregistrer la date et l'heure de création de l'enregistrement par le switch. Le format est JJMMAA/HHMMSS

- *Elément N°8 : Date et heure de dernière modification*

Ce champ sert à enregistrer la date et l'heure de la dernière modification de l'enregistrement dans la table de correspondance. Le format est JJMMAA/HHMMSS.

بنك المغرب
BANK AL-MAGHRIB

Annexe 2

Spécifications techniques relatives au QR Code Paiement Mobile

1. Tronc commun

Cette section a pour objectif de décrire les exigences, de ce format, communes à tous les types d'Operations : transfert P2P (personne à personne) ou paiement commerçant face à face.

1.1. Base de la spécification

Cette spécification est basée sur le format QR-Code Mini dans le document [EMV_QRCPS].
Comme spécifié dans [EMV_QRCPS], le contenu du QR-Code doit être au format texte UTF-8 & avoir une taille maximale de 512 caractères.

1.2. Champs spécifiques

Note : lorsqu'une donnée est encodée au format base64 (voir [BASE64]), le padding « == » (s'il est présent) doit être efface avant stockage dans le QR-Code.

1.2.1. Merchant Account Information Template

L'ID "XX" est indiqué comme étant l'identifiant du Template utilisé pour le Merchant Account Information Template (champs 26 à 51) spécifique au format décrit ci-après. Si le QR Code ne contient qu'un seul Template définissant les informations du compte commerçant, il est suggère d'utiliser l'identifiant « 26 ».

1.2.1.1 Globally Unique Identifier (XX-00)

Ce champ a pour but de clarifier le fait qu'il s'agit d'une opération dont le format est décrit dans le présent document. Sa valeur est constante à 5bb66a92d69c0ea742dd4f754590fa0a.

1.2.1.2 Reserve pour usage futur (XX-01)

Ce champ ne doit pas être utilisé.

1.2.1.3 Format de chiffrement (XX-02)

Ce champ a pour but d'indiquer le format du chiffrement utilisé pour masquer certains champs de ce Template. Liste des valeurs possibles :

Nom valeur	Référence valeur
0	Aucun chiffrement Note : ce mode ne doit être utilisé que pendant la période de tests.
1	Algorithme : AES Mode d'opération : Enchaînement des blocs (Cipher Block Chaining, CBC) Remplissage (padding) : ISO 10126
2-9	Réservé pour un usage futur

1.2.1.4 Reference paramètres de chiffrement (XX-03)

Ce champ a pour but d'indiquer le libellé des paramètres de chiffrement utilisés pour le chiffrement de certains champs de ce Template. Ces paramètres font référence à la clé utilisée (taille de la clé, contenu) ainsi que d'éventuels autres paramètres statiques (exemple : vecteur d'initialisation).

1.2.1.5 Vecteur d'initialisation (XX-04)

Ce champ a pour but, pour les méthodes de chiffrement utilisant un vecteur d'initialisation non statique, de contenir cette valeur nécessaire au déchiffrement. Pour les méthodes de chiffrement n'utilisant pas de vecteur d'initialisation, ce champ doit être absent. Ce vecteur est stocké au format base 64.

1.2.1.6 Format référence entité payée (XX-05)

Ce champ a pour but d'indiquer le format de la référence de l'entité payée.

Liste des valeurs possibles:

Nom valeur	Reference valeur
0	Numéro de téléphone de l'entité payée. Le numéro de téléphone doit être précédé de l'indicatif international & ne doit pas contenir de séparateur ou d'espace.
1-9	Réservé pour un usage futur

1.2.1.7 Reference entité payée (XX-06)

Ce champ a pour but de contenir la référence de l'entité payée. Le format de cette référence est Mini dans le champ « Format référence entité payée ». Cette référence est chiffrée selon la méthode définie dans le champ « Format de chiffrement >». Elle est affichée au format UTF-8 encode en base 64.

Exemple de valeur non chiffrée (XX-02 = 0) :
+212631415927 (brut) ➔ Kz IxMj YzMTQxNTkyNw (base64)

1.2.1.8 Référence entité payée masquée (XX-07)

Ce champ a pour but de contenir une partie de la référence de l'entité payée en clair, le reste étant masqué. Ce champ est interdit si la valeur Format de chiffrement (XX-02) est égale à 0 (non chiffre). Le caractère recommandé de masquage est # (U+0023).

Exemple : pour le numéro de téléphone +212631415927, on peut stocker ('information +2126######27

1.2.1.9 Champs XX-08 a XX-89

Ces champs sont réservés pour un futur usage.

1.2.1.10 Champs XX-90 a XX-99

Ces champs sont à libre usage pour les établissements générant le QR-Code.
La taille totale de ces champs au format TLV ne doit pas dépasser 30 caractères.

1.2.2. Unreserved Templates

L'ID "YY" est indiqué comme étant l'identifiant du Template utilise pour le Unreserved Templates (champs 80 à99) spécifique au format décrit dans ce document.

Si le QR-Code ne contient qu'un seul Template non réservé, il est suggéré d'utiliser l'identifiant « 80 ».

1.2.2.1 Globally Unique Identifier (YY-00)

Ce champ a pour but de clarifier le fait qu'il s'agit d'une opération dont le format est décrit dans le présent document. Sa valeur est constante à 37b3a355b830b3bf0974d23608a6f162.

1.2.2.2 Type d'opération (YY-01)

Ce champ a pour but d'indiquer le type d'opération décrit dans ce QR-Code. Liste des valeurs possibles :

Nom valeur	Reference valeur
0	Transfert P2P face à face
1	Paiement commerçant face à face
2	Paiement commerçant à distance (e-commerce)
3	Paiement livreur face à face
49	Reserve pour un usage futur

1.2.2.3 Date/heure de la génération (YY-02)

Ce champ indique la date ainsi que l'heure de la génération de ce QR-Code au format [IS0_8601]. L'inclusion de l'heure ainsi que du fuseau horaire sont facultatives. L'inclusion des fractions de secondes est déconseillée.

Exemple de valeur : 2017-12-15T17 :23

1.2.2.4 Localisation de l'entité payée (YY-03)

Ce champ indique la localisation géographique de l'entité payée. La donnée est représentée au format degrés décimaux, latitude puis longitude, séparés par un caractère virgule, (U+002C).

Exemple de valeur : 33.529704, 7.63921

1.2.2.5 Format de signature (YY-04)

Ce champ a pour but d'indiquer le format de la signature numérique utilisée pour signer le contenu de ce QR-Code. Liste des valeurs possibles :

Nom valeur	Reference valeur
0	Aucune signature
1-9	Reserve pour un usage futur

1.2.2.6 Champs XX-05 a XX-99

Les champs sont réservés pour un futur usage.

1.3. Tableau des champs :

Nom champ	Tag champ	Obligatoire / Facultatif	Format champ	Taille champ
Merchant Account Information Globally Unique Identifier	XX-00	O	ans	32
Format de chiffrement	XX-02	O	N	1
Référence paramètres de chiffrement	XX-03	F	ans	max 4
Vecteur d'initialisation	XX-04	F	ans	max 16
Format référence entité payée	XX-05	O	N	1
Référence entité payée	XX-06	O	ans	max 32
Référence entité payée masquée	XX-07	F	ans	max 32
Unreserved Template Globally Unique Identifier	YY-00	O	ans	32
Type d'opération	YY-01	O	N	1
Date/heure de la génération	YY-02	F	ans	max 32
Localisation de l'entité payée	YY-03	F	ans	max 23
Format de signature	YY-04	O	N	1

1.4. Affichage du QR-Code

Il est conseillé d'afficher le QR-Code sur le périphérique paye en noir (couleur #000 0 0 0) sur blanc (couleur **#FFFFFF**), avec un minimum de 4 modules de marge blanche. Il est également conseillé, afin de maximiser sa lisibilité par les scanners, de ne pas mettre d'image en superposition du contenu du QR-Code, masquant une partie de ce dernier.

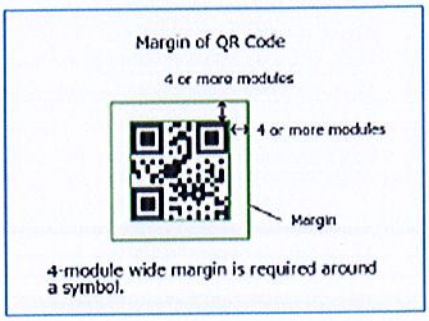

Figure 1 source : http://www.qrcode.com/en/howto/code.html

Il est conseillé d'afficher sur le périphérique paye le montant de l'opération ainsi que la devise, lorsque ces derniers sont disponibles & contenus dans le QR-Code. Lors de la génération du QR-Code, il est également conseillé d'utiliser un niveau minimum de correction d'erreur « Q » (25%, voir [ISO_IEC_18004]).

1.5. Scan du QR-Code

Il est conseillé d'afficher sur l'écran de scan du QR-Code un viseur permettant d'assister l'utilisateur dans son opération de scan.

Le fournisseur de l'application de scan est en charge de tester l'efficacité de son module dans diverses conditions de scan : angle, distance, orientation. Il est également en charge de vérifier que son module est en mesure de supporter les caractères UTF-8 tel qu'exigé par le standard [EMV_QRCPS].

L'application mobile scannée doit envoyer le contenu brut du QR-Code au serveur de son établissement.

1.5.1. Actions après scan

Après le scan du QR-Code, l'application de scan doit effectuer les vérifications suivantes :

- Vérifier que le contenu du QR-Code est bien une chaine de caractères UTF-8
- Vérifier le header du QR-Code : « 000201 »
- Vérifier le CRC du contenu (champ 63)
- Parser le contenu au format TLV, vérifier que le contenu ne contient pas d'erreur
- Vérifier que le contenu contienne bien les deux Templates obligatoires, avec les Globally Unique Identifier associés (champs XX-00 & YY-00)
- Vérifier la présence & le format des champs obligatoires

1.5.2. Affichage des informations

Une fois le QR-Code scanné l'application doit afficher son contenu (en particulier le type de l'opération : transfert P2P, paiement commerçant face à face, ...) avant validation de l'opération par le payeur.

Il est recommandé de ne pas afficher les informations suivantes sur le périphérique du payeur :

- Merchant Category Code (champ 52)

1.6. Véracité des données

Il est de la responsabilité de l'établissement du payé, générant le QR-Code, de vérifier la véracité des données affichées dans son contenu. Afin d'éviter tout risque de fraude par phishing, il est recommandé de porter une attention particulière aux champs suivants :

- Merchant Name (champ 59)
- Merchant City (champ 60)
- Postal Code (champ 61)
- Store Label (champ 62-03)
- Merchant Name—Alternate Language (champ 64-01)
- Merchant City—Alternate Language (champ 64-02)

Toujours dans le but d'éviter tout risque de fraude par phishing, il est également recommandé pour les établissements de vérifier, à chaque notification de paiement, que le contenu des champs précités corresponde bien à la référence de l'entité payée (champ XX-05).

1.7. Note légale

QR Code est une marque déposée de DENSO WAVE.

2. Transfert P2P face à face

Les données décrites dans ce paragraphe sont spécifiques à un QR-Code contenant les données d'un transfert P2P face à face.

Note : les informations du compte paye sont stockées dans les champs « Merchant Account Information Template » (voir section 2.2.1).

2.1. Champs interdits

Dans le cadre d'un transfert P2P face à face, les champs suivant sont interdits & ne doivent pas être contenus dans le QR-Code :

- Merchant Category Code (champ 52)
- Country Code (champ 58)
- Merchant Name (champ 59)
- Merchant City (champ 60)
- Postal Code (champ 61)
- Bill Number (champ 62-01)
- Store Label (champ 62-03)
- Loyalty Number (champ 62-04)
- Reference Label (champ 62-05)
- Customer Label (champ 62-06)
- Terminal Label (champ 62-07)
- Additional Consumer Data Request (champ 62-09)
- Data Objects—Merchant Information—Language Template (champ 64)
- Language Preference (champ 64-00)
- Merchant Name—Alternate Language (champ 64-01)
- Merchant City—Alternate Language (champ 64-02)

Note : cette contrainte annule & remplace la contrainte de la spécification [EMV_QRCPS] qui indique que les champs 52, 58, 59, & 60 sont obligatoires.

2.2. Champ Motif

Il est suggère de laisser au payeur ou au payé la possibilité de saisir manuellement un motif de transaction.

Ce motif doit être stocke dans le champ « Purpose of Transaction » (champ 62-28, maximum 25 caractères en code ASCII).

2.3. Exemple de QR-Code

2.3.1. PseudoCode

```
payloadFormatIndicator (00): 01
pointOfInitiationMethod (01): 12
merchantAccountInformation (26):
-- globallyUniqueIdentifier (26-00): 5bb66a92d69c0ea742dd4f754590fa0a
-- formatDeChiffrement (26-02): 0
-- formatReferenceEntitePayee (26-05): 0
-- referenceEntitePayee (26-06): KzIxMjYzMTQxNTkyNw
-- referenceEntitePayeeMasquee (26-07): +2126######27
transactionCurrency (53): 504
transactionAmount (54): 314.20
additionalDataField (62):
-- purposeOfTransaction (62-08): partage frais repas
unreservedTemplate (80):
-- globallyUniqueIdentifier (80-00): 37b3a355b830b3bf0974d23608a6f162
-- typeOperation (80-01): 0
-- dateHeureGeneration (80-02): 2017-12-15T17:23
-- formatSignature (80-04): 0
crc: XXXX
```

3. Paiement commerçant face à face

3.1. Contraintes métier

Si le commerçant a la possibilité de saisir le montant de l'opération lors de la génération du QR-Code, ce montant doit être non modifiable (hors pourboire tel que prévu par la spécification [EMV_QRCPS]) par le payeur.

Les champs « Merchant Name » (champ 59) & « Merchant City » (champ 60) ne peuvent pas contenir le caractère « / » (U+002F). La taille totale de ces deux champs ne peut pas dépasser 49 caractères.

Les champs suivants ne peuvent pas contenir le caractère « / » (U+002F). La taille totale de ces champs ne peut pas dépasser 49 caractères :

- Bill Number (champ 62-01)
- Mobile Number (champ 62-02)
- Store Label (champ 62-03)
- Loyalty Number (champ 62-04)
- Reference Label (champ 62-05)
- Customer Label (champ 62-06)
- Terminal Label (champ 62-07)
- Purpose of Transaction (champ 62-08)
- Additional Consumer Data Request (champ 62-09)

بنك المغرب
BANK AL-MAGHRIB

3.2. Exemple de QR-Code

3.2.1. Pseudo Code

```
payloadFormatIndicator (00): 01
pointOfInitiationMethod (01): 12
merchantAccountInformation (26):
-- globallyUniqueIdentifier (26-00): 5bb66a92d69c0ea742dd4f754590fa0a
-- formatDeChiffrement (26-02): 0
-- formatReferenceEntitePayee (26-05): 0
-- referenceEntitePayee (26-06): KzIxMjYzMTQxNTkyNw
merchantCategoryCode (52): 5411
transactionCurrency (53): 504
transactionAmount (54): 314.20
countryCode (58): MA
merchantName (59): Epicier
merchantCity (60): Casablanca
merchantInformationLanguageTemplate (64):
-- languagePreference (64-00): ar
-- merchantNameAlternateLanguage (64-01): البقالة
-- merchantCityAlternateLanguage (64-02): الدار البيضاء
unreservedTemplate (80):
-- globallyUniqueIdentifier (80-00): 37b3a355b830b3bf0974d23608a6f162
-- typeOperation (80-01): 1
-- dateHeureGeneration (80-02): 2018-04-05T17:23
-- localisationEntitePayee (80-03): 33.529704,-7.63921
-- formatSignature (80-04): 0
crc: AC77
```

3.2.2. Format Texte

278 caractères UTF-8 :

000201010212266800325bb66a92d69c0ea742dd4f754590fa0a02010050100618KzIxMjYzMTQxNTkyNw
52045411530350454063l4.205802MA5907Epicier6010Casablanca64340002ar0107 الدار0213البقالة
8088003237البيضاءb3a355b830b3bf0974d23608a6f1620101102162018-04-05T17:23031833.529704,-
7.639210401063045D01

3.2.3. Format hexadécimal

297 octets :

303030323031303130323132323636383030333235626236366139326436396330656137343264
643466373534353930666130613032303130303530313030363184B7A49784D6A597A4D545178
4E546B794E7735323034353431313533330333530343534303633313422E32303538303240413539
303745706963696572363031304361736162C616E6361363433343030303261723031303D8A7
D984D8A8D982D8A7D984D8A930323133D8A7D984D8AFD8A7D8B120D8A7D984D8A8D98AD8B6D8A7
D8A1383038383030333233376233613335356238333062336266303937346432333630386136663
313632303130313130323136323031382D30342D30355431373A32333033313833332E35323937
30342C2D372E363339323130343031303633303435443031

بنك المغرب
BANK AL-MAGHRIB

3.2.4. Format Image

QR-Code version 16 (81 x 81 modules), ECC niveau 0. Mode byte, texte encode en UTF-8.

3.3. Exemple de chiffrement de référence entité payée

Format de chiffrement (XX-02) = 1 (AES_CBC_ ISO-10126)

Format référence entité payée (XX-05) = 0 (numéro de téléphone)

Numéro de téléphone = +212631415927 (`0x2B32313236333134313539323 7`, 13 octets)

Clé AES (128 bits) = `0x0123456789ABCDEFFEDCBA9876543210`

Vecteur d'Initialisation statique (128 bits) = `0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF`

Numéro de téléphone chiffré = `0xE40A5267E27429FB26C277A4AA71914B` (16 octets) = `5ApSZ+J0KfsmwnekqnGRSw` (22 caractères format Base64)

Référence entité payée (XX-06) = `5ApSZ+J0KfsmwnekqnGRSw`